# REPORT DOCUMENTATION PAGE

*Form Approved*
*OMB No. 0704-0188*

| | | |
|---|---|---|
| **1. REPORT DATE** *(DD-MM-YYYY)*<br>07/24/2023 | **2. REPORT TYPE**<br>Conference Briefing | **3. DATES COVERED** *(From - To)* |

**4. TITLE AND SUBTITLE**
Cyber Threats and Engagements in 2022

**5a. CONTRACT NUMBER**
W56KGU-18-D-0004

**5b. GRANT NUMBER**

**5c. PROGRAM ELEMENT NUMBER**

**6. AUTHOR(S)**
Therese Robin Baisley; Youssef Cherrat;

**5d. PROJECT NUMBER**

**5e. TASK NUMBER**

**5f. WORK UNIT NUMBER**

**7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**
The MITRE Corporation
7515 Colshire Drive
McLean, VA 22102

**8. PERFORMING ORGANIZATION REPORT NUMBER**
PRS-23-2464

**9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)**
U.S. Army Europe and Africa

**10. SPONSOR/MONITOR'S ACRONYM(S)**
USAREUR-AF

**11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

**12. DISTRIBUTION/AVAILABILITY STATEMENT**
DISTRIBUTION STATEMENT A. Approved for public release: distribution unlimited.

**13. SUPPLEMENTARY NOTES**
Presentation for USAREUR-AF 2023 Cybersecurity Summit

**14. ABSTRACT**

*Global Stressors
*Threat Actors
*Technology Trends
*Attack Vectors
*Attack Trends

**15. SUBJECT TERMS**
Network Security; Computer Security; cyber threats; threat actors;

| | | | | | |
|---|---|---|---|---|---|
| **16. SECURITY CLASSIFICATION OF:** | | | **17. LIMITATION OF ABSTRACT** | **18. NUMBER OF PAGES** | **19a. NAME OF RESPONSIBLE PERSON**<br>Susan Carpenito |
| **a. REPORT** | **b. ABSTRACT** | **c. THIS PAGE** | | 77 | **19b. TELEPHONE NUMBER** *(Include area code)*<br>781-271-7646 |

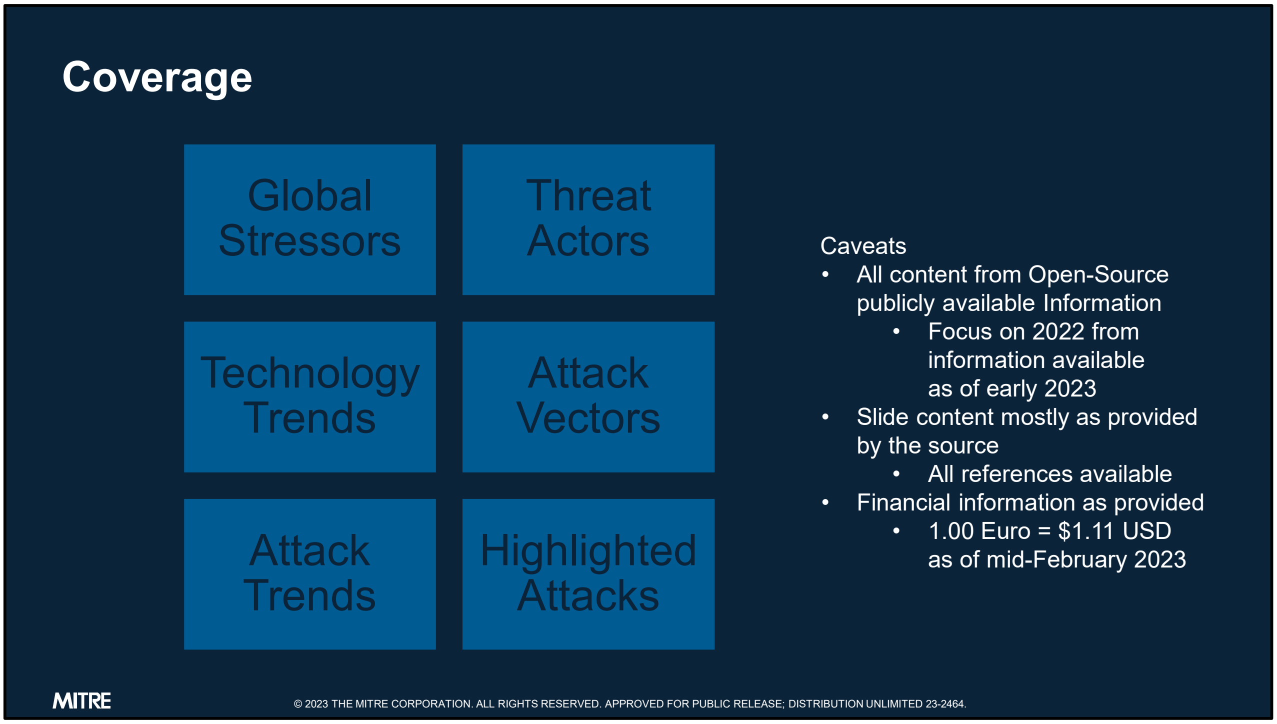
# Cyber Threats and Engagements in 2022

Therese Baisley, MITRE

with Youssef Cherrat, MITRE

July 2023

SOLVING PROBLEMS FOR A SAFER WORLD™



## Coverage

Global Stressors

Threat Actors

Technology Trends

Attack Vectors

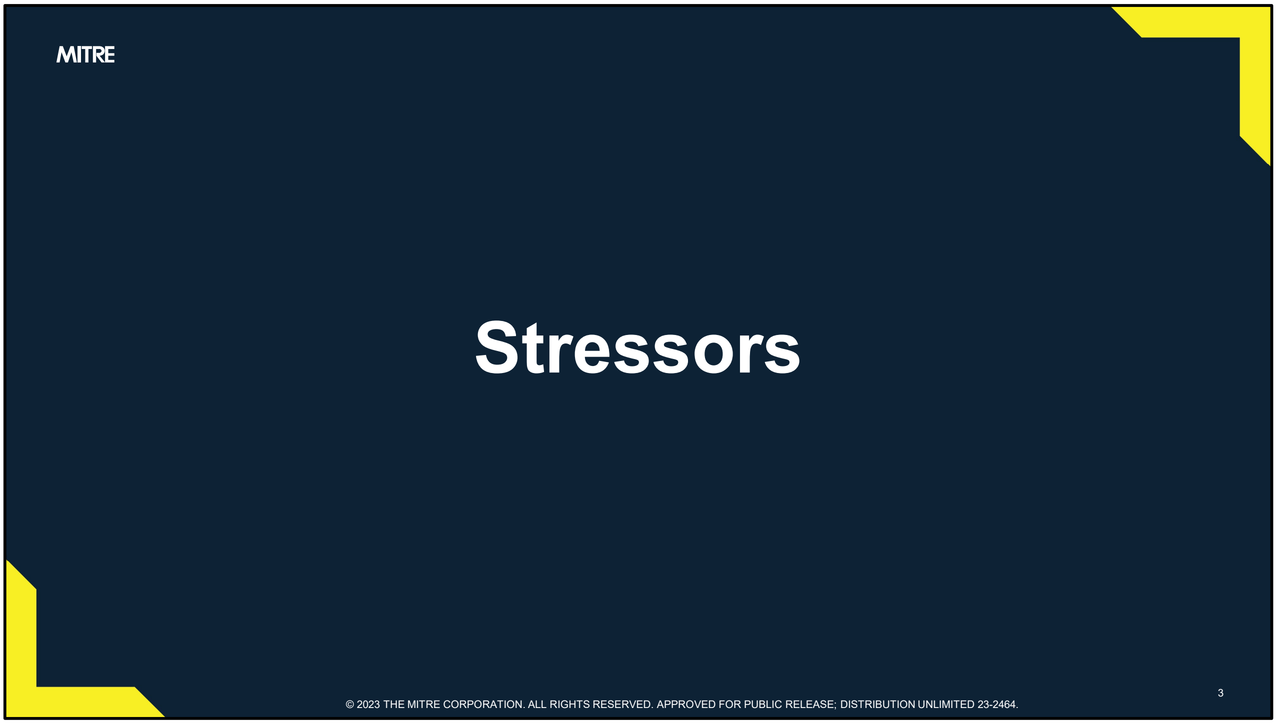
Attack Trends

Highlighted Attacks

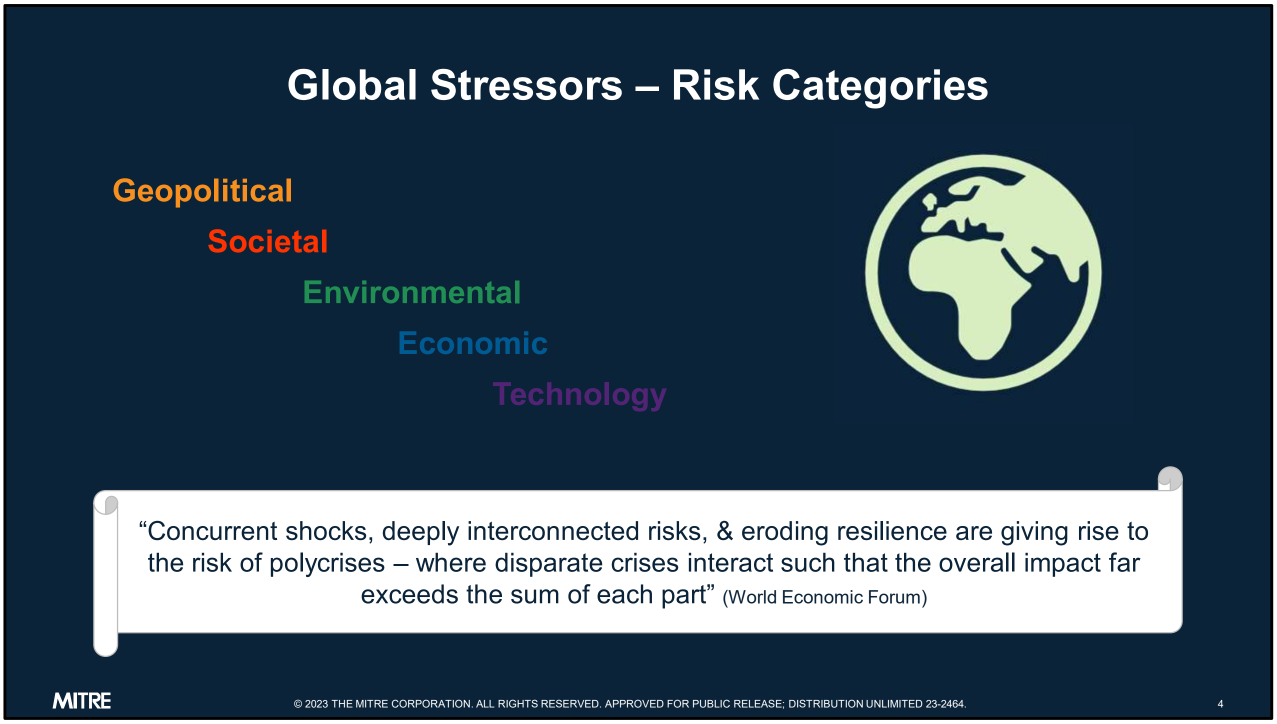
Caveats

- All content from Open-Source publicly available Information
  - Focus on 2022 from information available as of early 2023
- Slide content mostly as provided by the source
  - All references available
- Financial information as provided
  - 1.00 Euro = $1.11 USD as of mid-February 2023

MITRE



# Stressors



## Global Stressors – Risk Categories

Geopolitical

Societal

Environmental

Economic

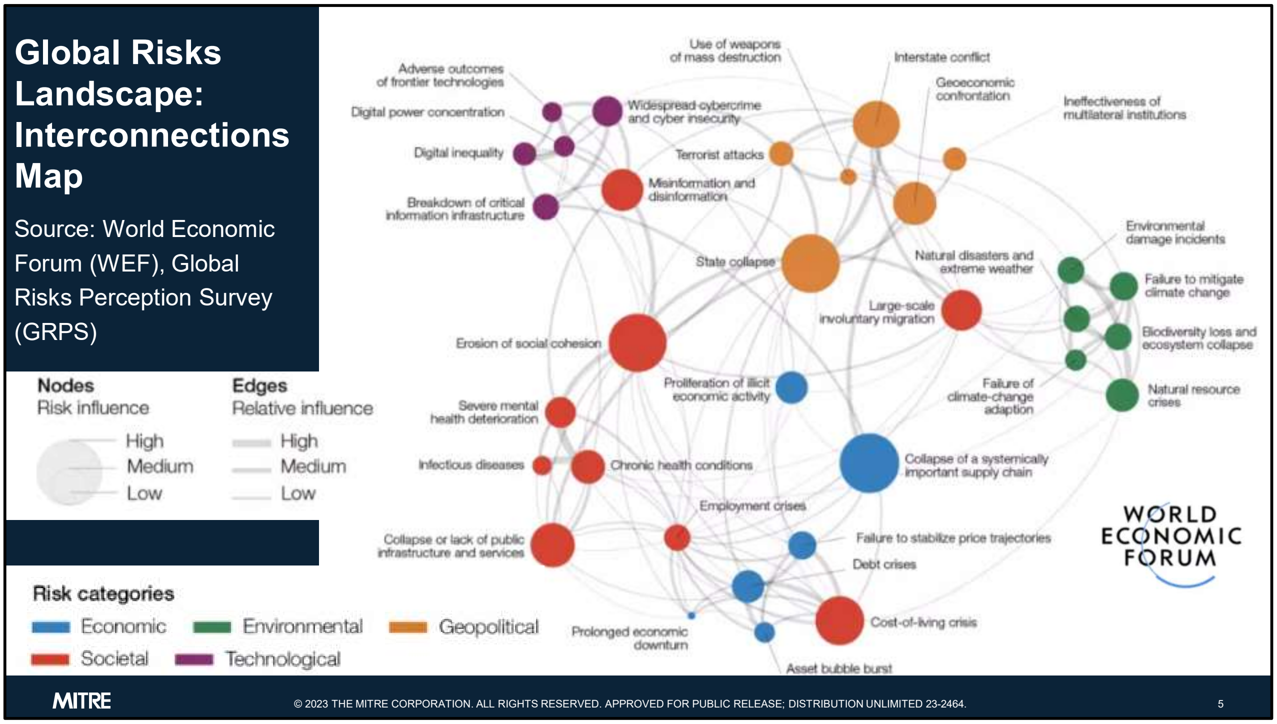
Technology

> “Concurrent shocks, deeply interconnected risks, & eroding resilience are giving rise to the risk of polycrises – where disparate crises interact such that the overall impact far exceeds the sum of each part” (World Economic Forum)

MITRE

Reference(s):

- 2023 Outlook: 5 Finance Risks to Monitor This Year, CFO, https://www.cfo.com/risk-compliance/risk-management/2023/01/2023-risks-to-monitor-economy-inflation-labor-costs-engagement-interest-rates/, 23 January 2023.
- Global Risks Report 2023, World Economic Forum’s (WEF), https://www.weforum.org/reports/global-risks-report-2023/digest, 11 January 2023.



## Global Risks Landscape: Interconnections Map

Source: World Economic Forum (WEF), Global Risks Perception Survey (GRPS)

Use of weapons of mass destruction
Interstate conflict
Adverse outcomes of frontier technologies
Geoeconomic confrontation
Digital power concentration
Widespread cybercrime and cyber insecurity
Ineffectiveness of multilateral institutions
Digital inequality
Terrorist attacks
Misinformation and disinformation
Breakdown of critical information infrastructure
Environmental damage incidents
Natural disasters and extreme weather
State collapse
Failure to mitigate climate change
Large-scale involuntary migration
Biodiversity loss and ecosystem collapse
Erosion of social cohesion
Proliferation of illicit economic activity
Failure of climate-change adaption
Natural resource crises
Severe mental health deterioration
Infectious diseases
Chronic health conditions
Collapse of a systemically important supply chain
Employment crises
Collapse or lack of public infrastructure and services
Failure to stabilize price trajectories
Debt crises
Cost-of-living crisis
Prolonged economic downturn
Asset bubble burst
WORLD ECONOMIC FORUM

**Nodes**
Risk influence
High
Medium
Low

**Edges**
Relative influence
High
Medium
Low

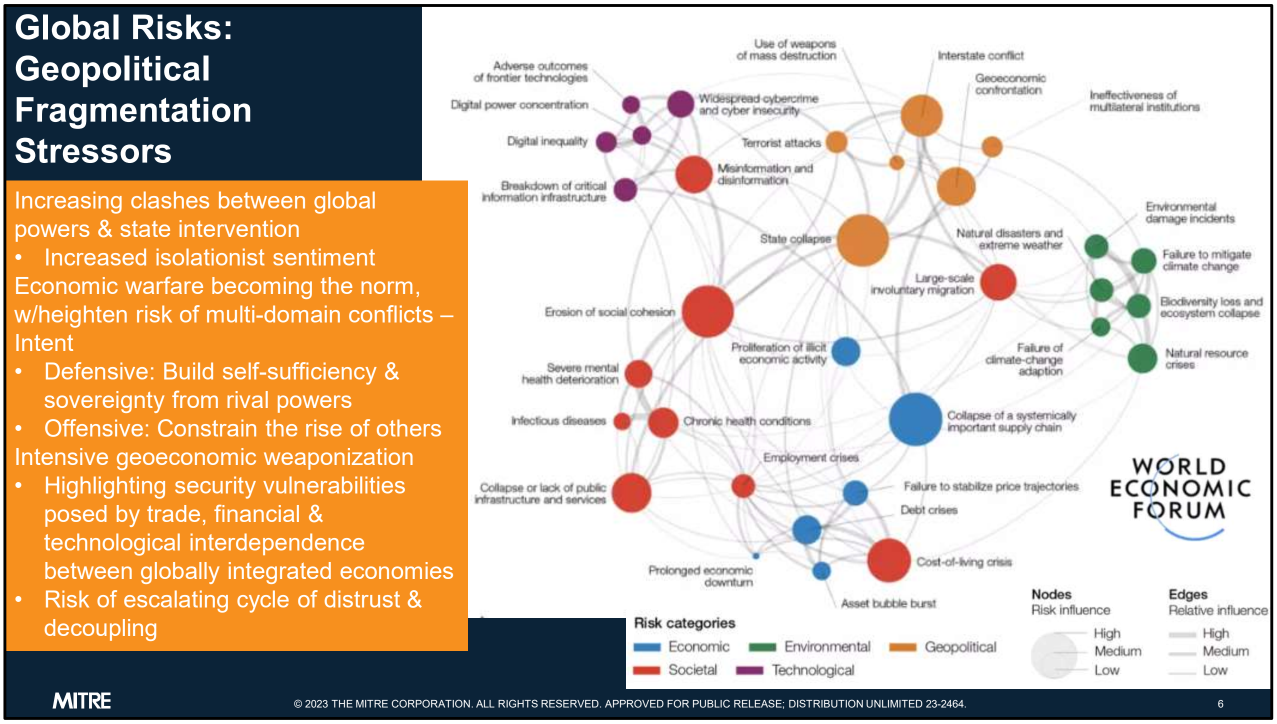
**Risk categories**

- 🟦 Economic
- 🟩 Environmental
- 🟧 Geopolitical
- 🟥 Societal
- 🟪 Technological

MITRE © 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED 23-2464. 5

Reference(s):

- 2023 Outlook: 5 Finance Risks to Monitor This Year, CFO, https://www.cfo.com/risk-compliance/risk-management/2023/01/2023-risks-to-monitor-economy-inflation-labor-costs-engagement-interest-rates/, 23 January 2023.
- Global Risks Report 2023, World Economic Forum's (WEF), https://www.weforum.org/reports/global-risks-report-2023/digest, 11 January 2023.



## Global Risks: Geopolitical Fragmentation Stressors

Increasing clashes between global powers & state intervention

- Increased isolationist sentiment

Economic warfare becoming the norm, w/heighten risk of multi-domain conflicts – Intent

- Defensive: Build self-sufficiency & sovereignty from rival powers
- Offensive: Constrain the rise of others

Intensive geoeconomic weaponization

- Highlighting security vulnerabilities posed by trade, financial & technological interdependence between globally integrated economies
- Risk of escalating cycle of distrust & decoupling

Use of weapons of mass destruction
Interstate conflict
Adverse outcomes of frontier technologies
Geoeconomic confrontation
Digital power concentration
Widespread cybercrime and cyber insecurity
Ineffectiveness of multilateral institutions
Digital inequality
Terrorist attacks
Breakdown of critical information infrastructure
Misinformation and disinformation
Environmental damage incidents
State collapse
Natural disasters and extreme weather
Failure to mitigate climate change
Large-scale involuntary migration
Biodiversity loss and ecosystem collapse
Erosion of social cohesion
Proliferation of illicit economic activity
Failure of climate-change adaption
Natural resource crises
Severe mental health deterioration
Infectious diseases
Chronic health conditions
Collapse of a systemically important supply chain
Employment crises
WORLD ECONOMIC FORUM
Collapse or lack of public infrastructure and services
Failure to stabilize price trajectories
Debt crises
Cost-of-living crisis
Prolonged economic downturn
Asset bubble burst
Risk categories
Economic
Environmental
Geopolitical
Societal
Technological
Nodes
Risk influence
High
Medium
Low
Edges
Relative influence
High
Medium
Low

MITRE

© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED 23-2464.

6

Reference(s):

- Global Risks Report 2023, World Economic Forum's (WEF), https://www.weforum.org/reports/global-risks-report-2023/digest, 11 January 2023.
- The ripple effects of Russia's war in Ukraine continue to change the world, NPR, Scott Neuman & Alyson Hurt, https://www.npr.org/2023/02/22/1157106172/ukraine-russia-war-refugees-food-prices, 22 February 2023.
- The key trends to watch in the Russia-Ukraine war, NPR, Greg Myre, https://www.npr.org/2023/02/25/1159274649/key-trends-russia-ukraine-war-second-year, 25 February 2023.
- How Ukraine Is Crowdsourcing Digital Evidence of War Crimes, TIME, Vera Bergengruen, https://time.com/6166781/ukraine-crowdsourcing-war-crimes/, 18 April 2022.
- Inside the Kremlin's Year of Ukraine Propaganda, TIME, Vera Bergengruen, https://time.com/6257372/russia-ukraine-war-disinformation/, 22 February 2023.
- Telegram is the app of choice in the war in Ukraine despite experts' privacy concerns, NPR, Bobby Allyn https://www.npr.org/2022/03/14/1086483703/telegram-ukraine-war-Russia, 14 March 2022.

Note(s):

- Crowdsource apps, chatbots & websites all feed into one centralized database set up by the office of Ukraine's Prosecutor General (TIME 11 April 2022)

- Website collected 10,000+ submissions of detailed evidence from citizens (TIME 11 April 22): https://warcrimes.gov.ua/
- War crimes portal dashboard lists ~6,500 submissions
  - Simple interface to share current location, show coordinates, upload files, & submit a link to Facebook, TikTok, or other social media
  - Site offers 18 detailed categories, including sexual violence, torture, death, hostage taking, kinds of weapons, and whether victim is a child
- e-Enemy chatbot, monitored 24/7
- Government mobile chatbot app w/verified Ukrainian citizen users:
  - Options illustrated by icons of military helmets and targets
    - Automated prompt helps one report Russian troop movements in your area, and rewards you with a flexed-arm emoji & message: "Remember each of your shots in this bot means one less enemy"
    - Menu option, illustrated by a droplet of blood, prompts Ukrainians to report and submit footage of war crimes in places now associated with horrific atrocities: Bucha, Irpin, Gostomel
  - 253,000+ people have sent reports and footage of Russian forces' movements
  - 66,000+ people submitted evidence of damage to their homes and cities - information is tied to a verified identity and location

Social media is Ukrainians' primary news source, surpassing television in 2020 (NPR)

- Telegram is the messaging app of choice in the war in Ukraine despite experts' privacy concerns
- Founded by Russian brothers, Nikolai and Pavel Durov after fleeing Russia due to allies of the Kremlin took control of their social networking VKontakte (VK) site & Russia's intelligence agency them to turn over anti-Kremlin protesters data
- Source of unverified information
  - Messages are not fully encrypted by default - significant risk of insider threat or hacking of Telegram systems

- Supports:

- Reinventing modern warfare
- Geolocate enemy movements in real-time
- Defense against Russian & pro-Kremlin activists' disinformation & targeted propaganda
    - Russia’s techniques include use of fake accounts, manipulated imagery like deepfakes, forged documents, and videos with fake news tickers purporting to be from respected brands like the BBC or Al Jazeera
    - Operatives aim to increase mistrust in foreign audiences about the credibility of Ukraine’s government and the effectiveness of its military (e.g., create customized messages to different audiences all over the globe)
    - Russia co-opted popular fact-checking formats. It created a host of multilingual channels, like one named “War on Fakes,” which “verified” or “fact-checked” allegations to support pro-Kremlin narratives and defend the Russian military’s actions. The original Russian-language channel amassed more than 750,000 followers on Telegram, and its website translated its content into Arabic, Chinese, English, French, German, and Spanish, which was then amplified by Russian embassies and other government channels, according to the report.
    - Uses Telegram as hub for Russian propaganda and misinformation
- Cataloging damages for future reparations
- Historic record
- Digital proof of war crimes
    - Levels up use of open-source information as evidence
    - Categorizes different kinds of war crimes and human-rights violations
- Contribute to international law development & use of open-source information as evidence in complex cases
- Modification of social-media practices (e.g., Pulling down content that might document eyewitness accounts of war crimes for violating its rules)
    - Note: Meta, owns Facebook & Instagram, “exploring ways to preserve this type & other types of content when we remove it” when it comes to the war in Ukraine

From How Ukraine Is Crowdsourcing Digital Evidence of War Crimes

It all looks like a game at first. Verified users of Ukraine's government mobile app are greeted with options illustrated by icons of military helmets and targets. An automated prompt helps you report Russian troop movements in your area, and rewards you with a flexed-arm emoji. "Remember," the message says. "Each of your shots in this bot means one less enemy." Another option on the menu, illustrated by a droplet of blood, prompts Ukrainians to report and submit footage of war crimes in places now associated with horrific atrocities: Bucha, Irpin, Gostomel.

This chatbot, created by Ukraine's Digital Ministry and dubbed "e-Enemy," is one of half a dozen digital tools the government has set up to crowdsource and corroborate evidence of alleged war crimes. Since the start of the invasion, Ukrainian officials, lawyers and human-rights groups have scrambled to design new ways to catalogue and verify reams of video, photo and eyewitness accounts of criminal behavior by Russian forces. Ukraine has adapted popular government apps to allow citizens to document damage to their homes, used facial-recognition software to identify Russian military officials in photos, and rolled out new tools to guide users through the process of geo-tagging and time-stamping their footage in hopes it may help authorities hold the perpetrators responsible.

The result is a systematic effort unlike any in the history of modern warfare, experts say. Crowdsourcing digital proof of war crimes from witnesses has been done in other conflicts, but "the use of open-source information as evidence in the case of Ukraine may be at altogether a different level," says Nadia Volkova, director of the Ukrainian Legal Advisory Group and a member an alliance of Ukrainian human-rights organizations called the 5AM coalition. Named for the time the Russian invasion began on Feb. 24, the group trains volunteers to document eyewitness testimony, and to collect, preserve and verify evidence in accordance with international protocols. The goal is not only to achieve justice for the victims, Volkova says, "but also contribute to the development of international law and the use of open-source information as evidence in complex cases."

The apps, chatbots and websites designed by Ukrainian officials categorize different kinds of war crimes and human-rights violations and all feed into one centralized database set up by the office of Ukraine's Prosecutor General. These include the killing or injury of civilians by Russians; physical violence or imprisonment; denial of medical care; looting; and seizure of property by occupying forces. Verified users are prompted to report violence against medical staff or religious clergy; damage to civilian infrastructure; and the use of military equipment in residential areas. Reports from chatbots like "e-Enemy" are also shared with the military, and have led Ukrainian forces to mount successful attacks on Russian positions, according to Ukraine's Security Service.

Ukrainians are rallying to the cause. A website set up by the office of Ukraine's Prosecutor General, warcrimes.gov.ua, has received more than 10,000 submissions of detailed evidence from citizens, an official told TIME. The government's efforts are supported by a legion of outside human-rights groups, citizen sleuths, cyber-volunteers, retired military officials, journalists, and open-source analysts with experience documenting this kind of proof in previous conflicts.

What all this will yield is still unclear. International war-crimes cases are notoriously difficult to prosecute. Successful efforts are typically built on traditional forensic evidence, witness testimonies and documents. But Ukrainian officials say the purpose of using digital tools to crowdsource evidence of Russian atrocities extends far beyond a war-crimes trial in The Hague. They see it as a defense against a flood of Russian disinformation, including claims from high-ranking Kremlin officials that the horrors from Bucha or Mariupol are "fake" or staged. And they believe it will create a historical record that will help hold the guilty responsible and win restitution for the victims.

Mykhailo Fedorov, Ukraine's Minister of Digital Transformation, says the country's collection and use of so-called "citizen evidence" is another way that Ukraine is reinventing modern warfare. "This war has been the most radical shift in warfare since WWII, at least in Europe," Fedorov tells TIME. "If you look at what happened in cyber war, we have changed the playbook basically overnight…I firmly believe that we will be able to change the way international justice is being administered as well in the aftermath of this war."

A few weeks into the war, a column of Russian armored vehicles with missile launchers rumbled through a neighborhood near Kherson, in southern Ukraine. As it rolled past an intersection, staff at Ukraine's digital ministry back in Kyiv watched as the "e-Enemy" chatbot, which is monitored 24/7, lit up with dozens of reports from residents' windows block by block. "Almost every apartment sent us a report," Fedorov recalls. "So we could geolocate them to almost every apartment on those two streets."

Since the beginning of the invasion, Fedorov's ministry has encouraged citizens to see the government apps on their phones as essential wartime tools. Ukrainians can use them for everything from applying for relocation funds to reporting the actions of Russian forces. But government officials quickly realized that their pre-war project to digitize the country's government services—passport applications, registering newborns—had now become an invaluable tool for documenting war crimes. The apps they had set up not only gave millions of Ukrainians a direct line to the government and military through the device in their pockets, but also automatically verified their identities.

In order to report anything through the e-Enemy chatbot, users have to log in through a portal launched in 2020 that lets Ukrainians share digital identifying documents on their smartphones for more than 50 government services. More than 17 million Ukrainians—roughly 40% of the population—uses the app, according to Fedorov. "We use rigorous authentication in order to weed out fake content, so we know who the person behind the report is," he says.

One example of an interaction shared with TIME show emojis and arrows guiding users through a series of automated prompts: first making sure they are safe, then telling them to focus their camera on enemy actions, shooting video for up to one minute, and attaching a timestamp and geolocation. "It corrals you towards doing the right things, so it will require several photos from certain angles and so forth," Fedorov says. "As a result, about 80% to 90% of the user-submitted content is usable by us and by our authorities."

More than 253,000 people have sent reports and footage of Russian forces' movements and actions through the chatbot, according to digital ministry officials. More than 66,000 people have submitted evidence of damage to their homes and cities, which a new state service is cataloging for future reparations. All this information is tied to a verified identity and location, creating a stream of information fed into a centralized database maintained by the Office of the Prosecutor General to corroborate reports of war crimes.

Many Ukrainian prosecutors now working on war-crimes investigations had previously been trained in using open-source intelligence, or OSINT, in human-rights cases following Russia's invasion of eastern Ukraine in 2014, says Serhiy Kropyva, a digital adviser to the Prosecutor General. "So we have experience with this kind of evidence, and we've focused all the forces of our prosecutors on the war crimes claims," Kropyva tells TIME. "It's still really hard, and all of us understand we need to operate really quickly to store all the evidence from the beginning if we want to use [it] in different courts."

The dashboard on the government's war crimes portal lists almost 6,500 submissions of photos, videos, and other documentation. One graphic on "crimes against children" counts at least 191 children killed and 349 wounded. The Prosecutor General's office has advertised the site through television interviews as well as billboards and digital banners, Kropvya says, encouraging Ukrainians to report any violations.

A simple interface allows users to share their current location to show coordinates, upload files, and submit a link to Facebook, TikTok, or other social media. The site offers 18 detailed categories, including sexual violence, torture, death, hostage taking, kinds of weapons, and whether victim is a child.

Another section is labeled "Enemy's personal data," allowing the user to provide any identifying information about Russian troops, including "documents, passports, call signs and pseudonyms, identification marks." As of April 14, the office said it has identified 570 "suspects," including Russian military and political officials, ministers, and heads of law enforcement.

The protocols for prosecution - Holding them accountable will be a complicated process. Even though Ukraine is not part of the International Criminal Court (ICC), a permanent body that has investigated war crimes for two decades, it has given it jurisdiction to prosecute war crimes committed in its territory. Last month, the ICC said it was opening an investigation and gathering evidence. But it too has been grappling with how to handle the barrage of digital evidence. Its top prosecutor, Karim Khan, has asked for new funding for technology to help his office. “Conflicts and international crises now generate audio, visual and documentary records on a massive scale,” he said in a statement on March 28. “The commission of international crimes leaves a significant digital footprint.”

Several countries have sent their own fact-finding missions, and the U.N. Human Rights Council has established a commission to investigate violations. These efforts are also backed up by a dizzying array of international human-rights analysts and organizations that use OSINT, including satellite imagery, weapons analysis, and geolocations tools.

While the use of OSINT to document war crimes is not new, one change has been the widespread adoption of the Berkeley Protocol, the first set of global guidelines that lays out standards for the collection of public digital information, including social media, as evidence for the investigation of human-rights violations. The protocol was published in 2020 after a three-year collaboration between the U.N. Office of Human Rights and the Human Rights Center at the University of California, Berkeley, building largely on the lessons of the war in Syria.

Most Ukrainian groups who spoke to TIME said they were using the Berkeley Protocol to determine how best to document and preserve evidence, as well as ethical and legal guidance for gathering eyewitness accounts. That could mean that a larger share of the evidence collected by these organizations and by the Ukrainian government will meet evidentiary standards of international courts of law. One key, experts say, is to focus on documentation that could identify those involved and communications that would help provide evidence of intent.

“Trying war criminals is incredibly difficult because the burden of proof is so high,” says Flynn Coleman, an international human-rights lawyer who has focused on digital war-crimes documentation. “The technology often moves faster than the laws…But there are indications that the legal system is moving toward accepting more of this citizen evidence.”

Still, the value of Ukraine’s crowdsourced evidence goes beyond what can be proven in international court. “It’s a basic right for all the survivors and families,” Coleman says. “We need a record for humanity of what happened here: not just justice, but a record, because memories fade. And we need to do it now, while recollections are fresh.”

This urgency has also led Fedorov and other officials to ask social-media companies to reconsider some of their practices, like pulling down content that might document eyewitness accounts of war crimes for violating its rules.

“The community guidelines were made in peaceful countries to account for normal, everyday communication going on in peacetime,” says Fedorov, who said he has recently asked companies like Meta to revise these guidelines for countries that are in an active state of war. “Some content which might not be permissible in peacetime could be instrumental to proving war crimes.”

Meta, which owns Facebook and Instagram, is "exploring ways to preserve this type and other types of content when we remove it" when it comes to the war in Ukraine, spokesman Andy Stone said on April 4. (Stone declined to provide further details to TIME.)

Ukrainian officials say they'll continue ramping up their efforts to create the most comprehensive body of digital evidence ever assembled in a modern war. Asked if he believes these efforts will be successful, Fedorov does not hesitate. "One hundred percent," he tells TIME. "We have satellite imagery, we have the verified content from our apps, we have other sources that I'm not at liberty to disclose…I am very sure it will help us prove our case in international jurisdictions."

For now, that promise is repeated every time a Ukrainian citizen uses the "e-Enemy" app to provide information about the actions of Russian forces. With every new crowdsourced report, a message pops up in the app: "Their relatives, friends and the whole world will learn about their brutal crimes against the Ukrainian people."

## From Inside the Kremlin's Year of Ukraine Propaganda

Three weeks after Russia invaded Ukraine last Feb. 24, a video appeared on a Ukrainian news site that seemed to show President Volodymyr Zelensky imploring his fellow countrymen to stop fighting and urging soldiers to lay down their weapons.

"There is no need to die in this war," he seemed to say in the video, which was widely circulated on social media and appeared briefly on Ukrainian television with a news ticker suggesting that he had fled the country. "I advise you to live."

The video—a crude deepfake that had been posted by hackers—was quickly taken down and debunked. It was dismissed by the real Zelensky as a "childish provocation," and roundly mocked online as an example of Russia's desperate and often cartoonish attempts to spread fake news. But researchers say the deepfake is just one example of a barrage of disinformation, manipulated imagery, forged documents, and targeted propaganda unleashed by Russia and pro-Kremlin activists that may have had a significant impact on audiences over the last year of war.

"Changing people's minds and positions is much harder than simply sowing doubt or fear," says Andy Carvin, a senior fellow at the Atlantic Council's Digital Forensic Research Lab, which has tracked Russian hybrid warfare activities since 2015 and on Wednesday released a pair of reports analyzing the Kremlin's information warfare before and after the invasion. "It's one of the reasons why Kremlin information operations focus so much on essentially generating chaos, causing contagion, causing a loss of morale, or just getting people simply confused about what's true and what's not."

Over the past year, the Kremlin and its allies used a dizzying array of strategies to defend its actions, seed doubt about news from the ground, and push misleading or false narratives to undercut support for Ukraine. Denied the easy victory they had hoped for, Russian officials working to erode global trust in Ukraine as a reliable partner. "To defeat Ukraine on the battlefield," the report argues, "Russia needed to strangle all sympathy and support for Ukraine as well."

In pursuit of that goal, the Kremlin targeted everyone from Ukrainian citizens to right-wing groups in the U.S. and Europe, countries taking in Ukrainian refugees and those supplying crucial aid, and potentially sympathetic audiences in Africa and Latin America, as well as domestic audiences in Russia itself. Russia's techniques for spreading these narratives included the use of fake accounts, manipulated imagery like deepfakes, forged documents, and videos with fake news tickers purporting to be from respected brands like the BBC or Al Jazeera. In other cases, operatives simply aimed to increase mistrust in foreign audiences about the credibility of Ukraine's government and the effectiveness of its military.

While many of these efforts may seem inept to digitally savvy Western observers, it's a mistake to depict Russia as "losing" the information war, says Carvin, who oversaw the project. "There really isn't a single information war going on," he says. "Russia and Ukraine are fighting multiple battles, but Russia has the resources to create customized messages to different audiences all over the globe…And in some parts of the world, their messages resonate better than others."

Before Putin ordered tens of thousands of troops into Ukraine, the Kremlin spent years seeding false narratives to justify military action. When the invasion began, the effort kicked into overdrive. Ukrainian researchers were taken aback by the volume of false information in the war's opening weeks.

"It very hard [to know what to believe], especially when you hear the bombs outside of your window," says Ksenia Iliuk, the co-founder of LetsData, a non-profit that uses artificial intelligence to analyze hostile information operations. In the first month of the invasion, her team identified about 35 new, unique pieces of Russian propaganda or disinformation narratives per day.

Ukrainian officials treated the digital space as a front line in the war from the start, setting up teams and processes to verify the facts in all updates posted on official channels as a way to pre-empt any challenges to their credibility. "In a way, we are trying to protect our brand," Ukraine's Minister of Digital Transformation, Mykhailo Fedorov, told TIME last March. "Our brand as one of an honest nation and an honest people trying to tell the truth."

Social media is Ukrainians' primary news source—surpassing television in 2020, according to a recent survey—and the Russians targeted popular apps with false narratives meant to demoralize the population, create panic, and undermine trust in Zelensky. Much of the information battle was fought on Telegram, a messaging app that surged in popularity due to its largely unmoderated platform which allowed raw footage of the war to be widely disseminated. The structure of the app made it easy to build massive propaganda channels that spread fake photos and videos to millions of followers.

As part of an effort to target Telegram, Russia co-opted popular fact-checking formats. It created a host of multilingual channels, like one named “War on Fakes,” which “verified” or “fact-checked” allegations to support pro-Kremlin narratives and defend the Russian military’s actions. The original Russian-language channel amassed more than 750,000 followers on Telegram, and its website translated its content into Arabic, Chinese, English, French, German, and Spanish, which was then amplified by Russian embassies and other government channels, according to the report.

Russia combined these efforts with more traditional intimidation tactics, including dropping leaflets in Dnipropetrovsk describing what residents should do if there was an explosion at the Zaporizhzhia nuclear power plant, military training flights that set off air-raid sirens, and rumors—fueled by Putin himself—that speculated about the potential use of nuclear weapons.

Some of these narratives hit their mark, breaking through on a global scale. False allegations spread by the Kremlin that Ukraine was utilizing U.S.-funded research labs to develop bioweapons were widely amplified by prominent U.S. right-wing voices last summer. The right-wing channel One America News ran segments spreading the Kremlin’s conspiracies that the Russian strike on a maternity hospital in Mariupol was a “false flag.”

The Russian government blocked access to Western social media platforms inside their own country—even designating Meta an “extremist organization”—criminalized independent reporting on the invasion, and passed a law imposing up to 15 years in prison for spreading intentionally “fake” news about the war. It also targeted the Russian diaspora abroad. In Europe, the Kremlin carried out “multichannel, full-spectrum disinformation campaigns” with tailored messages for different countries. For example, it used statements by high-level Russian officials, inauthentic social media accounts, and doctored documents to spread claims that Poland was planning to occupy parts of western Ukraine. In France, pro-Kremlin accounts amplified false claims of widespread reselling of Ukrainian weapons on the black market and hyped up fears that Europeans would freeze in the winter without access to Russian gas.

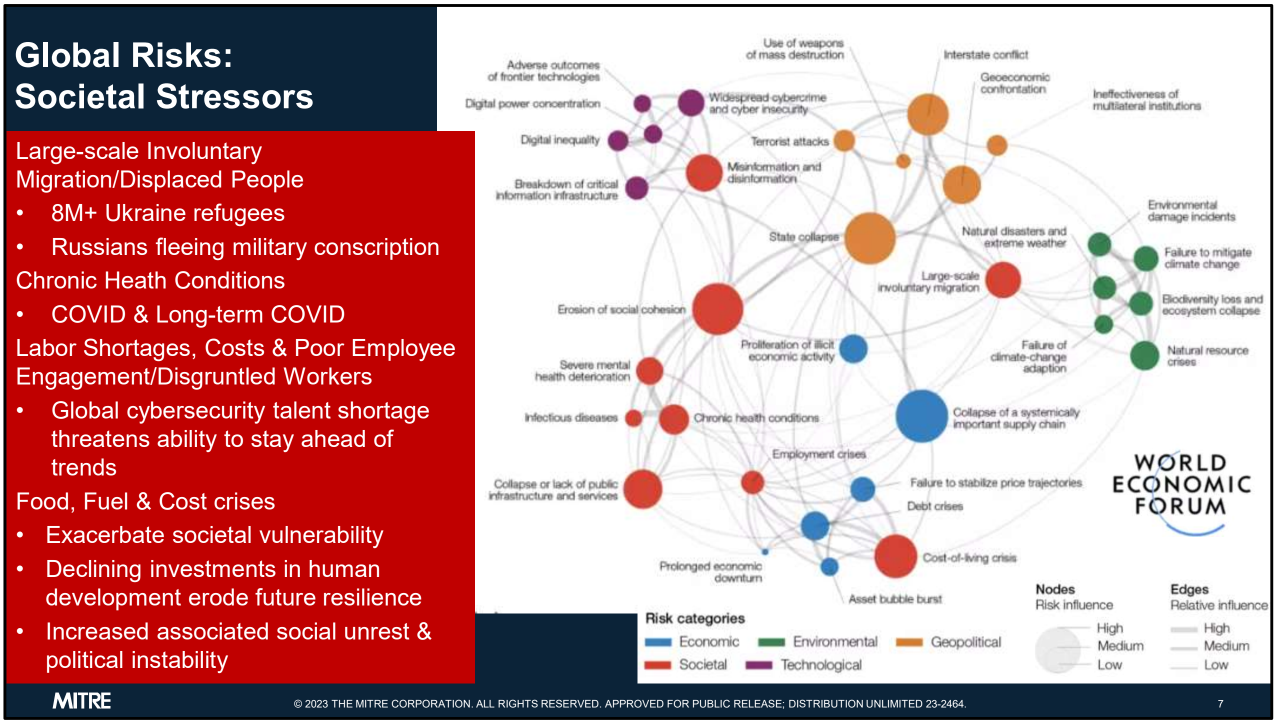
Pro-Kremlin media also continued to pour resources into Africa and Latin America, exploiting historical distrust in the West and anti-imperialist sentiments. “By maintaining these information operations at a global scale, Russia has successfully prevented international consensus rallying behind Ukraine at a level that is often presumed in the West,” the report found.

As the war enters its second year, the Kremlin is likely to continue to use these techniques to influence ongoing debates about whether to continue to supply Ukraine with weapons and funding, the report suggests. Russia may also continue to take advantage of the sympathy of China's global media ecosystem towards their interests, according to researchers.

“Russia's reputation as unparalleled information warriors has taken a beating in the West, but this view is by no means universal,” the report's authors found. “The more accurate assessment is that the impacts of information operations related to the war will have a much longer shelf life, well beyond the confines of the current conflict.”

Other

Three weeks after Russia invaded Ukraine last Feb. 24, a Video seemed to show Ukranian President Volodymyr Zelensky imploring his fellow countrymen to stop fighting and urging soldiers to lay down their weapons widely circulated on social media and appeared briefly on Ukrainian television



## Global Risks: Societal Stressors

Large-scale Involuntary Migration/Displaced People

- 8M+ Ukraine refugees
- Russians fleeing military conscription

Chronic Heath Conditions

- COVID & Long-term COVID

Labor Shortages, Costs & Poor Employee Engagement/Disgruntled Workers

- Global cybersecurity talent shortage threatens ability to stay ahead of trends

Food, Fuel & Cost crises

- Exacerbate societal vulnerability
- Declining investments in human development erode future resilience
- Increased associated social unrest & political instability

Use of weapons of mass destruction
Interstate conflict
Adverse outcomes of frontier technologies
Geoeconomic confrontation
Digital power concentration
Widespread cybercrime and cyber insecurity
Ineffectiveness of multilateral institutions
Digital inequality
Terrorist attacks
Misinformation and disinformation
Breakdown of critical information infrastructure
Environmental damage incidents
State collapse
Natural disasters and extreme weather
Failure to mitigate climate change
Large-scale involuntary migration
Biodiversity loss and ecosystem collapse
Erosion of social cohesion
Proliferation of illicit economic activity
Failure of climate-change adaption
Natural resource crises
Severe mental health deterioration
Infectious diseases
Chronic health conditions
Collapse of a systemically important supply chain
Employment crises
WORLD ECONOMIC FORUM
Collapse or lack of public infrastructure and services
Failure to stabilize price trajectories
Debt crises
Cost-of-living crisis
Prolonged economic downturn
Asset bubble burst
Nodes
Risk influence
High
Medium
Low
Edges
Relative influence
High
Medium
Low
Risk categories
Economic
Environmental
Geopolitical
Societal
Technological

Reference(s):

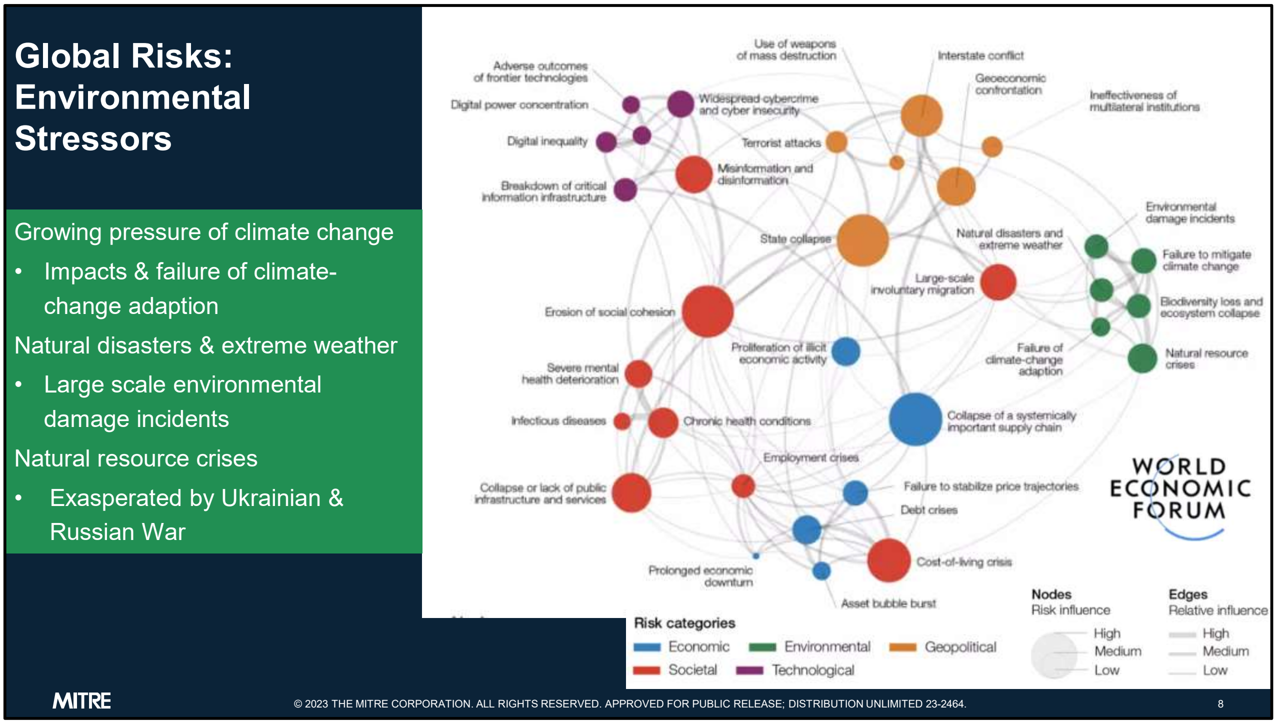
- 2023 Outlook: 5 Finance Risks to Monitor This Year, CFO, https://www.cfo.com/risk-compliance/risk-management/2023/01/2023-risks-to-monitor-economy-inflation-labor-costs-engagement-interest-rates/, 23 January 2023.
- Global Risks Report 2023, World Economic Forum's (WEF), https://www.weforum.org/reports/global-risks-report-2023/digest, 11 January 2023.
- The ripple effects of Russia's war in Ukraine continue to change the world, NPR, Scott Neuman & Alyson Hurt, https://www.npr.org/2023/02/22/1157106172/ukraine-russia-war-refugees-food-prices, 22 February 2023.
- Global Perspectives on Threat Intelligence, Mandiant now part of Google, Global-Perspectives-on-Threat-Intelligence-2-08-23.pdf, https://www.mandiant.com/global-perspectives-on-threat-intelligence, 8 February 2023.
- NYSIF SHINING A LIGHT ON LONG COVID: An Analysis of Workers' Compensation Data; NYSIF report leveraged NYSIF's data to contribute to the broader research on Long Covid. It analyzes the more than 3,000 established Covid-19 workers' compensation claims NYSIF received between 1 January 2020 and 31 March 2022, http://cl.s7.exct.net/?qs=a825d7d59e39500582395979c999633c45d0439195b912bb0877a34a88da43aa0e9ca5ca46660248b834f0f0b6a33486, January 2023.
- Steven Phillips and Michelle A. Williams, *Confronting Our Next National Health Disaster – Long-Haul Covid,* The New England Journal of Medicine,

https://www.nejm.org/doi/full/10.1056/NEJMp2109285, 12 August 2021.

- Benjamin Mazer, *Long COVID Could be a ‘Mass Deterioration Event,’* The Atlantic, https://www.theatlantic.com/health/archive/2022/06/long-covid-chronic-illnessdisability/661285/, 15 June 2022.

Note(s):

- Over 8million Ukraine refugees, largest European Region movement of people since World War II (WHO)
- COVID
    - Long-term COVID
    - Long-term health issues
        - NYSIF >3K COVID-19 workers’ compensation claims January 2020 through March 2022
        - Emerging threat to public health with ongoing, cascading, and yet unclear implications for employers, households, individuals, and the economy (New England Journal of Medicine)
        - Heart implications



## Global Risks: Environmental Stressors

Growing pressure of climate change

- Impacts & failure of climate-change adaption

Natural disasters & extreme weather

- Large scale environmental damage incidents

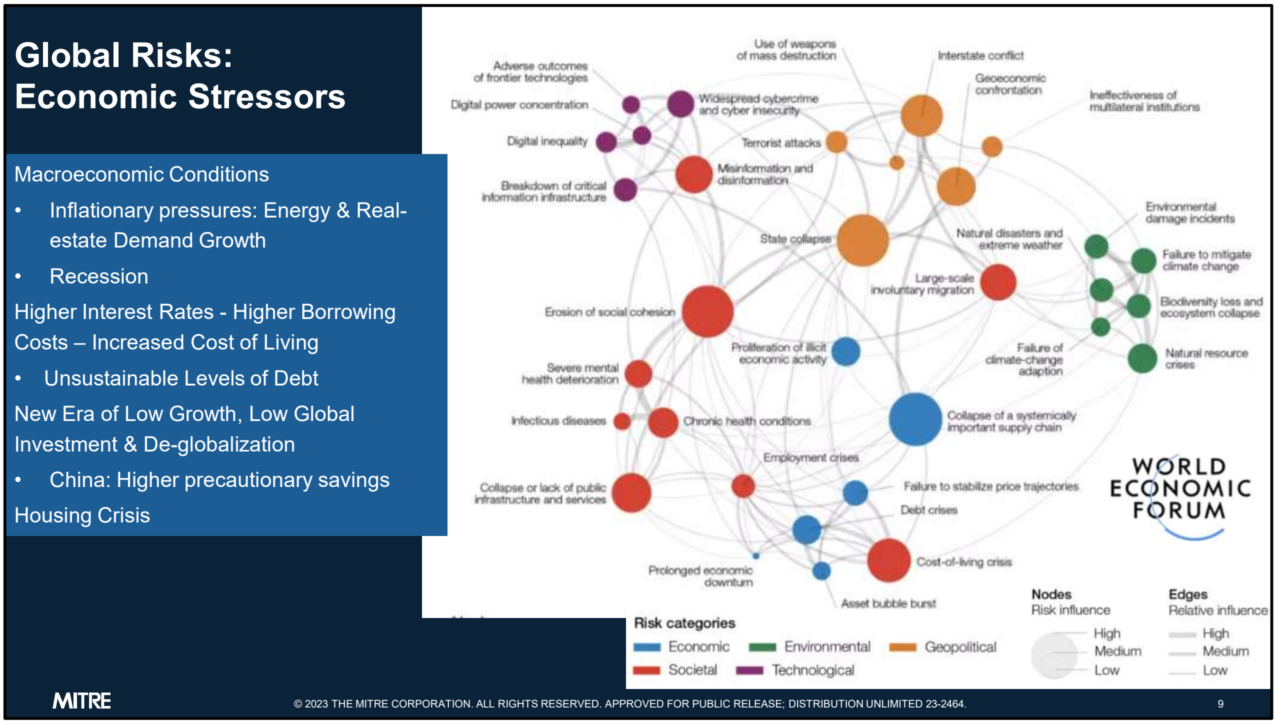
Natural resource crises

- Exasperated by Ukrainian & Russian War

Use of weapons of mass destruction
Interstate conflict
Adverse outcomes of frontier technologies
Geoeconomic confrontation
Ineffectiveness of multilateral institutions
Digital power concentration
Widespread cybercrime and cyber insecurity
Digital inequality
Terrorist attacks
Misinformation and disinformation
Breakdown of critical information infrastructure
Environmental damage incidents
State collapse
Natural disasters and extreme weather
Failure to mitigate climate change
Large-scale involuntary migration
Biodiversity loss and ecosystem collapse
Erosion of social cohesion
Proliferation of illicit economic activity
Failure of climate-change adaption
Natural resource crises
Severe mental health deterioration
Infectious diseases
Chronic health conditions
Collapse of a systemically important supply chain
Employment crises
WORLD ECONOMIC FORUM
Collapse or lack of public infrastructure and services
Failure to stabilize price trajectories
Debt crises
Cost-of-living crisis
Prolonged economic downturn
Asset bubble burst
Nodes
Risk influence
High
Medium
Low
Edges
Relative influence
High
Medium
Low
Risk categories
🟦 Economic
🟩 Environmental
🟧 Geopolitical
🟥 Societal
🟪 Technological
MITRE

Reference(s):

- Global Risks Report 2023, World Economic Forum’s (WEF), https://www.weforum.org/reports/global-risks-report-2023/digest, 11 January 2023.



## Global Risks: Economic Stressors

Macroeconomic Conditions

- Inflationary pressures: Energy & Real-estate Demand Growth
- Recession

Higher Interest Rates - Higher Borrowing Costs – Increased Cost of Living

- Unsustainable Levels of Debt

New Era of Low Growth, Low Global Investment & De-globalization

- China: Higher precautionary savings

Housing Crisis

Use of weapons of mass destruction
Interstate conflict
Adverse outcomes of frontier technologies
Geoeconomic confrontation
Digital power concentration
Widespread cybercrime and cyber insecurity
Ineffectiveness of multilateral institutions
Digital inequality
Terrorist attacks
Breakdown of critical information infrastructure
Misinformation and disinformation
Environmental damage incidents
State collapse
Natural disasters and extreme weather
Failure to mitigate climate change
Large-scale involuntary migration
Biodiversity loss and ecosystem collapse
Erosion of social cohesion
Proliferation of illicit economic activity
Failure of climate-change adaption
Natural resource crises
Severe mental health deterioration
Infectious diseases
Chronic health conditions
Collapse of a systemically important supply chain
Employment crises
WORLD ECONOMIC FORUM
Collapse or lack of public infrastructure and services
Failure to stabilize price trajectories
Debt crises
Cost-of-living crisis
Prolonged economic downturn
Asset bubble burst
Nodes
Risk influence
High
Medium
Low
Edges
Relative influence
High
Medium
Low
Risk categories
Economic
Environmental
Geopolitical
Societal
Technological
MITRE

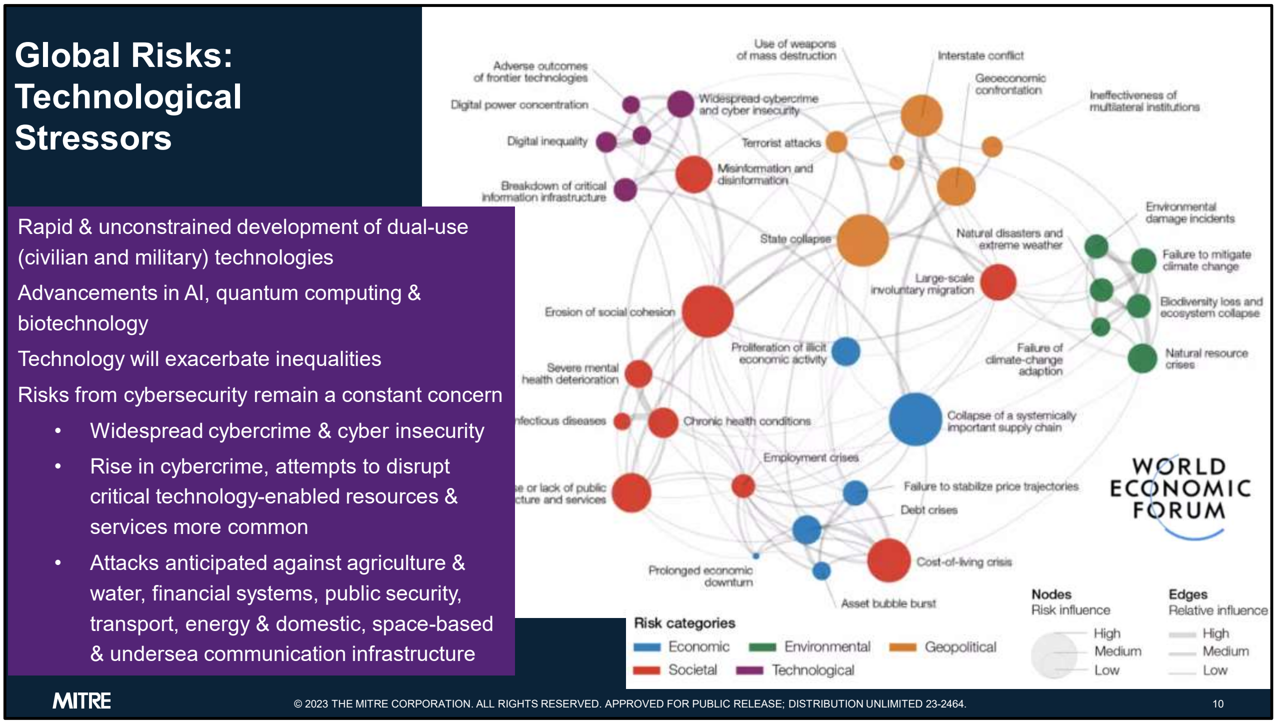
Reference(s):

- 2023 Outlook: 5 Finance Risks to Monitor This Year, CFO, https://www.cfo.com/risk-compliance/risk-management/2023/01/2023-risks-to-monitor-economy-inflation-labor-costs-engagement-interest-rates/, 23 January 2023.
- Global Risks Report 2023, World Economic Forum’s (WEF), https://www.weforum.org/reports/global-risks-report-2023/digest, 11 January 2023.
- China Signals More Tax Relief as Li Says GDP Goal Won’t be Easy – Bloomberg, https://www.bloomberg.com/news/articles/2022-03-11/china-s-premier-li-says-economic-growth-target-won-t-be-easy?cmpid=BBD012123_NEF&utm_medium=email&utm_source=newsletter&utm_term=230121&utm_campaign=nef&leadSource=uverify%20wall , 10 March 2022.
- China’s Property Woes Drive Household Savings to Record High, https://www.bloomberg.com/news/articles/2022-11-14/china-s-property-woes-drive-household-savings-to-record-high?leadSource=uverify wall, 23 January 2023.

Note(s):

- China
  - Higher than expected precautionary savings
    - Resulting from lockdown period (~25%)
    - Drop in property purchases

- Consumers resume spending in force - Forecasts
  - Increases in imports, domestic and foreign investment, overall consumption
  - Expected to push up commodity prices
- Increased foreign travel
- Government set~ 5.5% GDP goal 2023 – Li (Bloomberg)
- Tax and fee cuts
- Inflationary pressures abroad (e.g., energy and real estate demand growth)



## Global Risks: Technological Stressors

Rapid & unconstrained development of dual-use (civilian and military) technologies

Advancements in AI, quantum computing & biotechnology

Technology will exacerbate inequalities

Risks from cybersecurity remain a constant concern

- Widespread cybercrime & cyber insecurity
- Rise in cybercrime, attempts to disrupt critical technology-enabled resources & services more common
- Attacks anticipated against agriculture & water, financial systems, public security, transport, energy & domestic, space-based & undersea communication infrastructure

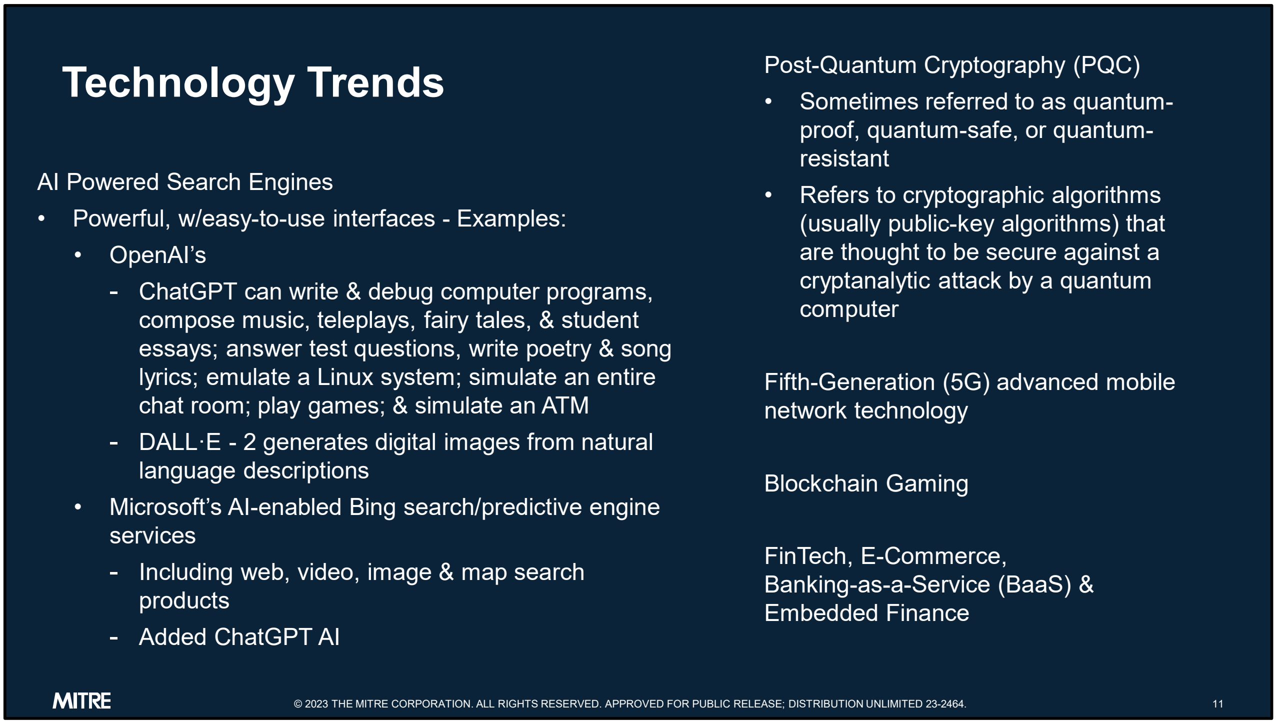
Use of weapons of mass destruction
Interstate conflict
Adverse outcomes of frontier technologies
Geoeconomic confrontation
Ineffectiveness of multilateral institutions
Digital power concentration
Widespread cybercrime and cyber insecurity
Digital inequality
Terrorist attacks
Breakdown of critical information infrastructure
Misinformation and disinformation
Environmental damage incidents
State collapse
Natural disasters and extreme weather
Failure to mitigate climate change
Large-scale involuntary migration
Biodiversity loss and ecosystem collapse
Erosion of social cohesion
Proliferation of illicit economic activity
Natural resource crises
Failure of climate-change adaption
Severe mental health deterioration
Collapse of a systemically important supply chain
nfectious diseases
Chronic health conditions
Employment crises
WORLD ECONOMIC FORUM
e or lack of public cture and services
Failure to stabilize price trajectories
Debt crises
Cost-of-living crisis
Prolonged economic downturn
Asset bubble burst
Nodes
Risk influence
Edges
Relative influence
Risk categories
High
Medium
Low
High
Medium
Low
Economic
Environmental
Geopolitical
Societal
Technological

Reference(s):

- Global Risks Report 2023, World Economic Forum’s (WEF), https://www.weforum.org/reports/global-risks-report-2023/digest, 11 January 23.
- Security Magazine, there are over 2,200 attacks each day which breaks down to nearly 1 cyberattack every 39 seconds, https://www.google.com/search?q=Cybercrime+every+39+seconds&source=hp&ei=iDa9ZJGZCvmj5NoP29CwoAk&iflsig=AD69kcEAAAAAZL1EmAoAIeXGxxxvUdUk7TNflfPiV3gU&ved=0ahUKEwiR_dzKgqWAAxX5EVkFHVsoDJQQ4dUDCAs&uact=5&oq=Cybercrime+every+39+seconds&gs_lp=Egdnd3Mtd2l6IhtDeWJlcmNyaW1lIGV2ZXJ5IDM5IHNlY29uZHNI5QRQAFgAcAB4AJABAJgBAKABAKoBALgBA8gBAPgBAvgBAQ&sclient=gws-wiz, 27 December 2022.

Note(s):

- According to Security Magazine, there are over 2,200 attacks each day which breaks down to nearly 1 cyberattack every 39 seconds



## Technology Trends

AI Powered Search Engines

- Powerful, w/easy-to-use interfaces - Examples:
  - OpenAI’s
    - ChatGPT can write & debug computer programs, compose music, teleplays, fairy tales, & student essays; answer test questions, write poetry & song lyrics; emulate a Linux system; simulate an entire chat room; play games; & simulate an ATM
    - DALL·E - 2 generates digital images from natural language descriptions
  - Microsoft’s AI-enabled Bing search/predictive engine services
    - Including web, video, image & map search products
    - Added ChatGPT AI

Post-Quantum Cryptography (PQC)

- Sometimes referred to as quantum-proof, quantum-safe, or quantum-resistant
- Refers to cryptographic algorithms (usually public-key algorithms) that are thought to be secure against a cryptanalytic attack by a quantum computer

Fifth-Generation (5G) advanced mobile network technology

Blockchain Gaming

FinTech, E-Commerce, Banking-as-a-Service (BaaS) & Embedded Finance

Reference(s):

- OpenAI’s ChatGPT, https://openai.com/blog/chatgpt/, Last accessed 13 February 2023.
  - ChatGPT, the chatbot released in late November 2022 by San Francisco 's OpenAI, reached the milestone in just 60 days. The viral growth came with a flurry of breathless journalism and Big Tech..., https://www.sfgate.com/tech/article/chatgpt-openai-everyday-guide-17777804.php –
  - Can write and debug computer programs,[13] compose music, teleplays, fairy tales, and student essays; answer test questions (sometimes, depending on the test, at a level above the average human test-taker);[14] write poetry and song lyrics;[15] emulate a Linux system; simulate an entire chat room; play games like tic-tac-toe; and simulate an ATM Limitations, e.g., "sometimes writes plausible-sounding but incorrect or nonsensical answers". This behavior is common to large language models and is called artificial intelligence hallucination,
- ChatGPT, Wikipedia, https://en.wikipedia.org/wiki/ChatGPT, Last accessed 13 February 2023.
  - ChatGPT (Chat Generative Pre-trained Transformer) is a chatbot developed by OpenAI and launched in November 2022. It is built on top of OpenAI's GPT-3 family of large language models and has been fine-tuned (an approach to transfer learning) using both supervised and reinforcement learning techniques.

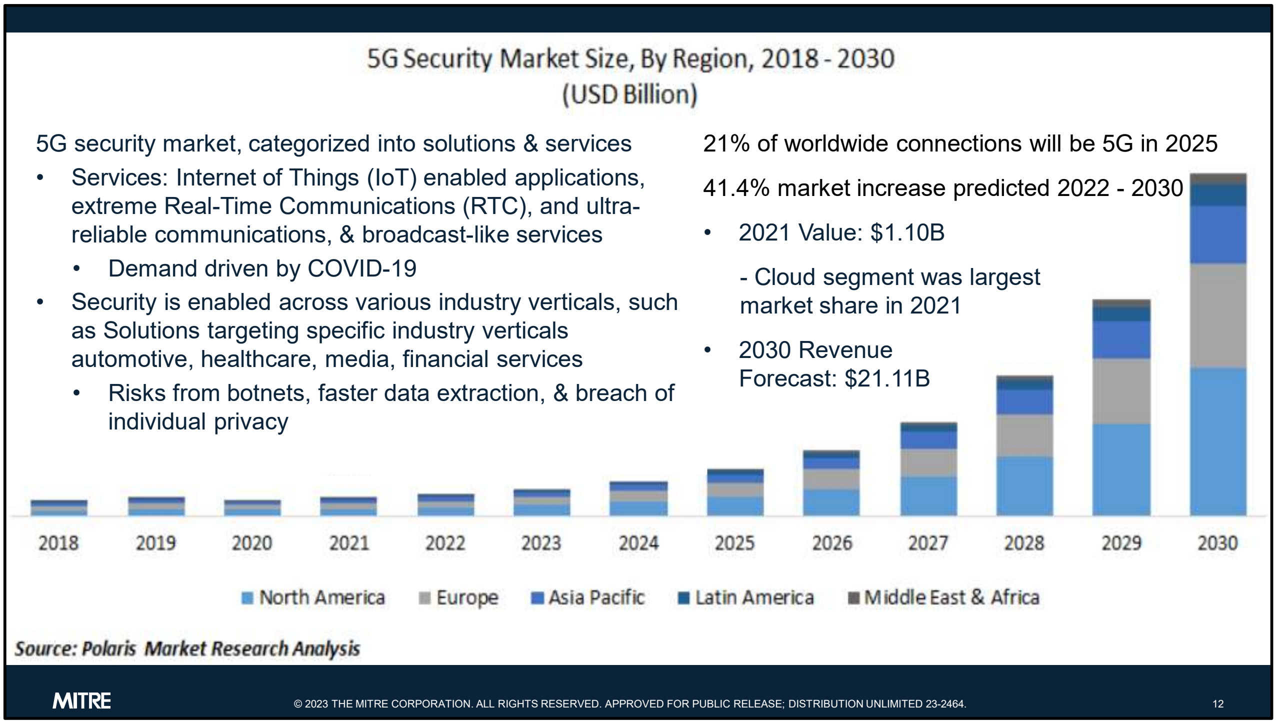
ChatGPT was launched as a prototype on November 30, 2022.

- DALL·E 2 Variations DALL·E 2 has learned the relationship between images and the text used to describe them. It uses a process called "diffusion," which starts with a pattern of random dots and gradually alters that pattern towards an image when it recognizes specific aspects of that image - DALL-E was revealed by OpenAI in a blog post in January 2021, and uses a version of GPT-3 modified to generate images. In April 2022, OpenAI announced DALL-E 2, a successor designed to generate more realistic images, DALL·E 2, https://openai.com/dall-e-2, Last accessed 13 February 2023.
- Microsoft's Bing, https://blogs.microsoft.com/blog/2023/02/07/reinventing-search-with-a-new-ai-powered-microsoft-bing-and-edge-your-copilot-for-the-web/, 7 February 2023.
    - France imposed a €60 million fine on Microsoft for privacy law violations using Bing cookies that prevented users rejecting those cookies (2022)
- AI Risk Management Framework (AI RMF) 1.0, https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf, Last accessed 13 February 2023.
- AI RMF Playbook 1.0, https://pages.nist.gov/AIRMF/, Last accessed 13 February 2023.
- Check Point Research (CPR) releases new data on 2022 cyberattack trends, DARKReading, https://www.darkreading.com/attacks-breaches/check-point-research-reports-a-38-increase-in-2022-global-cyberattacks#:~:text=Global%20cyberattacks%20increased%20by%2038,%2Dlearning%20post%20COVID%2D19, Last accessed 22 February 2023.
- Post-Quantum Cryptography (PQC), https://csrc.nist.gov/projects/post-quantum-cryptography & https://en.wikipedia.org/wiki/Post-quantum_cryptography, Last accessed 13 February 2023.

Note(s):

- AI Powered Search Engines – Powerful, with easy-to-use interfaces
    - OpenAI's
        - ChatGPT (Chat Generative Pre-trained Transformer) can write and debug computer programs, compose music, teleplays, fairy tales, and student essays; answer test questions,] write poetry and song lyrics;[ emulate a Linux system; simulate an entire chat room; play games like tic-tac-toe; and simulate an ATM (prototype 30 November 22)
        - DALL·E 2 generates digital images from natural language descriptions, called "prompts“ (April 22)
    - Microsoft's AI-enabled Bing search/predictive engine services, including web, video, image and map search products
        - Added ChatGPT AI to the search engine (7 February 23)
        - Delivers substantially different results for different parts of the world
    - ChatGPT bug exposed user data including chat history payment
        - Exposed March 2023
        - Open source library vulnerability - OpenAI has patched
- Must
    - Understand the limitations and risks of AI
    - Develop the frameworks and tools to create trustworthiness, mitigate risks, and

defend against malicious threats
    - Monitor use by attackers
        - “Maturity of AI technology, such as CHATGPT, can accelerate the number of cyberattacks in 2023” (DARKReading)
        - Allow attackers to generate malicious code and emails at a faster, more automated pace
- NIST
    - AI Risk Management Framework (AI RMF) 1.0 (26 January 23)
        - “The AI RMF refers to an AI system as an engineered or machine-based system that can, for a given set of objectives, generate outputs such as predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy (Adapted from: Organisation for Economic Co-operation and Development (OECD) Recommendation on AI:2019; ISO/IEC 22989:2022)”
    - AI RMF Playbook 1.0 (February 23)
    - Cyber Security Framework (CSF) 2.0 update in 2024
    - NIST draft standards 2023 & first standards to be published 2024 for PQC



5G Security Market Size, By Region, 2018 - 2030 (USD Billion)

5G security market, categorized into solutions & services

- Services: Internet of Things (IoT) enabled applications, extreme Real-Time Communications (RTC), and ultra-reliable communications, & broadcast-like services
  - Demand driven by COVID-19
- Security is enabled across various industry verticals, such as Solutions targeting specific industry verticals automotive, healthcare, media, financial services
  - Risks from botnets, faster data extraction, & breach of individual privacy

21% of worldwide connections will be 5G in 2025

41.4% market increase predicted 2022 - 2030

- 2021 Value: $1.10B

  - Cloud segment was largest market share in 2021
- 2030 Revenue Forecast: $21.11B

*Source: Polaris Market Research Analysis*

MITRE

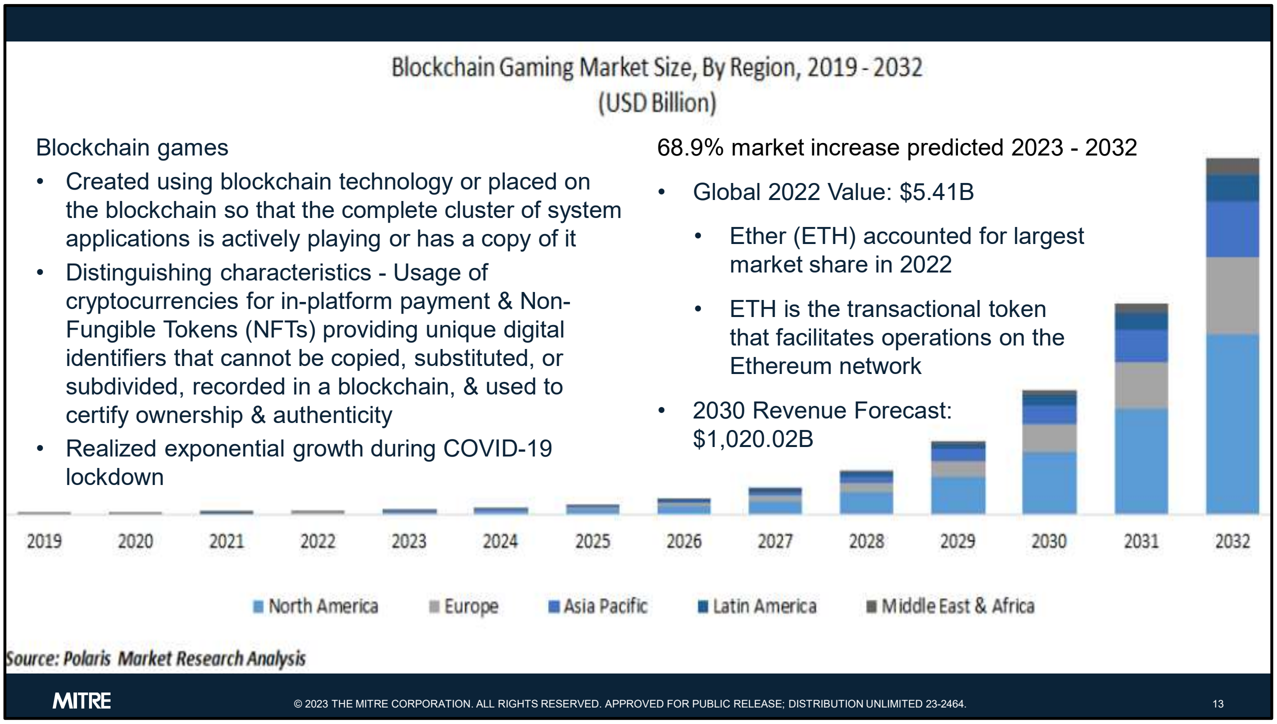
12

Reference(s):

- 5G Health Risks; The War Between Technology and Human Beings, Gaia, Paul Wagner, https://www.gaia.com/article/5g-health-risks-the-war-between-technology-and-human-beings?utm_platcamp=performancemax-acq+rmk-intl+usa-ancientcivilizations, 14 May 2019.
- Global: Forecasted 5G penetration rate 2025 by region, Published by Petroc Taylor, © Statista 2023, https://www.statista.com/statistics/1229971/5g-adoption-rate-forecast-by-region/, 19 January 2023.
- 5G Security Market Size Global Report, 2022 – 2030, Polaris Market Research, https://www.polarismarketresearch.com/industry-analysis/5g-security-market, July 2022.

Note(s):

- Fifth-Generation (5G) advanced mobile network technology
  - 100 times higher speed than 4G
  - Enables more devices to connect to mobile networks
  - Provides much lower network latencies & requires less energy than 4G - useful for resource-constrained devices
  - Public health risks from global electromagnetic radiation – Concerns have not been substantiated



Blockchain games

- Created using blockchain technology or placed on the blockchain so that the complete cluster of system applications is actively playing or has a copy of it
- Distinguishing characteristics - Usage of cryptocurrencies for in-platform payment & Non-Fungible Tokens (NFTs) providing unique digital identifiers that cannot be copied, substituted, or subdivided, recorded in a blockchain, & used to certify ownership & authenticity
- Realized exponential growth during COVID-19 lockdown

68.9% market increase predicted 2023 - 2032

- Global 2022 Value: $5.41B
  - Ether (ETH) accounted for largest market share in 2022
  - ETH is the transactional token that facilitates operations on the Ethereum network
- 2030 Revenue Forecast: $1,020.02B

Source: Polaris Market Research Analysis

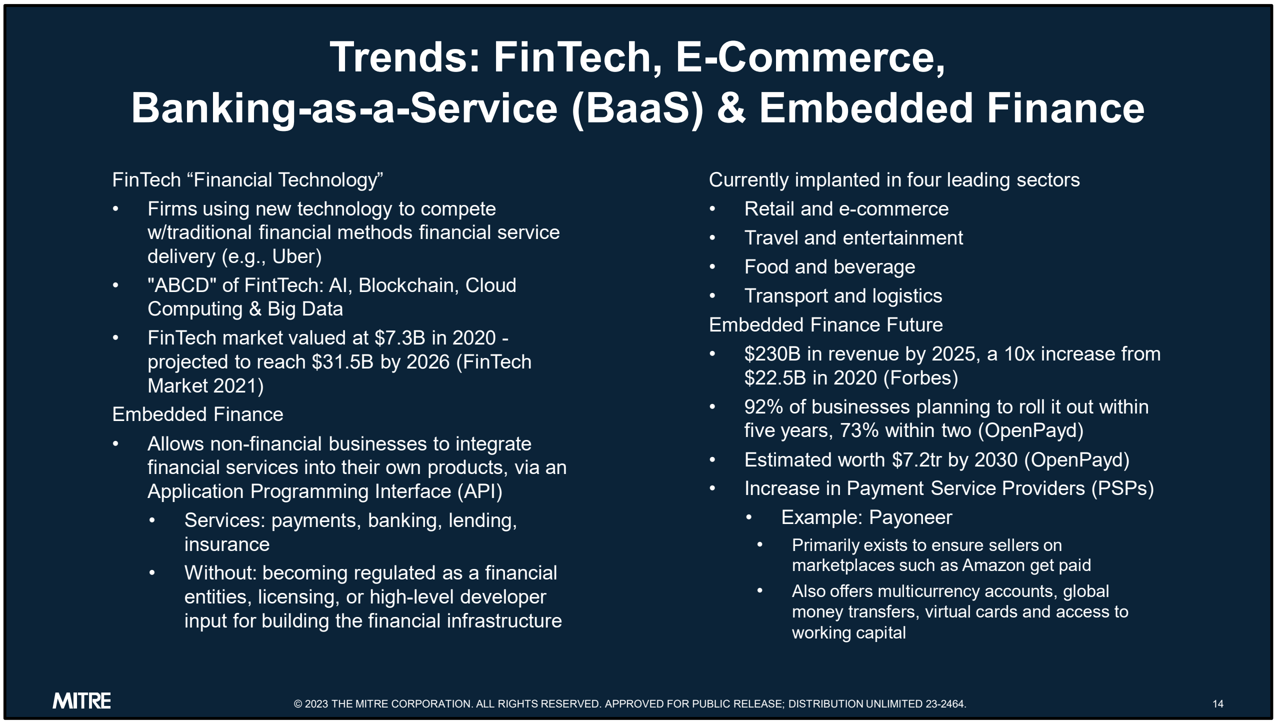
MITRE

Reference(s):

- Blockchain Gaming Market Share, Size, Trends, Industry Analysis Report, By Game Type (Collectible Games, Role Playing Games, Open World Games); By Platform; By Region; Segment Forecast, 2023 - 2032, Polaris Market Research, https://www.polarismarketresearch.com/industry-analysis/blockchain-gaming-market, February 2023.

Note(s):

- 68.9% expected growth at a CAGR of during the forecast period.
- Blockchain games are games created using blockchain technology or placed on the blockchain so that the complete cluster of system applications is actively playing or has a copy of it. The usage of cryptocurrencies for in-platform payment transactions and the use of NFTs are two characteristics that distinguish blockchain games.



# Trends: FinTech, E-Commerce, Banking-as-a-Service (BaaS) & Embedded Finance

FinTech “Financial Technology”

- Firms using new technology to compete w/traditional financial methods financial service delivery (e.g., Uber)
- "ABCD" of FintTech: AI, Blockchain, Cloud Computing & Big Data
- FinTech market valued at $7.3B in 2020 - projected to reach $31.5B by 2026 (FinTech Market 2021)

Embedded Finance

- Allows non-financial businesses to integrate financial services into their own products, via an Application Programming Interface (API)
  - Services: payments, banking, lending, insurance
  - Without: becoming regulated as a financial entities, licensing, or high-level developer input for building the financial infrastructure

Currently implanted in four leading sectors

- Retail and e-commerce
- Travel and entertainment
- Food and beverage
- Transport and logistics

Embedded Finance Future

- $230B in revenue by 2025, a 10x increase from $22.5B in 2020 (Forbes)
- 92% of businesses planning to roll it out within five years, 73% within two (OpenPayd)
- Estimated worth $7.2tr by 2030 (OpenPayd)
- Increase in Payment Service Providers (PSPs)
  - Example: Payoneer
    - Primarily exists to ensure sellers on marketplaces such as Amazon get paid
    - Also offers multicurrency accounts, global money transfers, virtual cards and access to working capital

MITRE

Reference(s):

- What-is-embedded-finance, https://www.openpayd.com/uk/blog/what-is-embedded-finance, Last accessed 21 February 2023.
- Whitepaper: The rise of embedded finance, https://www.openpayd.com/uk/blog/whitepaper-the-rise-of-embedded-finance, posted on 17 January 2022.
- Everything you need to know about PSD2, BBVA, regulation began 13 January 18, https://www.bbva.com/en/everything-need-know-psd2/, Last accessed 21 February 2023.
- Payment Services Directive 2 – an overview, J.P.Morgan, https://www.jpmorgan.com/europe/merchant-services/insights/PSD2-all-you-need-to-know, Last accessed 21 February 2023.
- Embedded Finance Research Report, OpenPayd, https://www.openpayd.com/uk/blog/whitepaper-the-rise-of-embedded-finance, (Embedded_Finance_Research_Report_single_pages.pdf), Report Issued: September 2021.
- Three Key Trends In Embedded Finance, Forbes, https://www.forbes.com/sites/forbesfinancecouncil/2022/01/06/three-key-trends-in-embedded-finance/?sh=67f16d881df7, 6 January 2022.
- Embedded Fintech Versus Embedded Finance: Jumpstarting New Product Innovation In

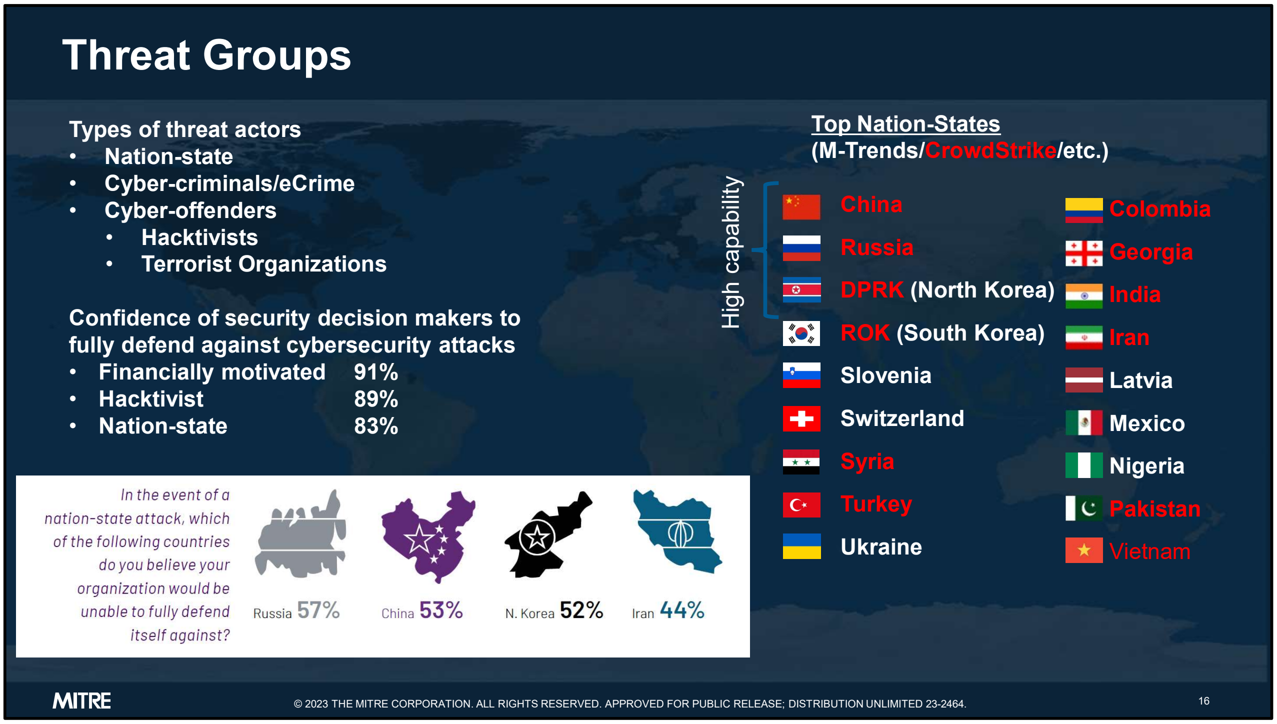
Banks, Forbes, https://www.forbes.com/sites/ronshevlin/2021/04/12/embedded-fintech-versus-embedded-finance-jumpstarting-new-product-innovation-in-banks/?sh=789e0b825892, 12 April 2021.

- All you need to know about Risk management in Fintech, Morgan McKinley, https://www.morganmckinley.com/sg/article/all-you-need-know-about-risk-management-fintech, 4 November 2021.
- Top 5 Biggest Risks Faced by Fintech Firms, 360factors$^{TM}$, Posted by: Sarah Hamilton, https://www.360factors.com/blog/top5-biggest-risks-faced-fintech-firms/, 10 May 2022.

Note(s)

- FinTech, E-Commerce, Banking-as-a-Service (BaaS) & Embedded Finance Risks:
    - Personal and Professional Liability/Merchant & Consumer Risks
        - Carelessness, service failures, fraud & fraud claims
        - Anti-money laundering and countering terrorist financing
    - Credit and Operational Risks
        - FinTech most vulnerable in real-time operations management, in which 99% of the most significant errors occur (360factors$^{TM}$)
        - Merchants overrun their operational capacity and cannot standardize new operational procedures
    - Data Thefts and Cyber Attacks
        - More systems linked by fintech, the more possible incursions for cyber assaults to exploit
        - Cybersecurity and Data Privacy
    - Outsourcing Risk
    - Unexpected Market Occurrences
        - GameStop Market Disruption
    - Increased Global Rivalry
    - Noncompliance with Regulatory Requirements
        - Need for new licensing models with new controls and processes

# Threat Actors & Attack Vectors



## Threat Groups

Types of threat actors

- Nation-state
- Cyber-criminals/eCrime
- Cyber-offenders
  - Hacktivists
  - Terrorist Organizations

Confidence of security decision makers to fully defend against cybersecurity attacks

- Financially motivated 91%
- Hacktivist 89%
- Nation-state 83%

*In the event of a nation-state attack, which of the following countries do you believe your organization would be unable to fully defend itself against?*

Russia 57% China 53% N. Korea 52% Iran 44%

Top Nation-States
(M-Trends/CrowdStrike/etc.)

High capability

- China
- Russia
- DPRK (North Korea)
- ROK (South Korea)
- Slovenia
- Switzerland
- Syria
- Turkey
- Ukraine
- Colombia
- Georgia
- India
- Iran
- Latvia
- Mexico
- Nigeria
- Pakistan
- Vietnam

MITRE

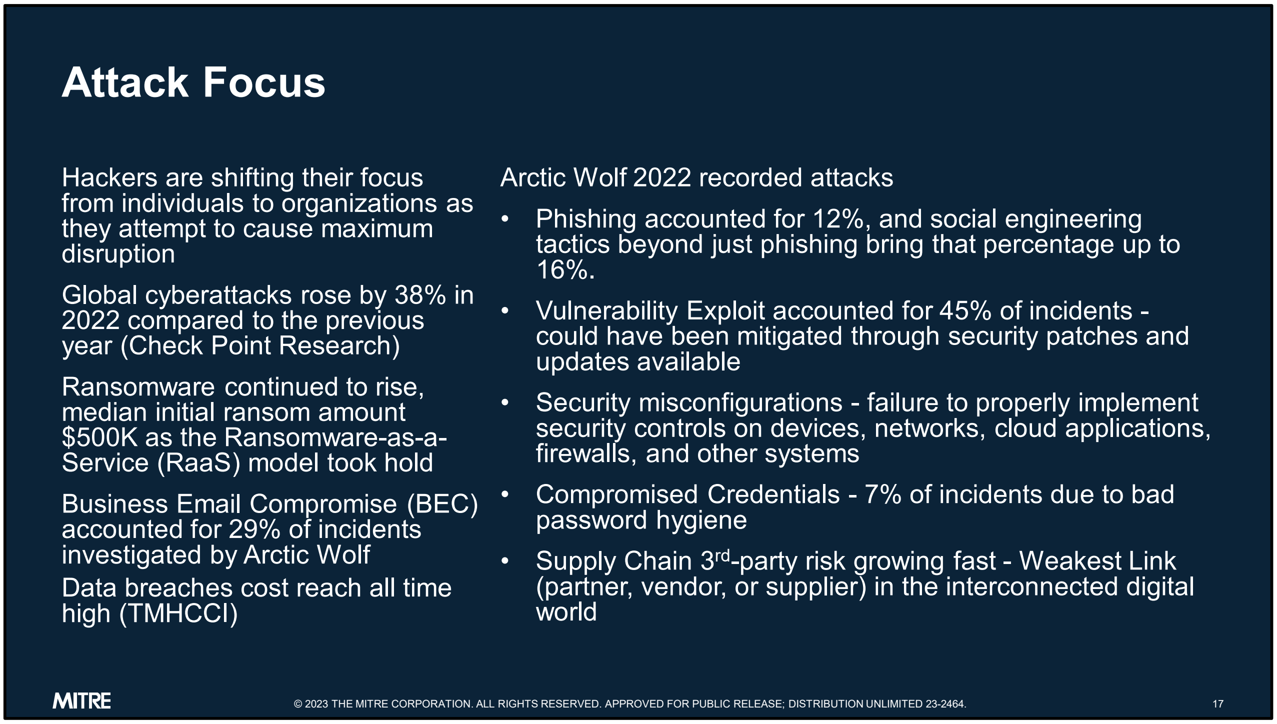
Reference(s):

- Mandiant, M-Trends 2022, Special Report, https://www.mandiant.com/resources/m-trends-2022, 19 April 2022.
- 2023 Global Threat Report, CrowdStrike, CrowdStrike2023GlobalThreatReport.pdf, https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrike2023GlobalThreatReport.pdf, 28 February 2023.
- Global Perspectives on Threat Intelligence, Mandiant now part of Google, Global-Perspectives-on-Threat-Intelligence-2-08-23.pdf, https://www.mandiant.com/global-perspectives-on-threat-intelligence, 8 February 2023.
- North Korean hackers target security researchers with a new backdoor, Campaign uses carefully crafted LinkedIn accounts that mimic legit people, Dan Goodin, https://arstechnica.com/information-technology/2023/03/security-researchers-are-again-in-the-crosshairs-of-north-korean-hackers/, 10 March 2023.
- Flag icons, https://flagpedia.net/index, Last accessed 19 July 2023.

Note(s):

- Understanding the types help ID and respond
  - Many actors have “signatures” – How they attack and what methods they use, as well as level of sophistication
- Types of actors/Perpetrators

  - Nation-state – primary motivation: espionage
  - Cyber-criminals – primary motivation: financial
    - Organized cyber-criminal groups behind 55% of breaches (Verizon 2020 DBIR)
  - Cyber-offenders – primary motivation: personal causes
    - Hacktivists
    - Terrorist Organizations
- There are other ways to group threat actors
  - FireEye threat groups
    - FireEye clients encountered activity from a wide range of established threat groups, as well as hundreds of new threat groups that emerged in the last.
    - Six of 10 named financial threat groups (FIN)
    - 17 named APT groups (44% of all known APT groups) from six different countries were active.
    - These named groups were joined by 159 other groups in intrusion attempts against clients.
  - FireEye, blog explains some internal processes for organizing their attacker observations in early stages
    - They group activity into “uncategorized” (UNC) groups and “temporary” (TEMP) groups until/unless they have sufficient intelligence to tie them to a known cyberespionage group (APT) or financial crime group (FIN), or alternatively create an entirely new APT group
- Targeting cybersecurity professionals.
  - The North Korean government also tried to gain inside information by trying to gain the trust of security experts around the world through elaborate fake personas. In January 2021, it was discovered that an army of supposed security experts were just fake accounts created by a malicious actor. The purpose of these accounts was to gain the trust of real security experts. This was done through careful, calculated conversations that could trick any expert. Once trust was gained, the fake persona would ask the experts to check out a website. … the websites contained exploits that would give the malicious actor access to the researcher’s machine. This is especially dangerous because researchers’ computers are likely to contain cybersecurity research that could teach the hacker how these experts make the locks used to block malware. With this information, they would be able to create ways to break those safeguards.



## Attack Focus

Hackers are shifting their focus from individuals to organizations as they attempt to cause maximum disruption

Global cyberattacks rose by 38% in 2022 compared to the previous year (Check Point Research)

Ransomware continued to rise, median initial ransom amount $500K as the Ransomware-as-a-Service (RaaS) model took hold

Business Email Compromise (BEC) accounted for 29% of incidents investigated by Arctic Wolf

Data breaches cost reach all time high (TMHCCI)

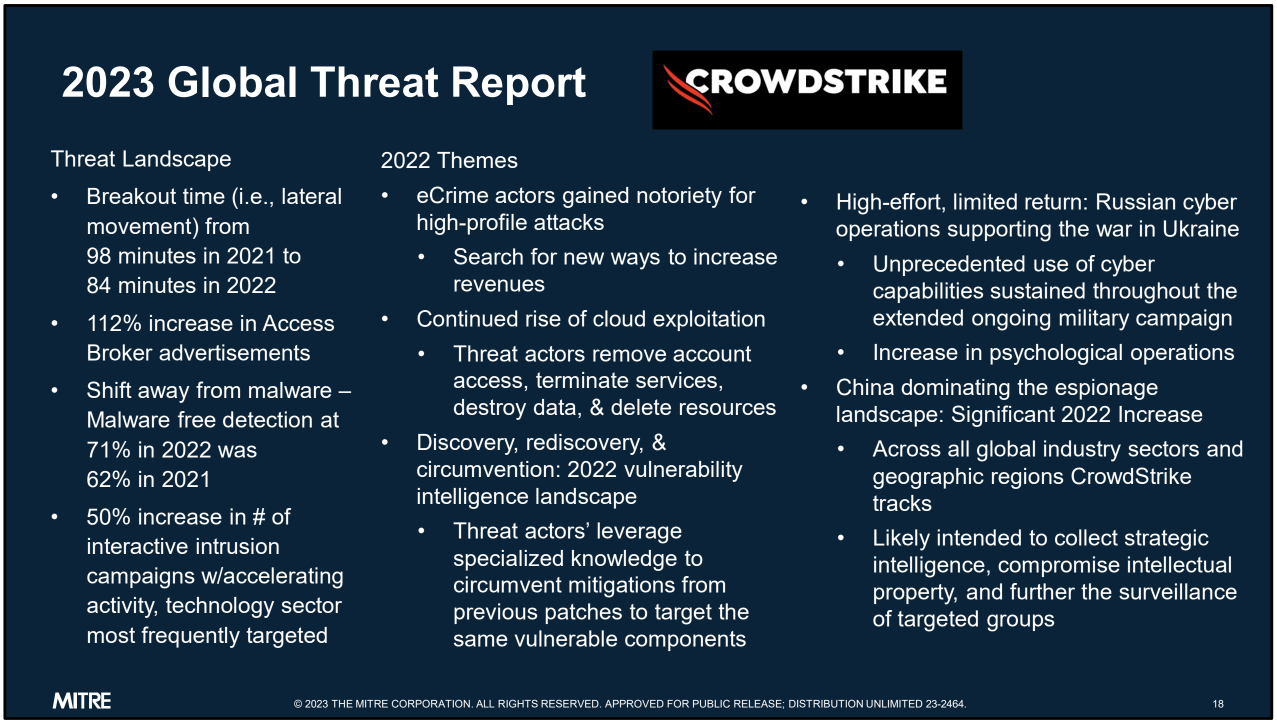
Arctic Wolf 2022 recorded attacks

- Phishing accounted for 12%, and social engineering tactics beyond just phishing bring that percentage up to 16%.
- Vulnerability Exploit accounted for 45% of incidents - could have been mitigated through security patches and updates available
- Security misconfigurations - failure to properly implement security controls on devices, networks, cloud applications, firewalls, and other systems
- Compromised Credentials - 7% of incidents due to bad password hygiene
- Supply Chain 3rd-party risk growing fast - Weakest Link (partner, vendor, or supplier) in the interconnected digital world

MITRE

Reference(s):

- Threat of multiple attack vectors ‘looms large’ in 2023, Staff Writer, TradeArabia, https://www.zawya.com/en/business/technology-and-telecom/threat-of-multiple-attack-vectors-looms-large-in-2023-usgvam4d, 25 April 2023.
- Recent Data Breaches – 2023, Michael X. Heiligenstein, Firewall Times, https://firewalltimes.com/recent-data-breaches/, 17 May 2023.
- The Top 5 Cyber Attack Vectors, Arctic Wolf, https://arcticwolf.com/resources/blog/top-five-cyberattack-vectors/, 26 May 2023.
    - Security misconfigurations example is a Remote Desktop Protocol (RDP) that functions properly but still has the initial admin username and password.



## 2023 Global Threat Report

CROWDSTRIKE

Threat Landscape

- Breakout time (i.e., lateral movement) from 98 minutes in 2021 to 84 minutes in 2022
- 112% increase in Access Broker advertisements
- Shift away from malware – Malware free detection at 71% in 2022 was 62% in 2021
- 50% increase in # of interactive intrusion campaigns w/accelerating activity, technology sector most frequently targeted

2022 Themes

- eCrime actors gained notoriety for high-profile attacks
  - Search for new ways to increase revenues
- Continued rise of cloud exploitation
  - Threat actors remove account access, terminate services, destroy data, & delete resources
- Discovery, rediscovery, & circumvention: 2022 vulnerability intelligence landscape
  - Threat actors' leverage specialized knowledge to circumvent mitigations from previous patches to target the same vulnerable components
- High-effort, limited return: Russian cyber operations supporting the war in Ukraine
  - Unprecedented use of cyber capabilities sustained throughout the extended ongoing military campaign
  - Increase in psychological operations
- China dominating the espionage landscape: Significant 2022 Increase
  - Across all global industry sectors and geographic regions CrowdStrike tracks
  - Likely intended to collect strategic intelligence, compromise intellectual property, and further the surveillance of targeted groups

MITRE

18

Reference(s):

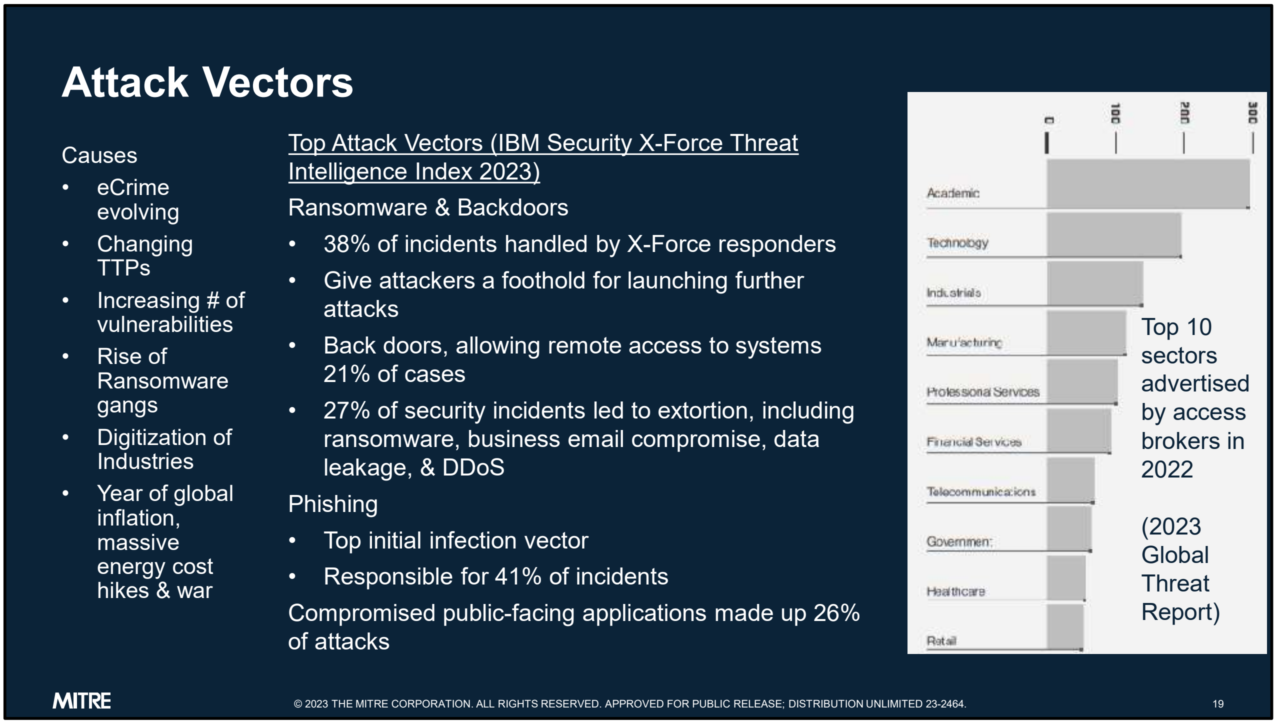
- 2023 Global Threat Report, CrowdStrike, CrowdStrike2023GlobalThreatReport.pdf, https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrike2023GlobalThreatReport.pdf, 28 February 2023.

Note(s):

- Vulnerability exploitation faster than ever
  - Zero-day (attack relies on an undisclosed vulnerability) & N-day (# of days since patch released) vulnerabilities demonstrated threat actors' ability to leverage specialized knowledge to circumvent mitigations from previous patches to target the same vulnerable components
  - Log4Shell exploitation continues
- How a new, emerging class of eCrime threat actors is using fileless attacks to target high-profile organizations with devastating campaigns
- eCrime Breakout Time: 84 minutes
  - Time an adversary takes to move laterally, from initially compromised host to another host within the victim environment
- Why identity protection continues to be a core requirement for risk mitigation as adversaries ramp up attacks on multi-factor authentication
- Why adversaries are accelerating cloud exploitation and the tactics they're using to

compromise cloud infrastructure

- How adversaries have created a new “state of the art” for vulnerability exploitation to sidestep patches and why the industry needs to demand more secure software
- Access brokers are threat actors who acquire access to organizations and provide or sell this access to other actors, including ransomware operators



## Attack Vectors

Causes

- eCrime evolving
- Changing TTPs
- Increasing # of vulnerabilities
- Rise of Ransomware gangs
- Digitization of Industries
- Year of global inflation, massive energy cost hikes & war

Top Attack Vectors (IBM Security X-Force Threat Intelligence Index 2023)

Ransomware & Backdoors

- 38% of incidents handled by X-Force responders
- Give attackers a foothold for launching further attacks
- Back doors, allowing remote access to systems 21% of cases
- 27% of security incidents led to extortion, including ransomware, business email compromise, data leakage, & DDoS

Phishing

- Top initial infection vector
- Responsible for 41% of incidents

Compromised public-facing applications made up 26% of attacks

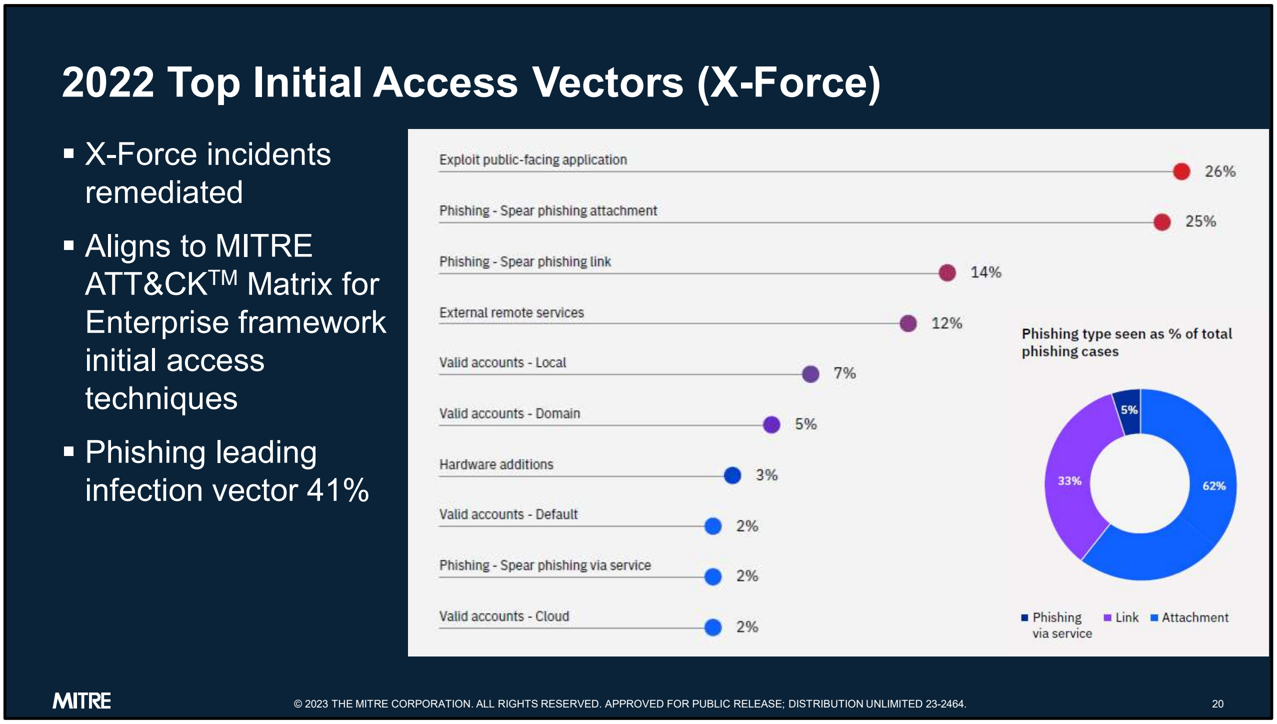
Top 10 sectors advertised by access brokers in 2022

(2023 Global Threat Report)

MITRE

Reference(s):

- Threat of multiple attack vectors ‘looms large’ in 2023, Staff Writer, TradeArabia, https://www.zawya.com/en/business/technology-and-telecom/threat-of-multiple-attack-vectors-looms-large-in-2023-usgvam4d, 25 April 2023.
- IBM Security X-Force Threat Intelligence Index 2023, https://www.ibm.com/reports/threat-intelligence?utm_id=SI-Blog-Inline-XFTII-2023, March 2023.
- 2023 Global Threat Report, CrowdStrike, CrowdStrike2023GlobalThreatReport.pdf, https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrike2023GlobalThreatReport.pdf, 28 February 2023.
- Top 10 Cyber Incidents 2022, Tokio Marine HCC International’s (TMHCCI), Isaac Guasch, https://issuu.com/tmhcci/docs/tmhcc_top_10_cyber_incidents_2022/1, 31 January 2023.
- Recent Data Breaches – 2023, Michael X. Heiligenstein, Firewall Times, https://firewalltimes.com/recent-data-breaches/, 17 May 2023.



## 2022 Top Initial Access Vectors (X-Force)

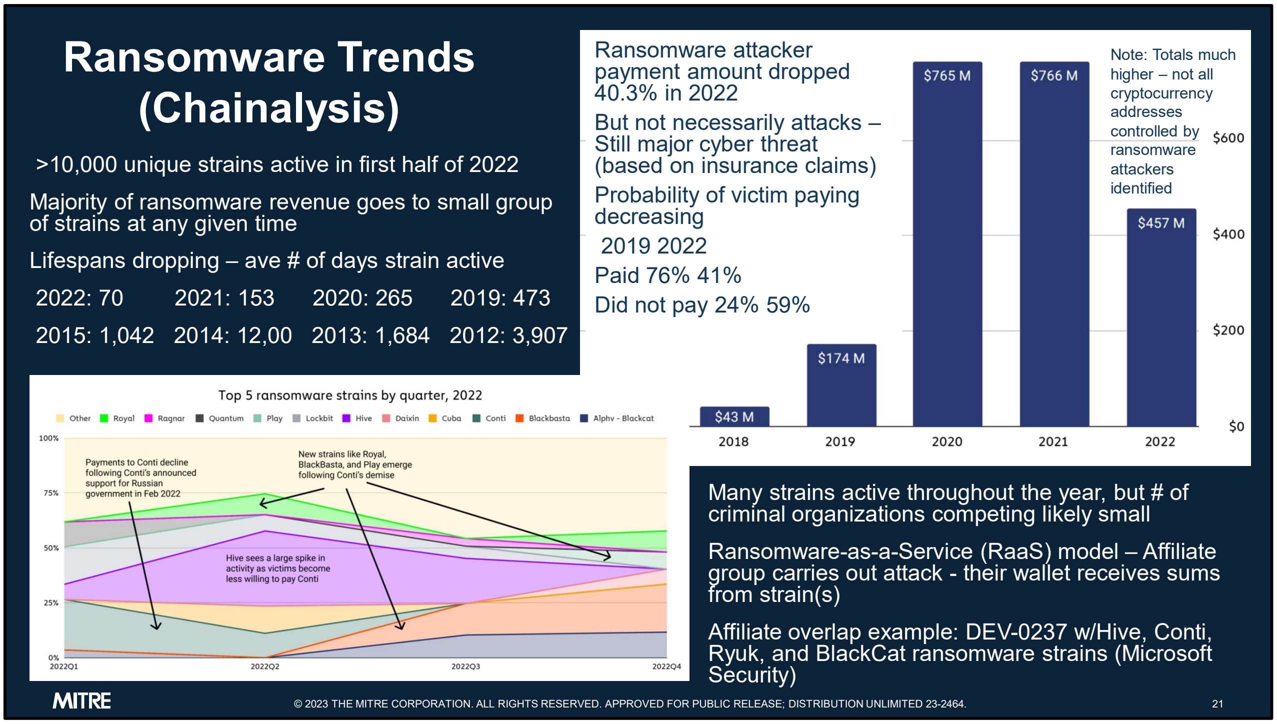
- X-Force incidents remediated
- Aligns to MITRE ATT&CK$^{TM}$ Matrix for Enterprise framework initial access techniques
- Phishing leading infection vector 41%

MITRE

20

Reference(s):

- X-Force Threat Intelligence Index 2023, IBM Security, https://www.ibm.com/downloads/cas/DB4GL8YM, February 2023.



## Ransomware Trends (Chainalysis)

>10,000 unique strains active in first half of 2022

Majority of ransomware revenue goes to small group of strains at any given time

Lifespans dropping – ave # of days strain active

| | | | |
|---|---|---|---|
| 2022: 70 | 2021: 153 | 2020: 265 | 2019: 473 |
| 2015: 1,042 | 2014: 12,00 | 2013: 1,684 | 2012: 3,907 |

Ransomware attacker payment amount dropped 40.3% in 2022

But not necessarily attacks – Still major cyber threat (based on insurance claims)

Probability of victim paying decreasing

| | 2019 | 2022 |
|---|---|---|
| Paid | 76% | 41% |
| Did not pay | 24% | 59% |

Note: Totals much higher – not all cryptocurrency addresses controlled by ransomware attackers identified

Top 5 ransomware strains by quarter, 2022

Payments to Conti decline following Conti's announced support for Russian government in Feb 2022

New strains like Royal, BlackBasta, and Play emerge following Conti's demise

Hive sees a large spike in activity as victims become less willing to pay Conti

Many strains active throughout the year, but # of criminal organizations competing likely small

Ransomware-as-a-Service (RaaS) model – Affiliate group carries out attack - their wallet receives sums from strain(s)

Affiliate overlap example: DEV-0237 w/Hive, Conti, Ryuk, and BlackCat ransomware strains (Microsoft Security)

MITRE

Reference(s):

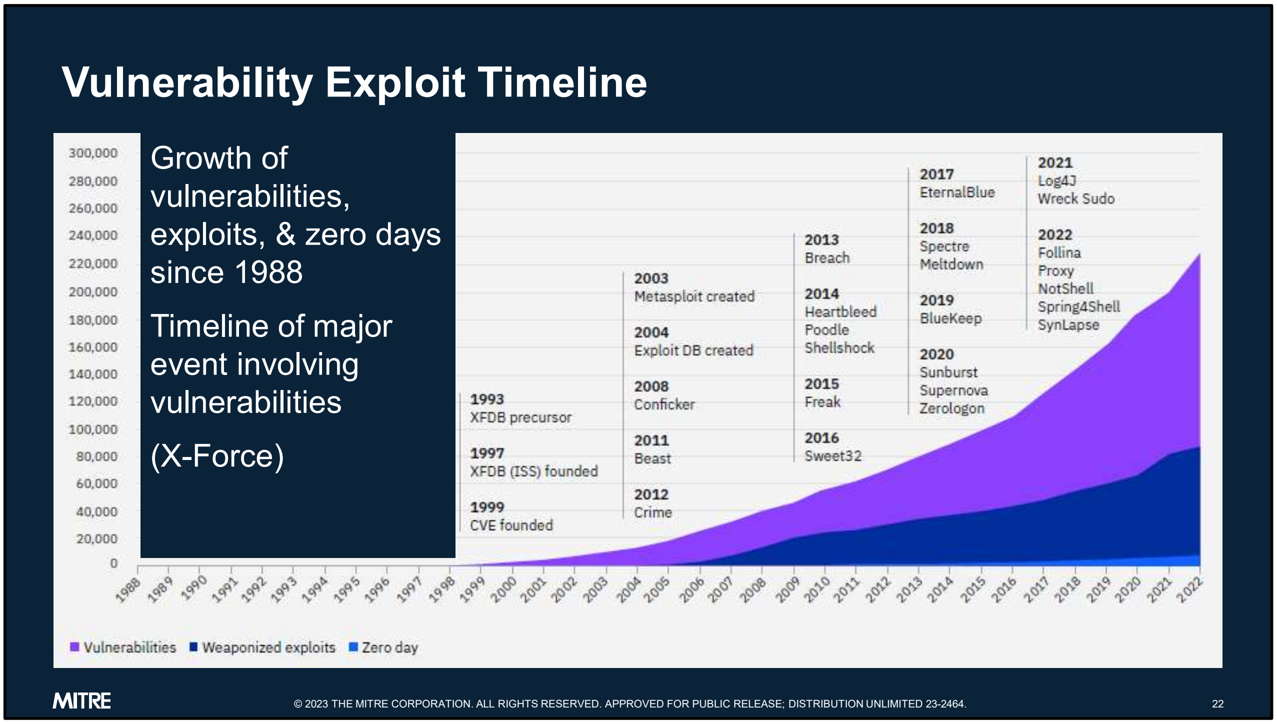
- Ransomware Revenue Down As More Victims Refuse to Pay, BY CHAINALYSIS TEAM, https://blog.chainalysis.com/reports/crypto-ransomware-revenue-down-as-victims-refuse-to-pay/, 19 January 2023.

Note(s):

- Microsoft Security discussed an example of this in a blog post earlier this year discussing one prolific affiliate group, whom they've labeled DEV-0237, who has carried out attacks using the Hive, Conti, Ryuk, and BlackCat ransomware strains. Microsoft Security researchers were able to identify this example of affiliate overlap by analyzing the technical details of how the attacks were carried out, but we can also identify examples of affiliate overlap on the blockchain. On the Chainalysis Reactor graph below, we see an affiliate whose wallet has received large sums from the Dharma, Conti, and BlackCat ransomware strains at different times, which means the affiliate has carried out attacks for all three strains.
- Conti is a particularly interesting case for observing how not just affiliates, but administrators as well rebrand themselves and switch between strains. Conti was a prolific ransomware strain for a few years, taking in more revenue than any other variant in 2021. But in February, immediately following Russia's invasion of Ukraine, the Conti team publicly announced its support for Vladimir Putin's government. Soon after, a

cache of Conti’s internal communications leaked, and indicated connections between the cybercrime organization and Russia’s Federal Security Service (FSB).

- For these reasons, many ransomware victims and incident response firms decided that paying Conti attackers was too risky, as the FSB is a sanctioned entity despite Conti itself not being one. Conti responded by announcing its closure in May, but soon after, much of the Conti team split up into smaller groups and continued their activity. Conti’s closure drove many affiliates to conduct attacks for other strains whose ransoms victims were more likely to pay, as we showed above. We can see another example of this activity below.



## Vulnerability Exploit Timeline

Growth of vulnerabilities, exploits, & zero days since 1988

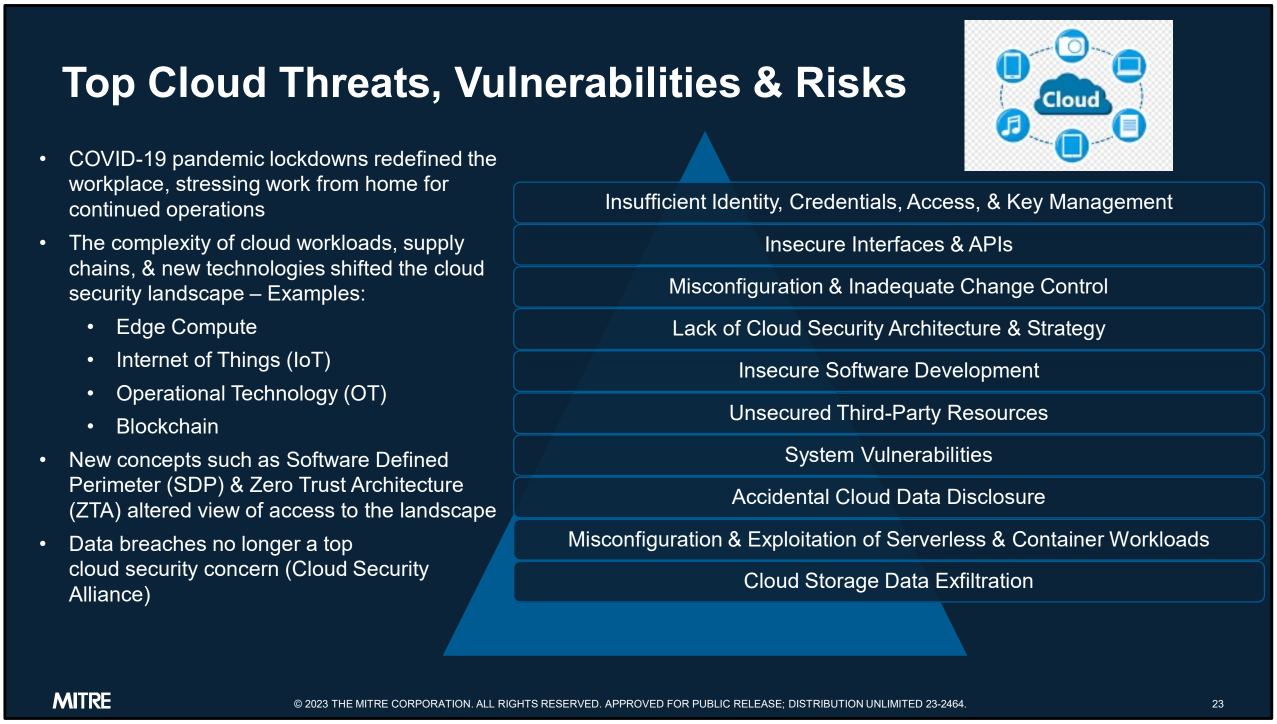
Timeline of major event involving vulnerabilities

(X-Force)

MITRE

Reference(s):

- X-Force Threat Intelligence Index 2023, IBM Security, https://www.ibm.com/downloads/cas/DB4GL8YM, February 2023.



## Top Cloud Threats, Vulnerabilities & Risks

- COVID-19 pandemic lockdowns redefined the workplace, stressing work from home for continued operations
- The complexity of cloud workloads, supply chains, & new technologies shifted the cloud security landscape – Examples:
  - Edge Compute
  - Internet of Things (IoT)
  - Operational Technology (OT)
  - Blockchain
- New concepts such as Software Defined Perimeter (SDP) & Zero Trust Architecture (ZTA) altered view of access to the landscape
- Data breaches no longer a top cloud security concern (Cloud Security Alliance)

Insufficient Identity, Credentials, Access, & Key Management

Insecure Interfaces & APIs

Misconfiguration & Inadequate Change Control

Lack of Cloud Security Architecture & Strategy

Insecure Software Development

Unsecured Third-Party Resources

System Vulnerabilities

Accidental Cloud Data Disclosure

Misconfiguration & Exploitation of Serverless & Container Workloads

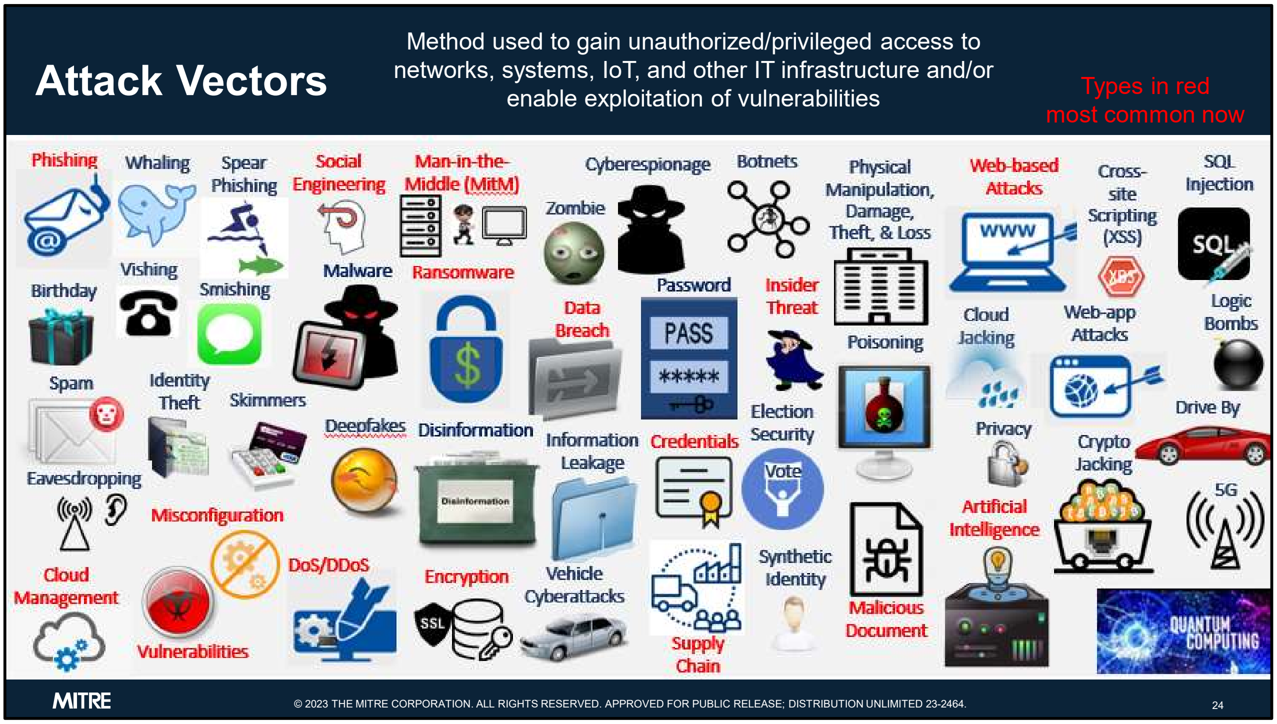
Cloud Storage Data Exfiltration

MITRE

23

Reference(s):

- 2022 “Top Threats to Cloud Computing - Pandemic Eleven” report, TopThreatstoCloudComputingPandemicEleven060622.pdf, https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-pandemic-eleven/, 4 November 2022.
  - Research conducted in two stages, surveying over 700 industry experts on security issues in the cloud industry - Gathered thoughts and opinions of cybersecurity professionals concerning the most relevant threats, vulnerabilities, and risks security issues) to cloud computing with the goal of identifying the Top Threats for 2022.
- Top Threats, Cloud Security Alliance (CSA), The permanent and official location for Cloud Security Alliance Top Threats research: https://cloudsecurityalliance.org/research/working-groups/top-threats/, Last accessed November 2022.
- Cloud icon, https://www.google.com/url?sa=i&url=https%3A%2F%2Fwww.pngwing.com%2Fen%2Ffree-png-nwepg&psig=AOvVaw2pNljPTp_mOUqrqE1Che-c&ust=1689954436844000&source=images&cd=vfe&opi=89978449&ved=0CAQQjB1qFwoTCJDKlorRnYADFQAAAAAdAAAAABAJ, Last accessed 20 July 2023.



## Attack Vectors

Method used to gain unauthorized/privileged access to networks, systems, IoT, and other IT infrastructure and/or enable exploitation of vulnerabilities

Types in red most common now

Phishing
Whaling
Spear Phishing
Social Engineering
Man-in-the-Middle (MitM)
Cyberespionage
Botnets
Physical Manipulation, Damage, Theft, & Loss
Web-based Attacks
Cross-site Scripting (XSS)
SQL Injection
Zombie
Birthday
Vishing
Smishing
Malware
Ransomware
Data Breach
Password
Insider Threat
Poisoning
Cloud Jacking
Web-app Attacks
Logic Bombs
Spam
Identity Theft
Skimmers
Deepfakes
Disinformation
Information Leakage
Credentials
Election Security
Vote
Privacy
Crypto Jacking
Drive By
Eavesdropping
Misconfiguration
Artificial Intelligence
5G
Cloud Management
Vulnerabilities
DoS/DDoS
Encryption
Vehicle Cyberattacks
Supply Chain
Synthetic Identity
Malicious Document

MITRE

© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED 23-2464.

24

Reference(s):

- The Top 5 Cyber Attack Vectors, Arctic Wolf, https://arcticwolf.com/resources/blog/top-five-cyberattack-vectors/, 26 May 2023.
- EXPEL BLOG Top Attack Vectors: January 2022, https://expel.com/blog/top-attack-vectors-january-2022/, Last accessed 7 June 2023
- Bad Guys, AARP Bulletin, http://www.owenfreeman.com/blog/2022/4/11/aarp-bad-guys, 11 April 2022.
- Icons, https://iconarchive.com/, Last accessed 20 July 2023.

Note(s):

- An attack vector is the way a threat actor gains access to a network, system, or endpoint. If ransomware is the kind of attack, the way the threat actor was able to deploy that ransomware would be the attack vector. An attack vector can also be called a root point of compromise, meaning the initial entry point method leveraged by a threat actor.
- Fraud against vets/military over doubled from 2021 to 2022 ($267m) #1 posers (govt/friend in need) #2 online shopping scams then #3 prize scams (FTC's annual "Consumer Sentinel Network" report, February 2023)
- An attack vector is a method used to gain unauthorized / privileged access to networks, systems, IoT, and other IT infrastructure. In other words, they enable hackers to exploit

vulnerabilities and can lead to security incidents (https://informer.io/resources/what-are-the-top-12-most-common-attack-vectors)

  - Attack surface refers to the sum of all possible attack vectors
  - Attack vectors are exploited to infiltrate a system, steal information, or disrupt service
- Types of threats
  - Sampling of emerging and existing cybersecurity threats based in part from Norton Cyberthreat trends: 15 cybersecurity threats for 2020 with others threaded throughout
  - 10 most common cyber attack types based on Netwrix Blog, Top 10 Most Common Types of Cyber Attacks, Jeff Melnick, Published: 15 May 2018, Updated: 8 October 2020
  - These themes are shared across the cybersecurity industry
- Types of Attacks
  - Malware - unwanted software installed in your system without consent, examples: viruses, trojans, worms, spyware, Ransomware
    - Ransomware – Get data back/expose data, sometimes auctioned off
      - Ransomware attacks on the public sector - In a ransomware attack, hackers access the computer systems of an end user, usually freezing them. These attackers will only unlock the infected systems if the victim pays a ransom. Hackers today often target the computer systems of government bodies, including municipalities, public utilities, and fire and police departments, hijacking their computer systems until these government agencies pay a ransom.
      - Through Spyware / Adware
      - “The top ransomware families seen in these attacks include FileCrypt/FileCoder variants, followed by Sodinokibi, Maze, and Ryuk family variants. A notable change in many of these ransomware family variants during the past year has been the addition of a data exfiltration feature. This new feature allows ransomware gangs to exfiltrate sensitive data from victims before encrypting the data. This exfiltrated data is like an insurance policy for attackers: even if the victim organization has good backups, they’ll pay the ransom to avoid having their data exposed.” (Zscaler ThreatLabZ)
    - Logic bombs - a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. For example, a programmer may hide a piece of code that starts deleting files, should they ever be terminated from the company
    - Emotet and TrickBot were the two most prevalent malware families seen in our analysis. (Zscaler ThreatLabZ) Trickbot is computer malware, a troJanuary for the Microsoft Windows and other operating systems. Its major function was originally the theft of banking details and

  other credentials, but its operators have extended its capabilities to create a complete modular malware ecosystem. (Wikipedia)

- Phishing involves a malicious actor impersonating a trustworthy entity to obtain private data. Such attacks can be carried out via emails, websites, or other means. Attackers can either trick victims into providing sensitive information — such as credit card information or passwords — or downloading malicious attachments
  - Emails that appear to be from trusted sources with the goal of gaining personal information or influencing users to do something
  - Spear phishing is a targeted type of phishing activity
  - Domain impersonation/spoofing using a company's domain to impersonate a company or one of its employees
- Email:
  - Spoofing is when someone disguises an email address, sender name, phone number, or website URL—often just by changing one letter, symbol, or number—to convince you that you are interacting with a legitimate entity
  - Spam
- Social Engineering is the psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme. (Wikipedia)
- Denial-of-Service (DoS) and distributed denial-of-service (DDoS) – DoD overwhelms a system’s resources so that it cannot respond to service requests, examples: Smurf attack, Ping of death attack – DDoS launched from a large number of other host machines that are infected by malicious software controlled by the attacker (e.g., Botnets)
- Skimmers - devices that enable thieves to steal card data and use it for fraudulent transactions
- Eavesdropping/Hijacking - interception of network traffic
- Man-in-the-Middle (MitM) - hacker inserts itself between the communications of a client and a server, examples: Session hijacking, IP Spoofing
- Web-based/app/Script-based
- Drive-by - Plant of malicious script into HTTP or PHP on insecure websites to be picked up by visitors
- SQL injection - malefactor executes a SQL query to the database via the input data from the client to server of database-driven websites
- Cross-site scripting (XSS) - use third-party web resources to run scripts in the victim’s web browser or scriptable application
- Encryption - SSL traffic is hiding malware; SSL encryption was designed to protect traffic from prying eyes, but adversaries are leveraging to hide attacks, turning the use of encryption - potential threat without proper inspection
- Data privacy - 14. Data privacy - Companies, medical providers and government

agencies store a large amount of important data, everything from the Social Security numbers of patients to the bank account numbers of customers. Data privacy refers to a branch of security focused on how to protect this information and keep it away from hackers and cyber-criminals.

- Breaches - 15. Breaches in hospitals and medical networks - Hospitals and other medical providers are prime targets for cyber-criminals. That's because these medial providers have access to the personal and financial information of so many patients. Data breaches can expose this information, which hackers can then sell on the dark web.
- Deepfakes
  - 1. Deepfakes – A combination of the words "deep learning" and "fake." Deepfakes happen when artificial intelligence technology creates fake images and sounds that appear real. A deepfake might create a video in which a politician's words are manipulated, making it appear that political leader said something they never did. Other deepfakes superimpose the face of popular actors or other celebrities onto other people's bodies.
  - 2. Deepfake voice technology - This technology allows people to spoof the voices of other people — often politicians, celebrities or CEOs — using artificial intelligence.
- Identity Theft/Synthetic identities - 3. Synthetic identities are a form of identity fraud in which scammers use a mix of real and fabricated credentials to create the illusion of a real person. For instance, a cyber-criminal might create a synthetic identity that includes a legitimate physical address. The Social Security number and birthdate associated with that address, though, might not be legitimate.
- Artificial Intelligence (AI)
  - 4. AI-powered cyberattacks - Using artificial intelligence, hackers are able to create programs that mimic known human behaviors. These hackers can then use these programs to trick people into giving up their personal or financial information.
  - 5. Hackers attacking AI while it's still learning - Artificial Intelligence evolves. It's most vulnerable to cyberattacks, though, when it's learning a new model or system. In these attacks, known as poisoning attacks, cyber-criminals can inject bad data into an AI program. This bad data can then cause the AI system to learn something it's not supposed to. Some cyber-criminals have used poisoning attacks on AI systems to get around spam detectors.
- Disinformation - 6. Disinformation in social media - You probably have heard the term "fake news." This is also known as disinformation, the deliberate spreading of news stories and information that is inaccurate and designed to persuade people — often voters — to take certain actions or hold specific beliefs. Social disinformation is often spread through social media such as Facebook and Twitter. "Fake news" became a hot topic during and after the 2016 presidential election. – Twitter
- Election security - 12. The U.S. government fears that hackers from other countries

might target the voter-registration databases for state and local governments, with the intent to either destroy or disrupt this information. This could prevent people from being able to vote. The U.S. government, then, has boosted efforts to protect this election information from cyber-criminals.

- Quantum computers - 8. Advances in quantum computers pose a threat to cryptographic systems. The idea of quantum computing is still new, but at its most basic, this is a type of computing that can use certain elements of quantum mechanics. What's important for cybersecurity is that these computers are fast and powerful. The threat is that quantum computers can decipher cryptographic codes that would take traditional computers far longer to crack — if they ever could.
- 5G - 7. New cybersecurity challenges that 5G creates - Tech experts worry that 5G will create additional cybersecurity challenges for businesses and governments. A 2019 study by Information Risk Management, titled Risky Business, said that survey respondents worried that 5G technology will result in a greater risk of cyberattacks on Internet of Things (IoT) networks. Also cited a lack of security in 5G hardware and firmware as a worry.
- Vehicle cyberattacks - 9. As more cars and trucks are connected to the Internet, the threat of vehicle-based cyberattacks rises. The worry is that cyber-criminals will be able to access vehicles to steal personal data, track the location or driving history of these vehicles, or even disable or take over safety functions.
- Cryptocurrency related
    - Cryptojacking – Cybercriminals can utilize the victim’s computing resources to mine cryptocurrency. Cybercriminals can either infect a website with cryptomining code or convince a user to click on or download a malicious link.
    - 10. Cloud jacking is a form of cyberattack in which hackers infiltrate the programs and systems of businesses, stored in the cloud, and use these resources to mine for cryptocurrency.
- Poisoning – corruption of system/system components
- Zombie - In computing, a zombie is a computer connected to the Internet that has been compromised by a hacker, computer virus, computer worm, or troJanuary horse program and can be used to perform malicious tasks of one sort or another under remote direction.
- Birthday - Replace message with same MD - Birthday attacks are made against hash algorithms that are used to verify the integrity of a message, software or digital signature. A message processed by a hash function produces a Message Digest (MD) of fixed length, independent of the length of the input message; this MD uniquely characterizes the message. The birthday attack refers to the probability of finding two random messages that generate the same MD when processed by a hash function. If an attacker calculates same MD for his message as the user has, he can safely replace the user’s message with his, and the receiver will not be able to detect the replacement even if he compares

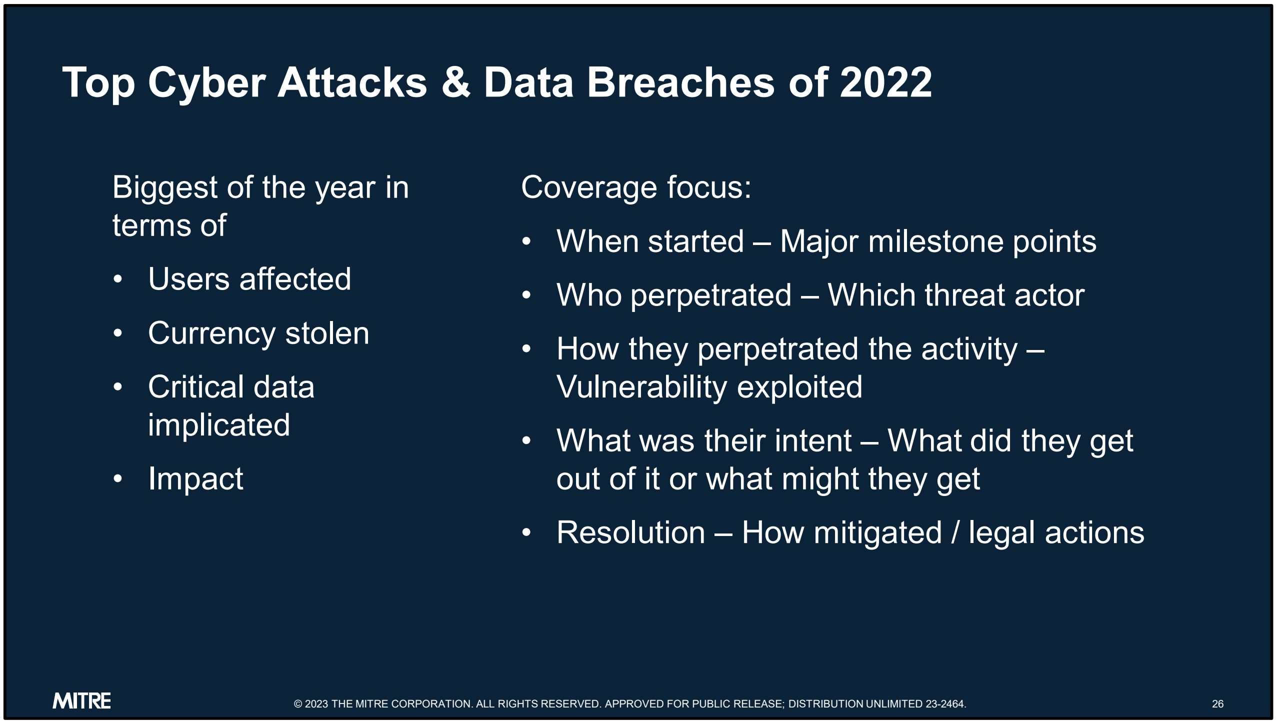
MDs.

  - Password attack – gain passwords through ‘sniffing’’ connection, physical recon, etc. Made easier by lack of password complexity, using same password across multiple accounts.
  - Credential Attacks (Arctic Wolf)
    - Brute-Force: An attempt by a malicious actor to gain unauthorized access to secure systems by trying all possible passwords and guessing the correct one.
    - Credential Stuffing: A form of brute-force that uses raw computing power and automation to repeatedly attempt password combinations until finding the right login.
    - Password Spraying: Another form of brute-force that attempts to log into an organization using known usernames in combination with common and/or default passwords.
    - Shoulder Surfing: Obtaining credentials through direct observation of a user’s screen when in a public setting.
    - MFA-Fatigue: A threat actor continuously prompts an MFA device, hoping the user will authenticate.
  - Malicious Documents: As the pandemic caused a rise in remote work, this type of attack vector surged in use. It can take the form of a locked pdf which requires your account password to “open”— effectively harvesting your credentials —or a malicious macro embedded in a Microsoft Office document. These documents are commonly used in phishing scams.
- How they get data
  - Calls, text, email, social media contact (ads/links, messages)
  - High target Mobile phone thought to be weakest link
  - Key loggers
  - Use boiler room call centers for data collection and illicit sales - spoof # to look like it's local - use social media to Target demographics - place ads on social media only target sees - openers may even think it's legitimate - closer usually in on it

2022 hot fraud scams – AARP Bulletin April 2022

1. Google voice scam - may respond to ad with your phone number, then say they want to verify it's you with a Google voice code and really are setting up a Google voice - Account in your name to perpetrate scams pretending to be you<br>
2. Rental Assistance cons<br>
3. Fake job frauds<br>
4. Fake Amazon employees<br>
5. Cryptocurrency ATM payments - no way to get money back<br>
7. Local tax imposter<br>
7. Favor for a friend- gift cards<br>
8. P2P payment requests

# Highlighted Attacks



## Top Cyber Attacks & Data Breaches of 2022

Biggest of the year in terms of

- Users affected
- Currency stolen
- Critical data implicated
- Impact

Coverage focus:

- When started – Major milestone points
- Who perpetrated – Which threat actor
- How they perpetrated the activity – Vulnerability exploited
- What was their intent – What did they get out of it or what might they get
- Resolution – How mitigated / legal actions

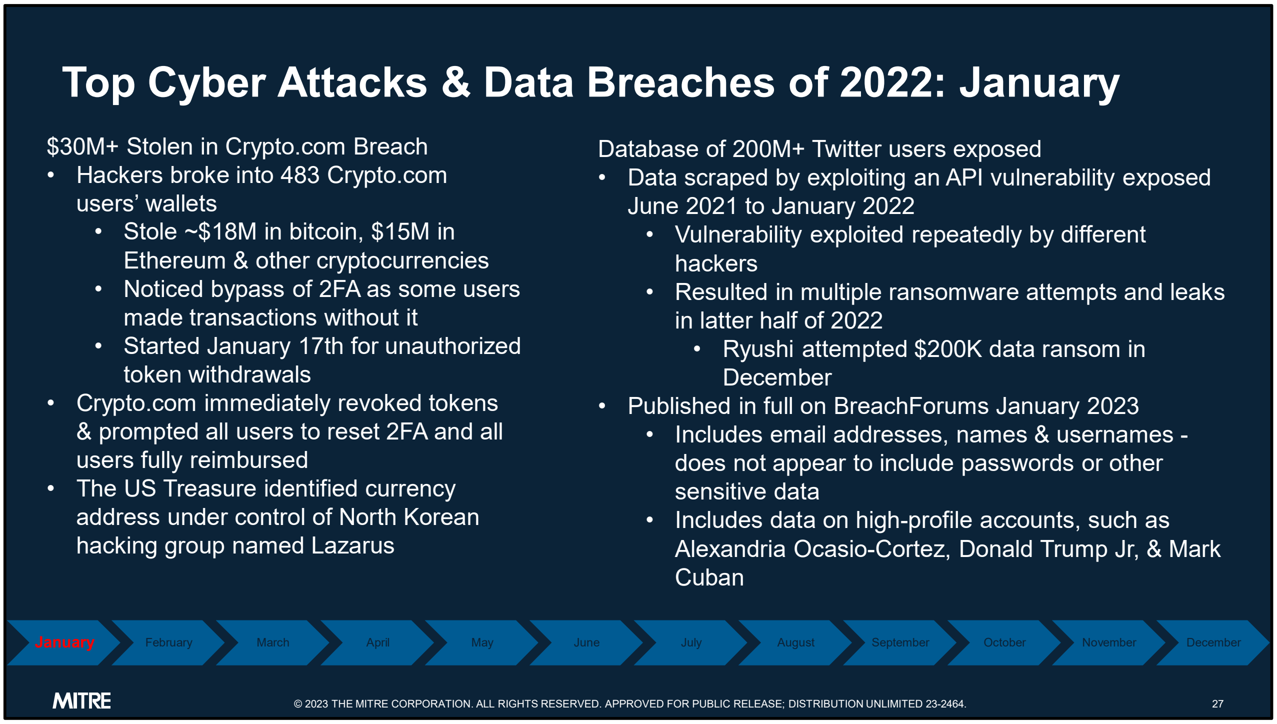
MITRE

Reference(s):

- Top 10 Biggest Data Breaches of 2022, Michael X. Heiligenstein, Firewall Times, https://firewalltimes.com/biggest-data-breaches-2022/, 10 January 2023.
- Recent Data Breaches – 2023, Michael X. Heiligenstein, Firewall Times, https://firewalltimes.com/recent-data-breaches/, 9 March 2023.

Note(s):

- International
- For continued attacks/breach put on initial month started if known or publicly reported, adding bullets with updated/ additional info through 2022 to present



## Top Cyber Attacks & Data Breaches of 2022: January

$30M+ Stolen in Crypto.com Breach

- Hackers broke into 483 Crypto.com users' wallets
  - Stole ~$18M in bitcoin, $15M in Ethereum & other cryptocurrencies
  - Noticed bypass of 2FA as some users made transactions without it
  - Started January 17th for unauthorized token withdrawals
- Crypto.com immediately revoked tokens & prompted all users to reset 2FA and all users fully reimbursed
- The US Treasure identified currency address under control of North Korean hacking group named Lazarus

Database of 200M+ Twitter users exposed

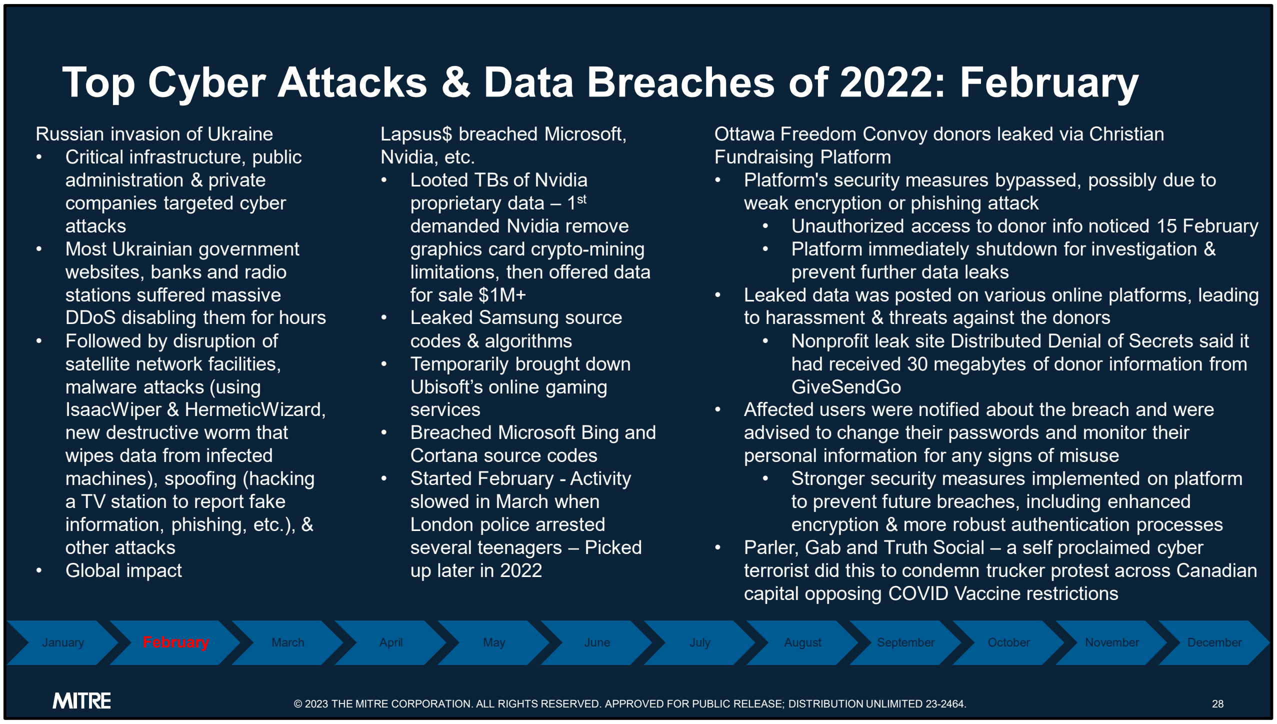
- Data scraped by exploiting an API vulnerability exposed June 2021 to January 2022
  - Vulnerability exploited repeatedly by different hackers
  - Resulted in multiple ransomware attempts and leaks in latter half of 2022
    - Ryushi attempted $200K data ransom in December
- Published in full on BreachForums January 2023
  - Includes email addresses, names & usernames - does not appear to include passwords or other sensitive data
  - Includes data on high-profile accounts, such as Alexandria Ocasio-Cortez, Donald Trump Jr, & Mark Cuban

January February March April May June July August September October November December

MITRE

Reference(s):

- Top 10 Biggest Data Breaches of 2022, Michael X. Heiligenstein, Firewall Times, https://firewalltimes.com/biggest-data-breaches-2022/, 10 January 2023.
- Recent Data Breaches – 2023, Michael X. Heiligenstein, Firewall Times, https://firewalltimes.com/recent-data-breaches/, 17 May 2023.
- Crypto.com Says more than 35 Million Stolen – 2022, The Street, https://www.thestreet.com/investing/crypto-com-says-over-35-million-dollars-stolen-by-hackers, 20 January 2022.
- U.S. ties North Korean hacker group Lazarus to huge cryptocurrency theft, Reuters, https://www.reuters.com/technology/us-ties-north-korean-hacker-group-lazarus-huge-cryptocurrency-theft-2022-04-14/#:~:text=No%20one%20has%20explicitly%20assigned%20blame%20for%20the,a%20North%20Korean%20hacking%20group%20often%20dubbed%20%22Lazarus.%22, April 2022.



# Top Cyber Attacks & Data Breaches of 2022: February

Russian invasion of Ukraine

- Critical infrastructure, public administration & private companies targeted cyber attacks
- Most Ukrainian government websites, banks and radio stations suffered massive DDoS disabling them for hours
- Followed by disruption of satellite network facilities, malware attacks (using IsaacWiper & HermeticWizard, new destructive worm that wipes data from infected machines), spoofing (hacking a TV station to report fake information, phishing, etc.), & other attacks
- Global impact

Lapsus$ breached Microsoft, Nvidia, etc.

- Looted TBs of Nvidia proprietary data – 1st demanded Nvidia remove graphics card crypto-mining limitations, then offered data for sale $1M+
- Leaked Samsung source codes & algorithms
- Temporarily brought down Ubisoft's online gaming services
- Breached Microsoft Bing and Cortana source codes
- Started February - Activity slowed in March when London police arrested several teenagers – Picked up later in 2022

Ottawa Freedom Convoy donors leaked via Christian Fundraising Platform

- Platform's security measures bypassed, possibly due to weak encryption or phishing attack
  - Unauthorized access to donor info noticed 15 February
  - Platform immediately shutdown for investigation & prevent further data leaks
- Leaked data was posted on various online platforms, leading to harassment & threats against the donors
  - Nonprofit leak site Distributed Denial of Secrets said it had received 30 megabytes of donor information from GiveSendGo
- Affected users were notified about the breach and were advised to change their passwords and monitor their personal information for any signs of misuse
  - Stronger security measures implemented on platform to prevent future breaches, including enhanced encryption & more robust authentication processes
- Parler, Gab and Truth Social – a self proclaimed cyber terrorist did this to condemn trucker protest across Canadian capital opposing COVID Vaccine restrictions

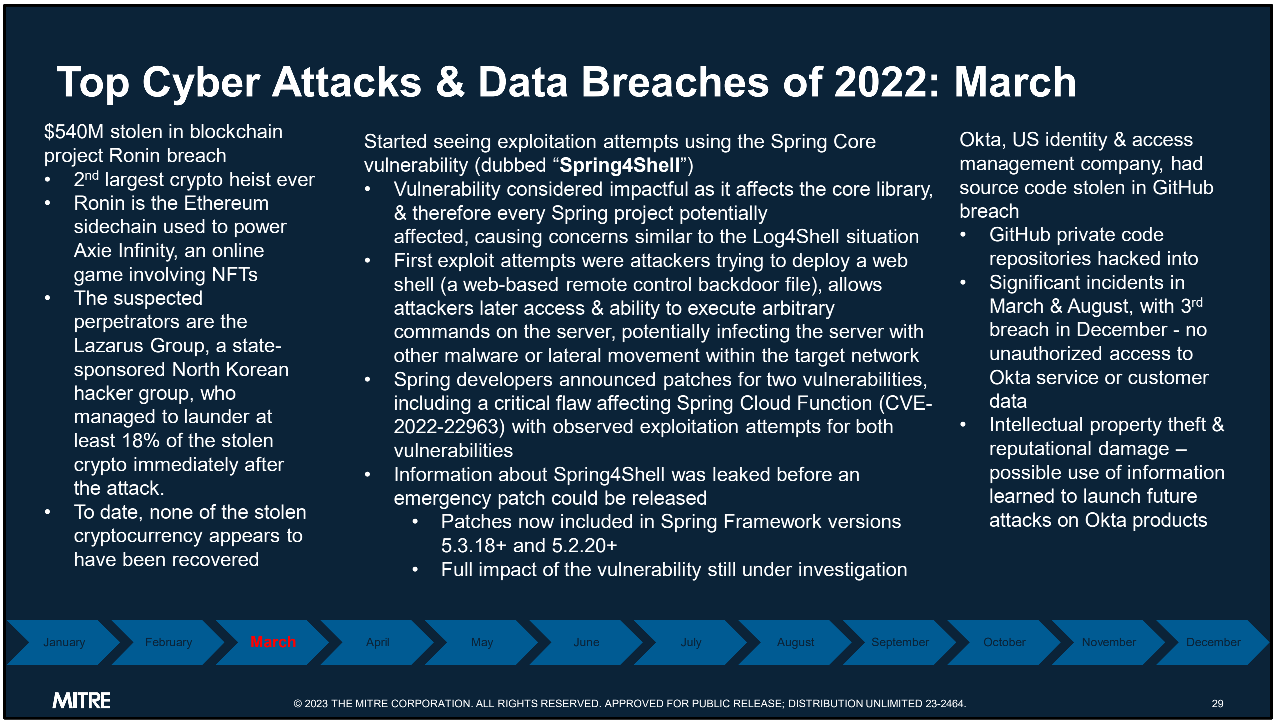
January February March April May June July August September October November December

MITRE

28

Reference(s):

- Top 10 Biggest Data Breaches of 2022, Michael X. Heiligenstein, Firewall Times, https://firewalltimes.com/biggest-data-breaches-2022/, 10 January 2023.
- Recent Data Breaches – 2023, Michael X. Heiligenstein, Firewall Times, https://firewalltimes.com/recent-data-breaches/, 9 March 2023.
- Top 10 Cyber Incidents 2022, Tokio Marine HCC International's (TMHCCI), Isaac Guasch, https://issuu.com/tmhcci/docs/tmhcc_top_10_cyber_incidents_2022/1, 31 January 2023.
- 'Cyberterrorist' boasts about hacking Freedom Convoy fundraiser — Analysis, MassNews, https://www.massnews.com/cyberterrorist-boasts-about-hacking-freedom-convoy-fundraiser-analysis/#:~:text=Hacking%20of%20other%20sites%20was%20also%20claimed%20by,who%20donated%20to%20the%20protesting%20truckers%20in%20Ottawa, February 2022.
- Hackers leak names of 'Freedom Convoy' donors after GiveSendGo breach, TechCrunch, https://techcrunch.com/2022/02/14/freedom-convoy-donor-leak-givesendgo/, February 2022.



## Top Cyber Attacks & Data Breaches of 2022: March

$540M stolen in blockchain project Ronin breach

- 2nd largest crypto heist ever
- Ronin is the Ethereum sidechain used to power Axie Infinity, an online game involving NFTs
- The suspected perpetrators are the Lazarus Group, a state-sponsored North Korean hacker group, who managed to launder at least 18% of the stolen crypto immediately after the attack.
- To date, none of the stolen cryptocurrency appears to have been recovered

Started seeing exploitation attempts using the Spring Core vulnerability (dubbed “**Spring4Shell**”)

- Vulnerability considered impactful as it affects the core library, & therefore every Spring project potentially affected, causing concerns similar to the Log4Shell situation
- First exploit attempts were attackers trying to deploy a web shell (a web-based remote control backdoor file), allows attackers later access & ability to execute arbitrary commands on the server, potentially infecting the server with other malware or lateral movement within the target network
- Spring developers announced patches for two vulnerabilities, including a critical flaw affecting Spring Cloud Function (CVE-2022-22963) with observed exploitation attempts for both vulnerabilities
- Information about Spring4Shell was leaked before an emergency patch could be released
    - Patches now included in Spring Framework versions 5.3.18+ and 5.2.20+
    - Full impact of the vulnerability still under investigation

Okta, US identity & access management company, had source code stolen in GitHub breach

- GitHub private code repositories hacked into
- Significant incidents in March & August, with 3rd breach in December - no unauthorized access to Okta service or customer data
- Intellectual property theft & reputational damage – possible use of information learned to launch future attacks on Okta products

January · February · **March** · April · May · June · July · August · September · October · November · December

MITRE

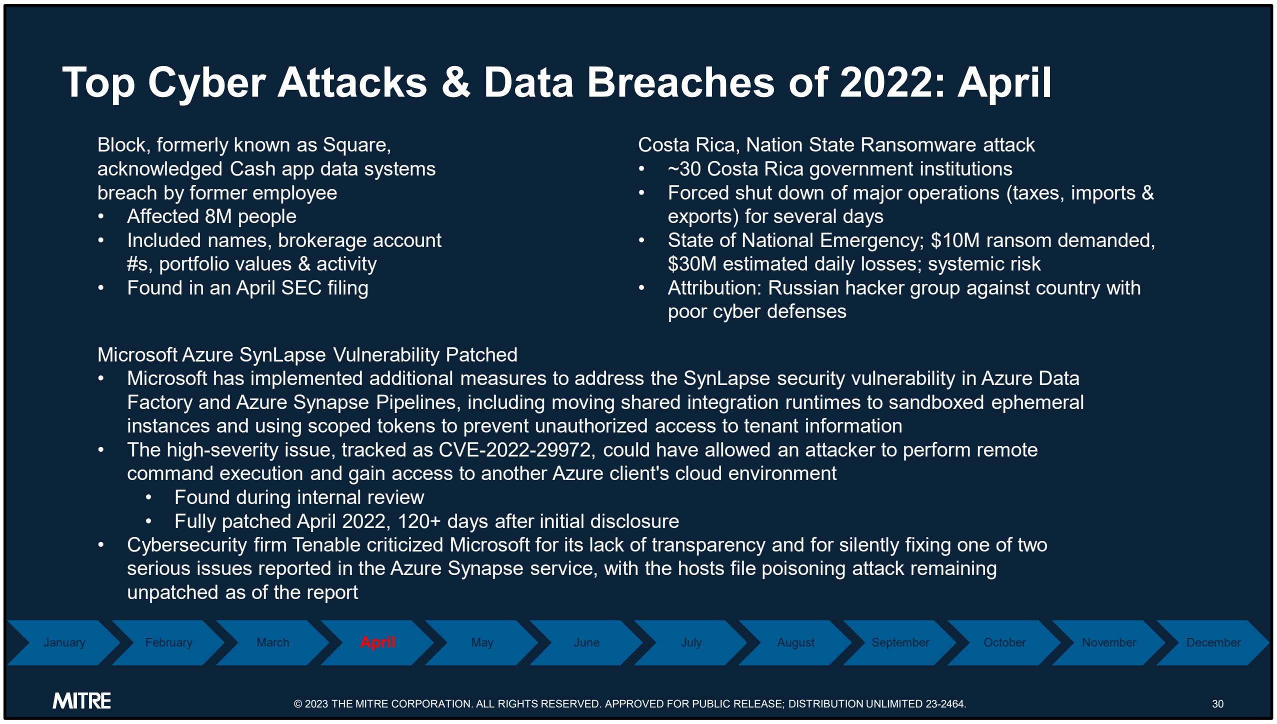
29

Reference(s):

- Top 10 Biggest Data Breaches of 2022, Michael X. Heiligenstein, Firewall Times, https://firewalltimes.com/biggest-data-breaches-2022/, 10 January 2023.
- Recent Data Breaches – 2023, Michael X. Heiligenstein, Firewall Times, https://firewalltimes.com/recent-data-breaches/, 9 March 2023.
- Mitigating Spring Core “Spring4Shell” Zero-Day, Akamai Threat Research Team, Akamai blue wave Blog, https://www.akamai.com/blog/security/spring-core-spring4shell-zero-day, 31 March 2022.
- Spring4Shell Exploitation Attempts Confirmed as Patches Are Released, The Spring zero-day vulnerability named Spring4Shell (SpringShell) has been patched, just as several cybersecurity firms have confirmed seeing exploitation attempts, SecurityWeek Network: Malware & Threats, https://www.securityweek.com/spring4shell-exploitation-attempts-confirmed-patches-are-released/, 1 April 2022.

Note(s):

- Spring Cloud Function is a project with the following high-level goals: Promote the implementation of business logic via functions. Decouple the development lifecycle of business logic from any specific runtime target so that the same code can run as a web endpoint, a stream processor, or a task.



## Top Cyber Attacks & Data Breaches of 2022: April

Block, formerly known as Square, acknowledged Cash app data systems breach by former employee
- Affected 8M people
- Included names, brokerage account #s, portfolio values & activity
- Found in an April SEC filing

Costa Rica, Nation State Ransomware attack
- ~30 Costa Rica government institutions
- Forced shut down of major operations (taxes, imports & exports) for several days
- State of National Emergency; $10M ransom demanded, $30M estimated daily losses; systemic risk
- Attribution: Russian hacker group against country with poor cyber defenses

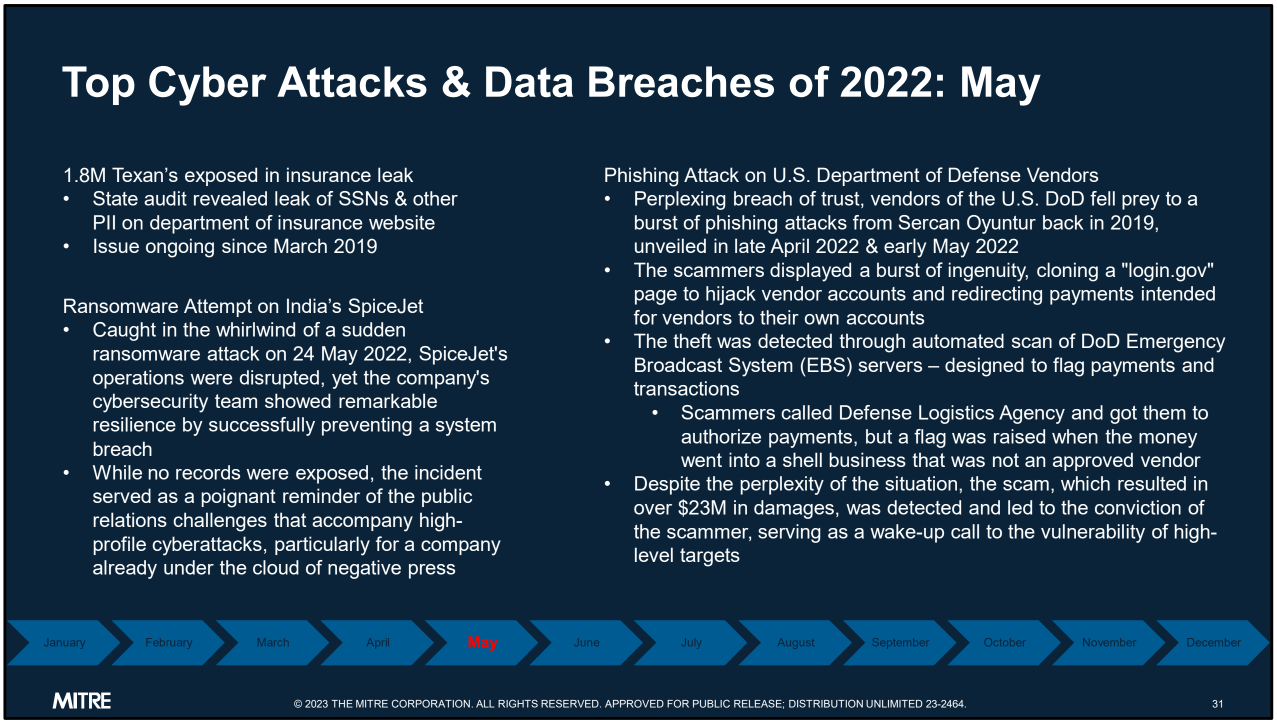
Microsoft Azure SynLapse Vulnerability Patched
- Microsoft has implemented additional measures to address the SynLapse security vulnerability in Azure Data Factory and Azure Synapse Pipelines, including moving shared integration runtimes to sandboxed ephemeral instances and using scoped tokens to prevent unauthorized access to tenant information
- The high-severity issue, tracked as CVE-2022-29972, could have allowed an attacker to perform remote command execution and gain access to another Azure client's cloud environment
  - Found during internal review
  - Fully patched April 2022, 120+ days after initial disclosure
- Cybersecurity firm Tenable criticized Microsoft for its lack of transparency and for silently fixing one of two serious issues reported in the Azure Synapse service, with the hosts file poisoning attack remaining unpatched as of the report

January February March April May June July August September October November December

MITRE

30

Reference(s):
- Recent Data Breaches – 2023, Michael X. Heiligenstein, Firewall Times, https://firewalltimes.com/recent-data-breaches/, 9 March 2023.
- Top 10 Cyber Incidents 2022, Tokio Marine HCC International’s (TMHCCI), Isaac Guasch, https://issuu.com/tmhcci/docs/tmhcc_top_10_cyber_incidents_2022/1, 31 January 2023.
- Technical Details Released for 'SynLapse' RCE Vulnerability Reported in Microsoft Azure, The Hacker News, Ravie Lakshmanan, https://thehackernews.com/2022/06/technical-details-released-for-synlapse.html, 14 June 2022.



# Top Cyber Attacks & Data Breaches of 2022: May

1.8M Texan’s exposed in insurance leak

- State audit revealed leak of SSNs & other PII on department of insurance website
- Issue ongoing since March 2019

Ransomware Attempt on India’s SpiceJet

- Caught in the whirlwind of a sudden ransomware attack on 24 May 2022, SpiceJet's operations were disrupted, yet the company's cybersecurity team showed remarkable resilience by successfully preventing a system breach
- While no records were exposed, the incident served as a poignant reminder of the public relations challenges that accompany high-profile cyberattacks, particularly for a company already under the cloud of negative press

Phishing Attack on U.S. Department of Defense Vendors

- Perplexing breach of trust, vendors of the U.S. DoD fell prey to a burst of phishing attacks from Sercan Oyuntur back in 2019, unveiled in late April 2022 & early May 2022
- The scammers displayed a burst of ingenuity, cloning a "login.gov" page to hijack vendor accounts and redirecting payments intended for vendors to their own accounts
- The theft was detected through automated scan of DoD Emergency Broadcast System (EBS) servers – designed to flag payments and transactions
  - Scammers called Defense Logistics Agency and got them to authorize payments, but a flag was raised when the money went into a shell business that was not an approved vendor
- Despite the perplexity of the situation, the scam, which resulted in over $23M in damages, was detected and led to the conviction of the scammer, serving as a wake-up call to the vulnerability of high-level targets

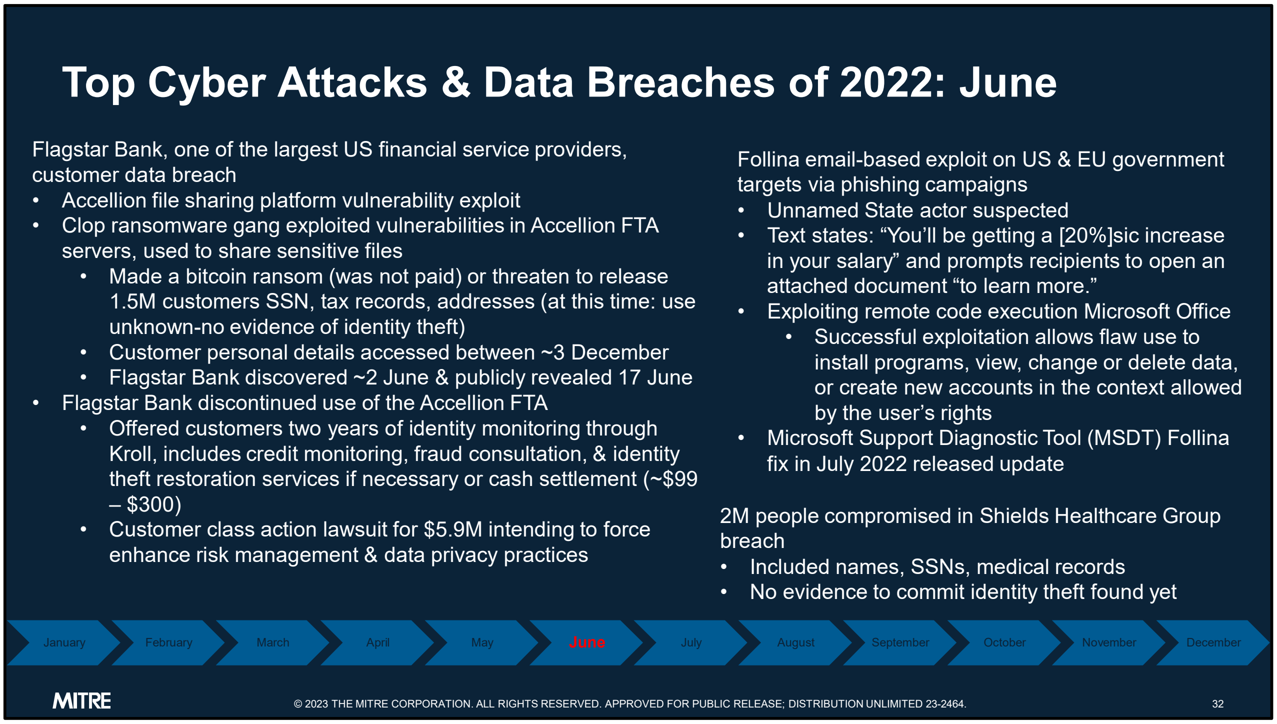
January February March April May June July August September October November December

MITRE

31

Reference(s):

- Recent Data Breaches – 2023, Michael X. Heiligenstein, Firewall Times, https://firewalltimes.com/recent-data-breaches/, 9 March 2023.
- Top Cyber Attacks of May 2022, Artic Wolf, https://arcticwolf.com/resources/blog/top-cyber-attacks-may-2022/, 7 June 2022.



## Top Cyber Attacks & Data Breaches of 2022: June

Flagstar Bank, one of the largest US financial service providers, customer data breach

- Accellion file sharing platform vulnerability exploit
- Clop ransomware gang exploited vulnerabilities in Accellion FTA servers, used to share sensitive files
  - Made a bitcoin ransom (was not paid) or threaten to release 1.5M customers SSN, tax records, addresses (at this time: use unknown-no evidence of identity theft)
  - Customer personal details accessed between ~3 December
  - Flagstar Bank discovered ~2 June & publicly revealed 17 June
- Flagstar Bank discontinued use of the Accellion FTA
  - Offered customers two years of identity monitoring through Kroll, includes credit monitoring, fraud consultation, & identity theft restoration services if necessary or cash settlement (~$99 – $300)
  - Customer class action lawsuit for $5.9M intending to force enhance risk management & data privacy practices

Follina email-based exploit on US & EU government targets via phishing campaigns

- Unnamed State actor suspected
- Text states: “You’ll be getting a [20%]sic increase in your salary” and prompts recipients to open an attached document “to learn more.”
- Exploiting remote code execution Microsoft Office
  - Successful exploitation allows flaw use to install programs, view, change or delete data, or create new accounts in the context allowed by the user’s rights
- Microsoft Support Diagnostic Tool (MSDT) Follina fix in July 2022 released update

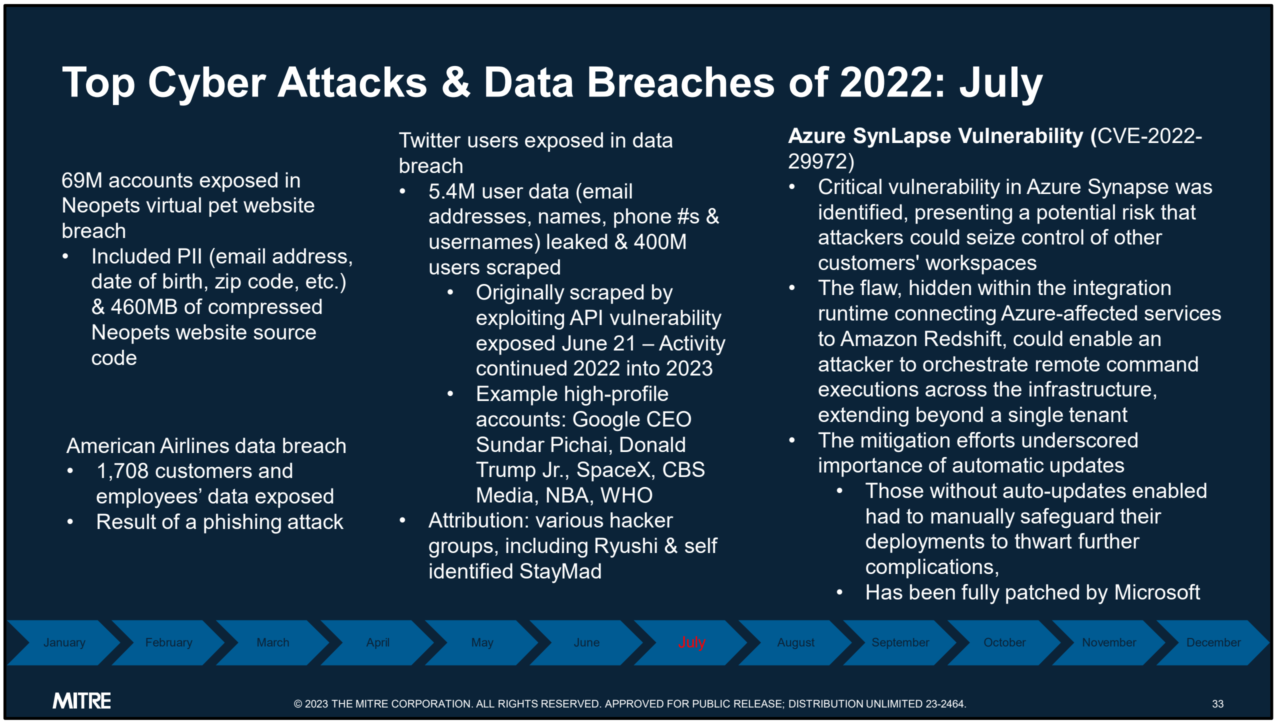
2M people compromised in Shields Healthcare Group breach

- Included names, SSNs, medical records
- No evidence to commit identity theft found yet

MITRE

Reference(s):

- Recent Data Breaches – 2023, Michael X. Heiligenstein, Firewall Times, https://firewalltimes.com/recent-data-breaches/, 9 March 2023.
- A government-aligned attacker tried using a Microsoft vulnerability to attack U.S. and E.U. government targets, Nate Nelson, https://threatpost.com/follina-exploited-by-state-sponsored-hackers/179890/, 7 June 2022.
- Microsoft Releases Workaround Guidance for MSDT “Follina” Vulnerability, CISA, https://www.cisa.gov/news-events/alerts/2022/05/31/microsoft-releases-workaround-guidance-msdt-follina-vulnerability, 31 May 2022.
- Flagstar Bank hit by data breach exposing customer, employee data, Lawrence Adams, https://www.bleepingcomputer.com/news/security/flagstar-bank-hit-by-data-breach-exposing-customer-employee-data/ , March 2022.
- Flagstar Bank Was Hacked in December, Over 1.5 Million Customers Impacted, Matthew Humphries, https://www.pcmag.com/news/flagstar-bank-was-hacked-but-didnt-realize-for-months, June 2022.



## Top Cyber Attacks & Data Breaches of 2022: July

69M accounts exposed in Neopets virtual pet website breach

- Included PII (email address, date of birth, zip code, etc.) & 460MB of compressed Neopets website source code

American Airlines data breach

- 1,708 customers and employees' data exposed
- Result of a phishing attack

Twitter users exposed in data breach

- 5.4M user data (email addresses, names, phone #s & usernames) leaked & 400M users scraped
  - Originally scraped by exploiting API vulnerability exposed June 21 – Activity continued 2022 into 2023
  - Example high-profile accounts: Google CEO Sundar Pichai, Donald Trump Jr., SpaceX, CBS Media, NBA, WHO
- Attribution: various hacker groups, including Ryushi & self identified StayMad

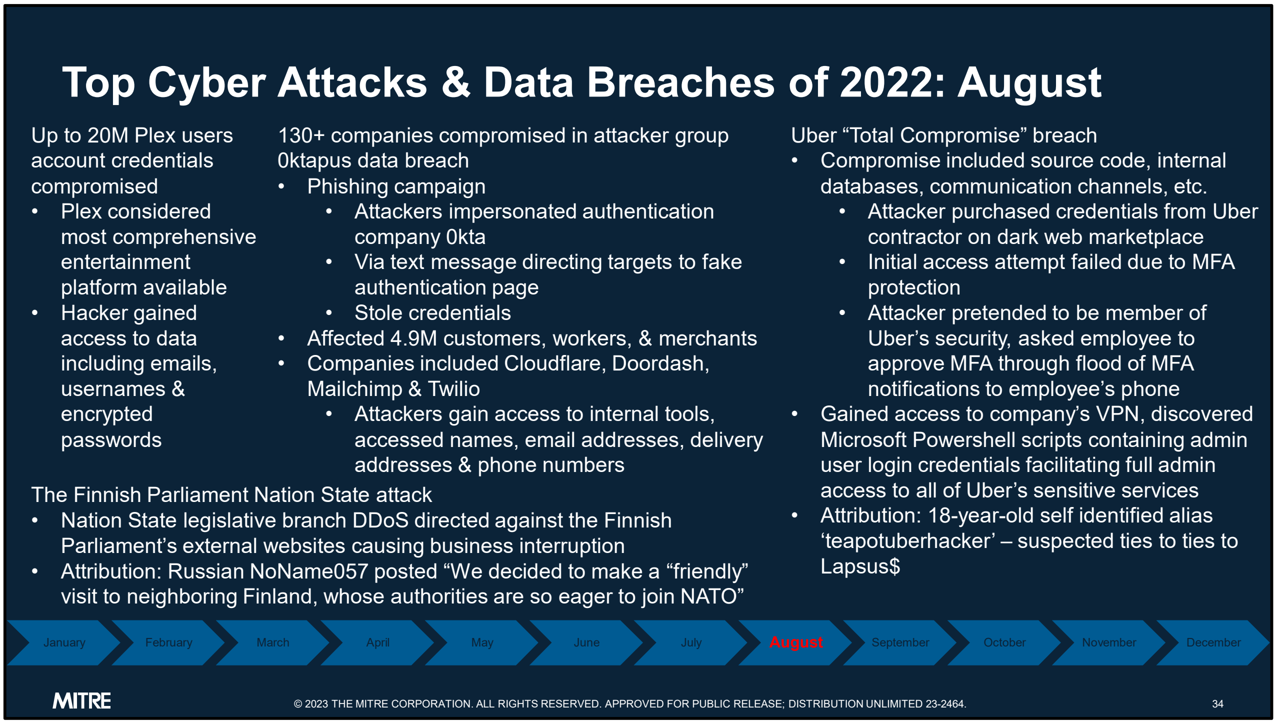
**Azure SynLapse Vulnerability** (CVE-2022-29972)

- Critical vulnerability in Azure Synapse was identified, presenting a potential risk that attackers could seize control of other customers' workspaces
- The flaw, hidden within the integration runtime connecting Azure-affected services to Amazon Redshift, could enable an attacker to orchestrate remote command executions across the infrastructure, extending beyond a single tenant
- The mitigation efforts underscored importance of automatic updates
  - Those without auto-updates enabled had to manually safeguard their deployments to thwart further complications,
  - Has been fully patched by Microsoft

MITRE

Reference(s):

- Top 10 Biggest Data Breaches of 2022, Michael X. Heiligenstein, Firewall Times, https://firewalltimes.com/biggest-data-breaches-2022/, 10 January 2023.
- Recent Data Breaches – 2023, Michael X. Heiligenstein, Firewall Times, https://firewalltimes.com/recent-data-breaches/, 9 March 2023.
- Twitter Data Leak: Account Details Of 200 Million Users Breached, Including Sundar Pichai, Donald Trump Jr., More, APB Live, https://news.abplive.com/technology/twitter-data-breach-account-details-of-200-million-users-including-sundar-pichai-donald-trump-jr-leaked-1573794, 6 January 2023.
- Top 10 Cyber Incidents 2022, Tokio Marine HCC International's (TMHCCI), Isaac Guasch, https://issuu.com/tmhcci/docs/tmhcc_top_10_cyber_incidents_2022/1, 31 January 2023.
- Critical Vulnerability in Azure Synapse Let Attackers Control other Customers' Workspaces, GBhackers, Gru Baran, https://gbhackers.com/vulnerability-in-azure-synapse/, 12 May 2022.



## Top Cyber Attacks & Data Breaches of 2022: August

Up to 20M Plex users account credentials compromised

- Plex considered most comprehensive entertainment platform available
- Hacker gained access to data including emails, usernames & encrypted passwords

130+ companies compromised in attacker group 0ktapus data breach

- Phishing campaign
  - Attackers impersonated authentication company 0kta
  - Via text message directing targets to fake authentication page
  - Stole credentials
- Affected 4.9M customers, workers, & merchants
- Companies included Cloudflare, Doordash, Mailchimp & Twilio
  - Attackers gain access to internal tools, accessed names, email addresses, delivery addresses & phone numbers

The Finnish Parliament Nation State attack

- Nation State legislative branch DDoS directed against the Finnish Parliament's external websites causing business interruption
- Attribution: Russian NoName057 posted "We decided to make a "friendly" visit to neighboring Finland, whose authorities are so eager to join NATO"

Uber "Total Compromise" breach

- Compromise included source code, internal databases, communication channels, etc.
  - Attacker purchased credentials from Uber contractor on dark web marketplace
  - Initial access attempt failed due to MFA protection
  - Attacker pretended to be member of Uber's security, asked employee to approve MFA through flood of MFA notifications to employee's phone
- Gained access to company's VPN, discovered Microsoft Powershell scripts containing admin user login credentials facilitating full admin access to all of Uber's sensitive services
- Attribution: 18-year-old self identified alias 'teapotuberhacker' – suspected ties to ties to Lapsus$

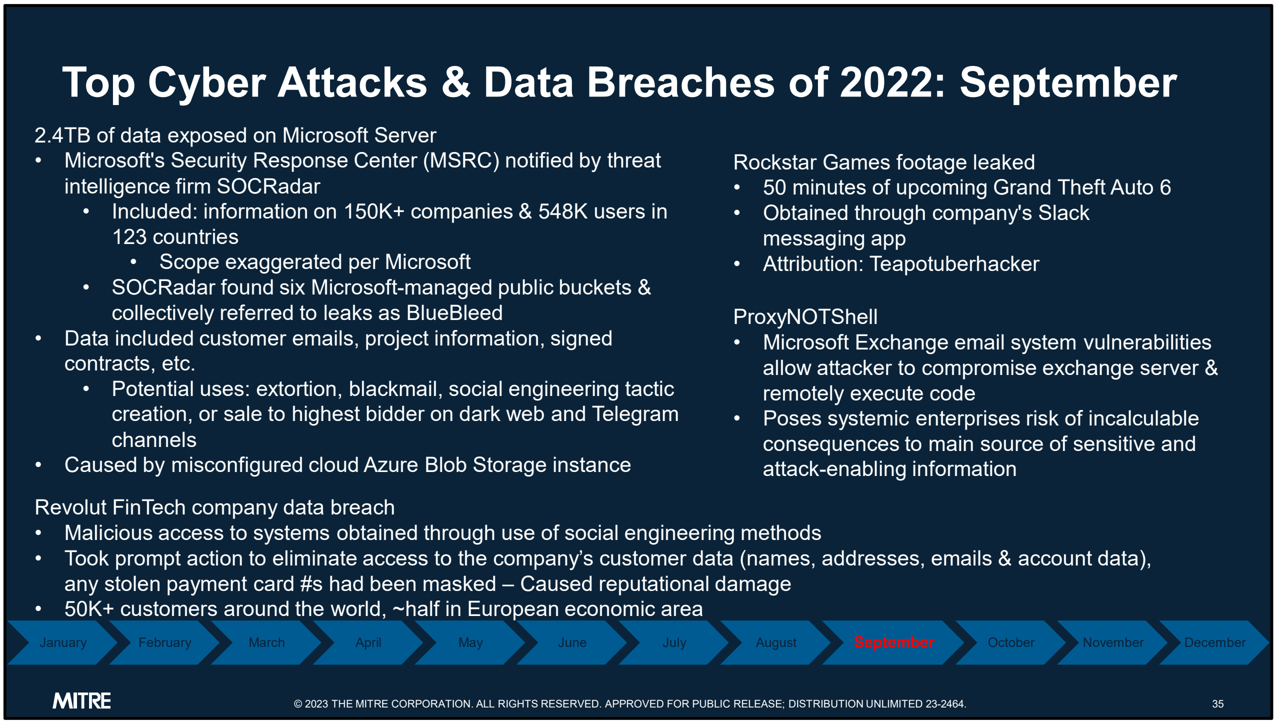
MITRE

Reference(s):

- Top 10 Biggest Data Breaches of 2022, Michael X. Heiligenstein, Firewall Times, https://firewalltimes.com/biggest-data-breaches-2022/, 10 January 2023.
- Recent Data Breaches – 2023, Michael X. Heiligenstein, Firewall Times, https://firewalltimes.com/recent-data-breaches/, 9 March 2023.
- Top 10 Cyber Incidents 2022, Tokio Marine HCC International's (TMHCCI), Isaac Guasch, https://issuu.com/tmhcci/docs/tmhcc_top_10_cyber_incidents_2022/1, 31 January 2023.
- What Caused the Uber Data Breach in 2022?, UpGuard, Edward Kost, https://www.upguard.com/blog/what-caused-the-uber-data-breach, 2 March 2023.
- Threat of multiple attack vectors 'looms large' in 2023, Staff Writer, TradeArabia, https://www.zawya.com/en/business/technology-and-telecom/threat-of-multiple-attack-vectors-looms-large-in-2023-usgvam4d, 25 April 2023.
- The Top 5 Cyber Attack Vectors, Arctic Wolf, https://arcticwolf.com/resources/blog/top-five-cyberattack-vectors/, 26 May 2023.
    - Security misconfigurations example is a Remote Desktop Protocol (RDP) that functions properly but still has the initial admin username and password.

Note(s):

- Example: DoorDash - attackers stole credentials from employees of a third-party vendor then used to gain access to DoorDash’s internal tools and accessed names, email addresses, delivery addresses and phone numbers of customers - data breach affected 4.9 million customers, workers, and merchants



## Top Cyber Attacks & Data Breaches of 2022: September

2.4TB of data exposed on Microsoft Server

- Microsoft's Security Response Center (MSRC) notified by threat intelligence firm SOCRadar
  - Included: information on 150K+ companies & 548K users in 123 countries
    - Scope exaggerated per Microsoft
  - SOCRadar found six Microsoft-managed public buckets & collectively referred to leaks as BlueBleed
- Data included customer emails, project information, signed contracts, etc.
  - Potential uses: extortion, blackmail, social engineering tactic creation, or sale to highest bidder on dark web and Telegram channels
- Caused by misconfigured cloud Azure Blob Storage instance

Rockstar Games footage leaked

- 50 minutes of upcoming Grand Theft Auto 6
- Obtained through company's Slack messaging app
- Attribution: Teapotuberhacker

ProxyNOTShell

- Microsoft Exchange email system vulnerabilities allow attacker to compromise exchange server & remotely execute code
- Poses systemic enterprises risk of incalculable consequences to main source of sensitive and attack-enabling information

Revolut FinTech company data breach

- Malicious access to systems obtained through use of social engineering methods
- Took prompt action to eliminate access to the company's customer data (names, addresses, emails & account data), any stolen payment card #s had been masked – Caused reputational damage
- 50K+ customers around the world, ~half in European economic area

January February March April May June July August September October November December

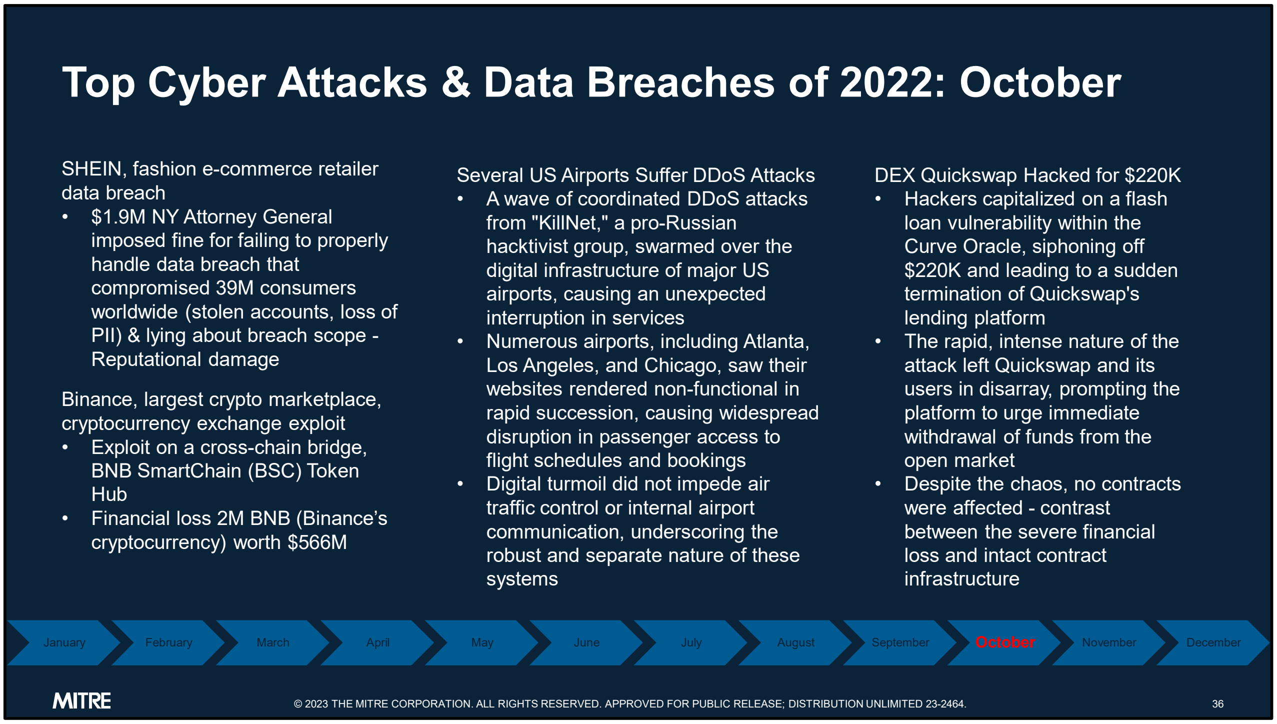
MITRE

Reference(s):

- Top 10 Biggest Data Breaches of 2022, Michael X. Heiligenstein, Firewall Times, https://firewalltimes.com/biggest-data-breaches-2022/, 10 January 2023.
- Recent Data Breaches – 2023, Michael X. Heiligenstein, Firewall Times, https://firewalltimes.com/recent-data-breaches/, 9 March 2023.
- Microsoft leaked 2.4TB of data belonging to sensitive customer, Dan Goodin, https://arstechnica.com/information-technology/2022/10/microsoft-under-fire-for-response-to-leak-of-2-4tb-of-sensitive-customer-data/, 20 October 2022.
- BlueBleed: Microsoft customer data leak claimed to be 'one of the largest' in years, Jeff Burt, The Resgister, https://www.theregister.com/2022/10/20/microsoft_data_leak_socradar/, 20 October 2022.
- Top 10 Cyber Incidents 2022, Tokio Marine HCC International's (TMHCCI), Isaac Guasch, https://issuu.com/tmhcci/docs/tmhcc_top_10_cyber_incidents_2022/1, 31 January 2023.
- Revolut confirms cyberattack exposed personal data of tens of thousands of users, https://techcrunch.com/2022/09/20/revolut-cyberattack-thousands-exposed/, 20 September 2022.

Note(s):

- Revolut FinTech company data breach
  - Confirmed it was hit by a highly targeted cyberattack that allowed hackers to access the personal details of tens of thousands of customers – September 2022
  - “unauthorized third party obtained access to the details of a small percentage (0.16%) of our customers for a short period of time”
    - Approximately 20 million customers overall
    - Isolated attack by next morning – email notification to effected customers



# Top Cyber Attacks & Data Breaches of 2022: October

SHEIN, fashion e-commerce retailer data breach

- $1.9M NY Attorney General imposed fine for failing to properly handle data breach that compromised 39M consumers worldwide (stolen accounts, loss of PII) & lying about breach scope - Reputational damage

Binance, largest crypto marketplace, cryptocurrency exchange exploit

- Exploit on a cross-chain bridge, BNB SmartChain (BSC) Token Hub
- Financial loss 2M BNB (Binance's cryptocurrency) worth $566M

Several US Airports Suffer DDoS Attacks

- A wave of coordinated DDoS attacks from "KillNet," a pro-Russian hacktivist group, swarmed over the digital infrastructure of major US airports, causing an unexpected interruption in services
- Numerous airports, including Atlanta, Los Angeles, and Chicago, saw their websites rendered non-functional in rapid succession, causing widespread disruption in passenger access to flight schedules and bookings
- Digital turmoil did not impede air traffic control or internal airport communication, underscoring the robust and separate nature of these systems

DEX Quickswap Hacked for $220K

- Hackers capitalized on a flash loan vulnerability within the Curve Oracle, siphoning off $220K and leading to a sudden termination of Quickswap's lending platform
- The rapid, intense nature of the attack left Quickswap and its users in disarray, prompting the platform to urge immediate withdrawal of funds from the open market
- Despite the chaos, no contracts were affected - contrast between the severe financial loss and intact contract infrastructure

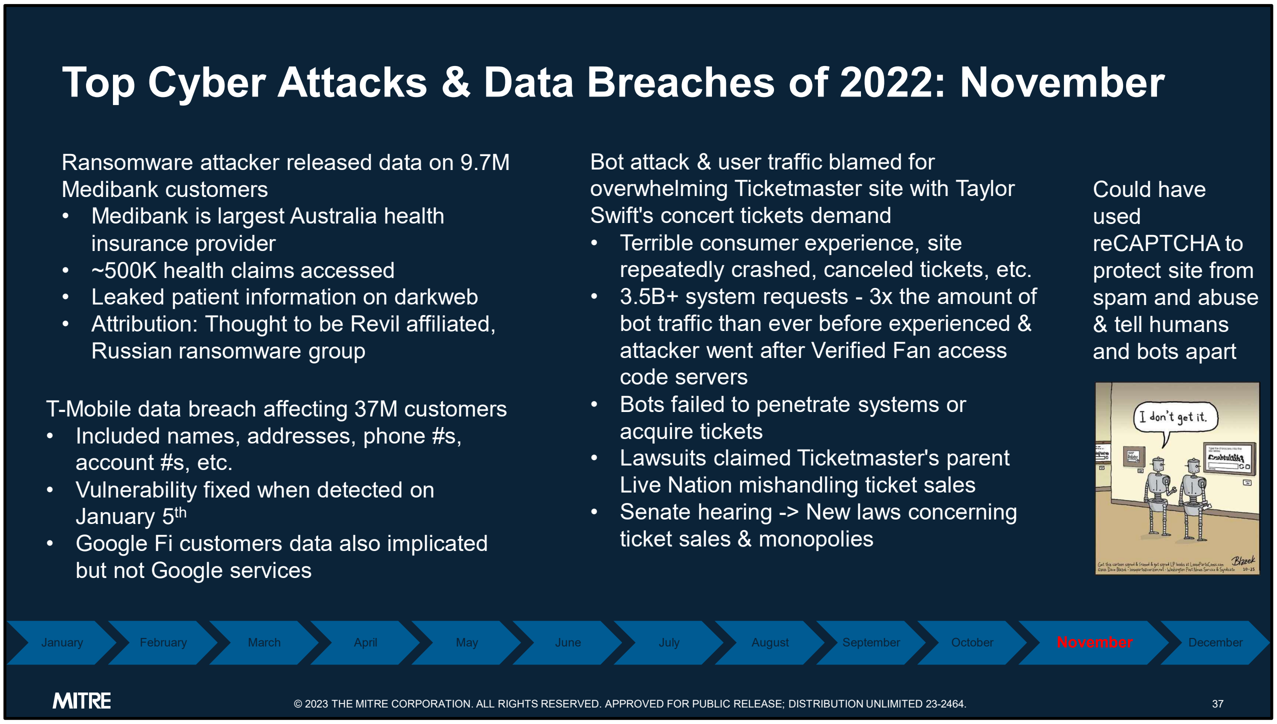
January February March April May June July August September October November December

MITRE

36

Reference(s):

- Top 10 Cyber Incidents 2022, Tokio Marine HCC International's (TMHCCI), Isaac Guasch, https://issuu.com/tmhcci/docs/tmhcc_top_10_cyber_incidents_2022/1, 31 January 2023.
- Top October 2022 Cyber-Attacks, Agile Blue, Samantha Parker, https://agileblue.com/top-october-2022-cyber-attacks/, 2 November 2022.
- Cyberattacks force over a dozen US airport websites offline, The Guardian, Betsy Reed, https://www.theguardian.com/us-news/2022/oct/10/cyberattacks-disrupt-us-airport-websites, 10 October 2022.



# Top Cyber Attacks & Data Breaches of 2022: November

Ransomware attacker released data on 9.7M Medibank customers
- Medibank is largest Australia health insurance provider
- ~500K health claims accessed
- Leaked patient information on darkweb
- Attribution: Thought to be Revil affiliated, Russian ransomware group

T-Mobile data breach affecting 37M customers
- Included names, addresses, phone #s, account #s, etc.
- Vulnerability fixed when detected on January 5th
- Google Fi customers data also implicated but not Google services

Bot attack & user traffic blamed for overwhelming Ticketmaster site with Taylor Swift's concert tickets demand
- Terrible consumer experience, site repeatedly crashed, canceled tickets, etc.
- 3.5B+ system requests - 3x the amount of bot traffic than ever before experienced & attacker went after Verified Fan access code servers
- Bots failed to penetrate systems or acquire tickets
- Lawsuits claimed Ticketmaster's parent Live Nation mishandling ticket sales
- Senate hearing -> New laws concerning ticket sales & monopolies

Could have used reCAPTCHA to protect site from spam and abuse & tell humans and bots apart

I don't get it.
Type the characters into the box below.
Crabtul2&63
Blazek
Get this cartoon signed & framed & get signed LP books at LoosePartsComic.com
©2021 Dave Blazek · looseparts@verizon.net · Washington Post News Service & Syndicate
10-25

January February March April May June July August September October **November** December

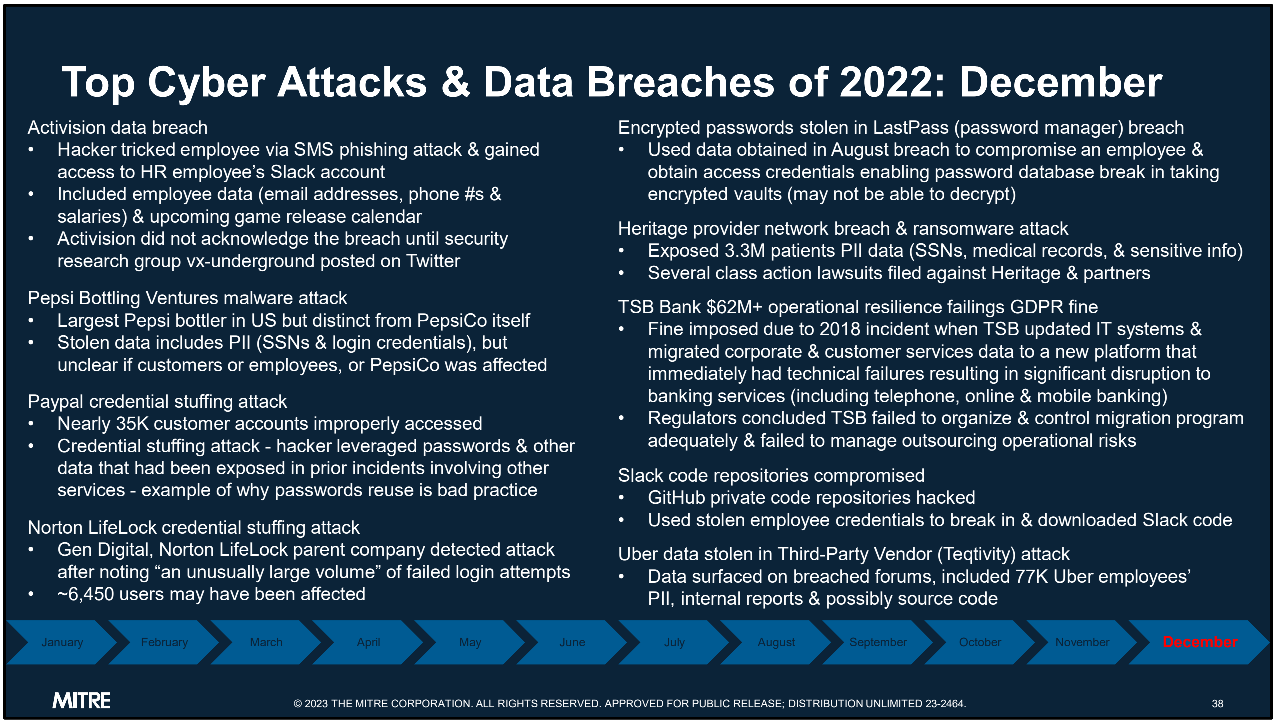
MITRE

37

Reference(s):

- Top 10 Biggest Data Breaches of 2022, Michael X. Heiligenstein, Firewall Times, https://firewalltimes.com/biggest-data-breaches-2022/, 10 January 2023.
- Recent Data Breaches – 2023, Michael X. Heiligenstein, Firewall Times, https://firewalltimes.com/recent-data-breaches/, 9 March 2023.
- Lawmakers grill ticketing industry after Taylor Swift concert fiasco, Aditi Sangal and Brian Fung, CNN, https://www.cnn.com/business/live-news/ticketmaster-taylor-swift-senate-hearing/index.html, 24 January 2023.
  - "hit with three times the amount of bot traffic than we had ever experienced, and for the first time in 400 Verified Fan on sales they came after our Verified Fan access code servers
  - While the bots failed to penetrate our systems or acquire any tickets, the attack required us to slow down and even pause our sales. This is what led to a terrible consumer experience that we deeply regret.
- Ticketmaster blames bots, demand for ticket issues, https://www.axios.com/local/nashville/2022/11/22/ticketmaster-blames-bots-demand-for-ticket-issues, 22 November 2022.
- Public Law No: 114-274, Better Online Ticket Sales Act of 2016 or the BOTS Act of 2016, Sec. 2, https://www.congress.gov/bill/114th-congress/senate-bill/3183, 14 December 2016.

- Bill prohibits the circumvention of a security measure, access control system, or other technological measure on an Internet website or online service of a ticket issuer that is used to enforce posted event ticket purchasing limits or to maintain the integrity of posted online ticket purchasing order rules for a public event with an attendance capacity exceeding 200 persons; etc.



# Top Cyber Attacks & Data Breaches of 2022: December

Activision data breach
- Hacker tricked employee via SMS phishing attack & gained access to HR employee's Slack account
- Included employee data (email addresses, phone #s & salaries) & upcoming game release calendar
- Activision did not acknowledge the breach until security research group vx-underground posted on Twitter

Pepsi Bottling Ventures malware attack
- Largest Pepsi bottler in US but distinct from PepsiCo itself
- Stolen data includes PII (SSNs & login credentials), but unclear if customers or employees, or PepsiCo was affected

Paypal credential stuffing attack
- Nearly 35K customer accounts improperly accessed
- Credential stuffing attack - hacker leveraged passwords & other data that had been exposed in prior incidents involving other services - example of why passwords reuse is bad practice

Norton LifeLock credential stuffing attack
- Gen Digital, Norton LifeLock parent company detected attack after noting "an unusually large volume" of failed login attempts
- ~6,450 users may have been affected

Encrypted passwords stolen in LastPass (password manager) breach
- Used data obtained in August breach to compromise an employee & obtain access credentials enabling password database break in taking encrypted vaults (may not be able to decrypt)

Heritage provider network breach & ransomware attack
- Exposed 3.3M patients PII data (SSNs, medical records, & sensitive info)
- Several class action lawsuits filed against Heritage & partners

TSB Bank $62M+ operational resilience failings GDPR fine
- Fine imposed due to 2018 incident when TSB updated IT systems & migrated corporate & customer services data to a new platform that immediately had technical failures resulting in significant disruption to banking services (including telephone, online & mobile banking)
- Regulators concluded TSB failed to organize & control migration program adequately & failed to manage outsourcing operational risks

Slack code repositories compromised
- GitHub private code repositories hacked
- Used stolen employee credentials to break in & downloaded Slack code

Uber data stolen in Third-Party Vendor (Teqtivity) attack
- Data surfaced on breached forums, included 77K Uber employees' PII, internal reports & possibly source code

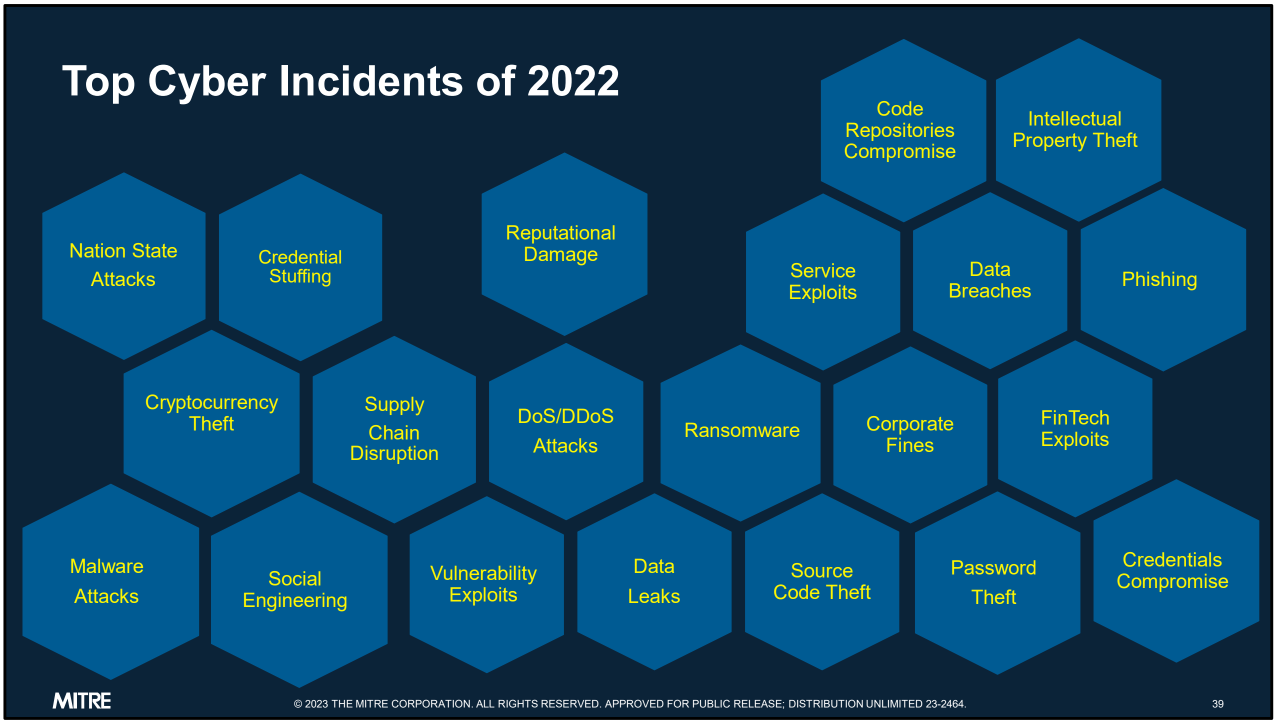
January February March April May June July August September October November December

MITRE

38

Reference(s):

- Top 10 Biggest Data Breaches of 2022, Michael X. Heiligenstein, Firewall Times, https://firewalltimes.com/biggest-data-breaches-2022/, 10 January 2023.
- Recent Data Breaches – 2023, Michael X. Heiligenstein, Firewall Times, https://firewalltimes.com/recent-data-breaches/, 17 May 2023.
- Top 10 Cyber Incidents 2022, Tokio Marine HCC International's (TMHCCI), Isaac Guasch, https://issuu.com/tmhcci/docs/tmhcc_top_10_cyber_incidents_2022/1, 31 January 2023.



## Top Cyber Incidents of 2022

Code Repositories Compromise

Intellectual Property Theft

Nation State Attacks

Credential Stuffing

Reputational Damage

Service Exploits

Data Breaches

Phishing

Cryptocurrency Theft

Supply Chain Disruption

DoS/DDoS Attacks

Ransomware

Corporate Fines

FinTech Exploits

Malware Attacks

Social Engineering

Vulnerability Exploits

Data Leaks

Source Code Theft

Password Theft

Credentials Compromise

MITRE

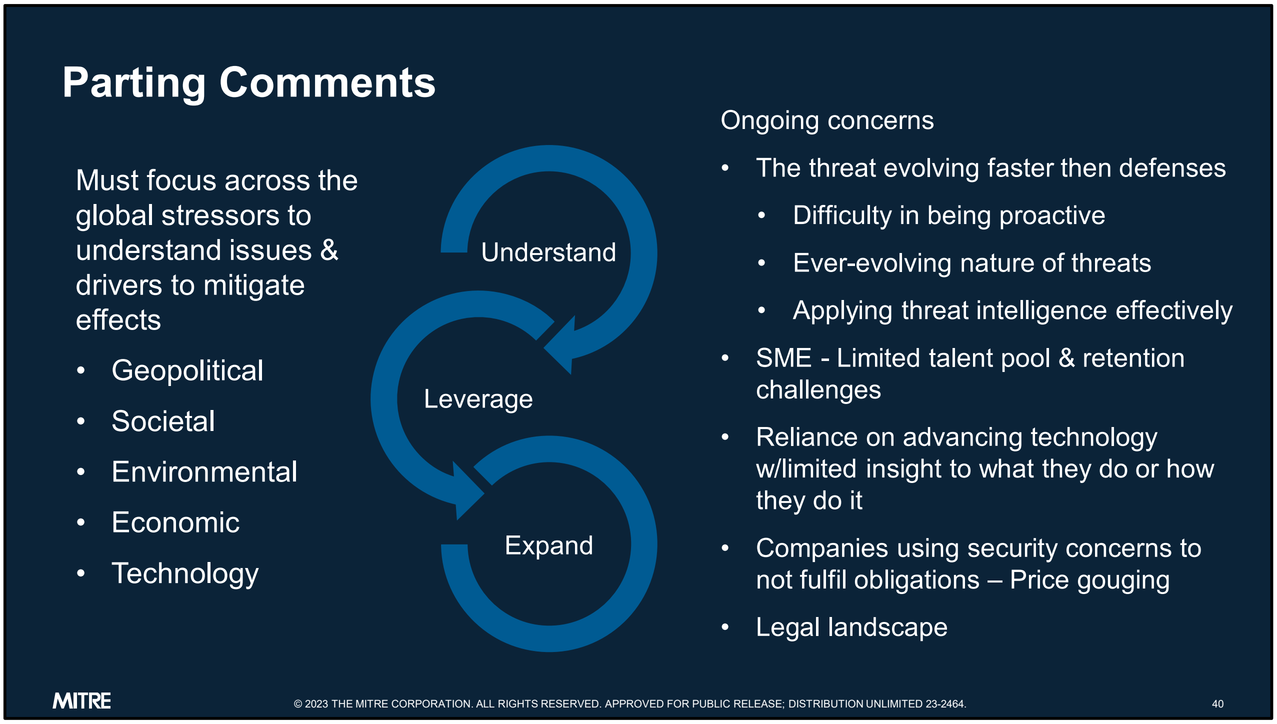
Reference(s):

- Top 10 Biggest Data Breaches of 2022, Michael X. Heiligenstein, Firewall Times, https://firewalltimes.com/biggest-data-breaches-2022/, 10 January 2023.
- Recent Data Breaches – 2023, Michael X. Heiligenstein, Firewall Times, https://firewalltimes.com/recent-data-breaches/, 17 May 2023.
- Top 10 Cyber Incidents 2022, Tokio Marine HCC International's (TMHCCI), Isaac Guasch, https://issuu.com/tmhcci/docs/tmhcc_top_10_cyber_incidents_2022/1, 31 January 2023.
- Top October 2022 Cyber-Attacks, Agile Blue, Samantha Parker, https://agileblue.com/top-october-2022-cyber-attacks/, 2 November 2022.
- Cyberattacks force over a dozen US airport websites offline, The Guardian, Betsy Reed, https://www.theguardian.com/us-news/2022/oct/10/cyberattacks-disrupt-us-airport-websites, 10 October 2022.
- Microsoft leaked 2.4TB of data belonging to sensitive customer, Dan Goodin, https://arstechnica.com/information-technology/2022/10/microsoft-under-fire-for-response-to-leak-of-2-4tb-of-sensitive-customer-data/, 20 October 2022.
- BlueBleed: Microsoft customer data leak claimed to be 'one of the largest' in years, Jeff Burt, The Resgister, https://www.theregister.com/2022/10/20/microsoft_data_leak_socradar/, 20 October 2022.

- Revolut confirms cyberattack exposed personal data of tens of thousands of users, https://techcrunch.com/2022/09/20/revolut-cyberattack-thousands-exposed/, 20 September 2022.
- What Caused the Uber Data Breach in 2022?, UpGuard, Edward Kost, https://www.upguard.com/blog/what-caused-the-uber-data-breach, 2 March 2023.
- Threat of multiple attack vectors ‘looms large’ in 2023, Staff Writer, TradeArabia, https://www.zawya.com/en/business/technology-and-telecom/threat-of-multiple-attack-vectors-looms-large-in-2023-usgvam4d, 25 April 2023.
- Ticketmaster blames bots, demand for ticket issues, https://www.axios.com/local/nashville/2022/11/22/ticketmaster-blames-bots-demand-for-ticket-issues, 22 November 2022.
- The Top 5 Cyber Attack Vectors, Arctic Wolf, https://arcticwolf.com/resources/blog/top-five-cyberattack-vectors/, 26 May 2023.
- Twitter Data Leak: Account Details Of 200 Million Users Breached, Including Sundar Pichai, Donald Trump Jr., More, APB Live, https://news.abplive.com/technology/twitter-data-breach-account-details-of-200-million-users-including-sundar-pichai-donald-trump-jr-leaked-1573794, 6 January 2023.
- Critical Vulnerability in Azure Synapse Let Attackers Control other Customers’ Workspaces, GBhackers, Gru Baran, https://gbhackers.com/vulnerability-in-azure-synapse/, 12 May 2022.
- A government-aligned attacker tried using a Microsoft vulnerability to attack U.S. and E.U. government targets, Nate Nelson, https://threatpost.com/follina-exploited-by-state-sponsored-hackers/179890/, 7 June 2022.
- Microsoft Releases Workaround Guidance for MSDT “Follina” Vulnerability, CISA, https://www.cisa.gov/news-events/alerts/2022/05/31/microsoft-releases-workaround-guidance-msdt-follina-vulnerability, 31 May 2022.
- Flagstar Bank hit by data breach exposing customer, employee data, Lawrence Adams, https://www.bleepingcomputer.com/news/security/flagstar-bank-hit-by-data-breach-exposing-customer-employee-data/ , March 2022.
- Flagstar Bank Was Hacked in December, Over 1.5 Million Customers Impacted, Matthew Humphries, https://www.pcmag.com/news/flagstar-bank-was-hacked-but-didnt-realize-for-months, June 2022.
- Mitigating Spring Core “Spring4Shell” Zero-Day, Akamai Threat Research Team, Akamai blue wave Blog, https://www.akamai.com/blog/security/spring-core-spring4shell-zero-day, 31 March 2022.
- Spring4Shell Exploitation Attempts Confirmed as Patches Are Released, The Spring zero-day vulnerability named Spring4Shell (SpringShell) has been patched, just as several cybersecurity firms have confirmed seeing exploitation attempts, SecurityWeek Network: Malware & Threats, https://www.securityweek.com/spring4shell-exploitation-attempts-confirmed-patches-are-released/, 1 April 2022.
- ‘Cyberterrorist’ boasts about hacking Freedom Convoy fundraiser — Analysis, MassNews, https://www.massnews.com/cyberterrorist-boasts-about-hacking-freedom-convoy-fundraiser-analysis/#:~:text=Hacking%20of%20other%20sites%20was%20also%20claimed%20by,wh

o%20donated%20to%20the%20protesting%20truckers%20in%20Ottawa, February 2022.

- Hackers leak names of ‘Freedom Convoy’ donors after GiveSendGo breach, TechCrunch, https://techcrunch.com/2022/02/14/freedom-convoy-donor-leak-givesendgo/, February 2022.
- U.S. ties North Korean hacker group Lazarus to huge cryptocurrency theft, Reuters, https://www.reuters.com/technology/us-ties-north-korean-hacker-group-lazarus-huge-cryptocurrency-theft-2022-04-14/#:~:text=No%20one%20has%20explicitly%20assigned%20blame%20for%20the,a%20North%20Korean%20hacking%20group%20often%20dubbed%20%22Lazarus.%22, April 2022.



## Parting Comments

Must focus across the global stressors to understand issues & drivers to mitigate effects

- Geopolitical
- Societal
- Environmental
- Economic
- Technology

Understand

Leverage

Expand

Ongoing concerns

- The threat evolving faster then defenses
  - Difficulty in being proactive
  - Ever-evolving nature of threats
  - Applying threat intelligence effectively
- SME - Limited talent pool & retention challenges
- Reliance on advancing technology w/limited insight to what they do or how they do it
- Companies using security concerns to not fulfil obligations – Price gouging
- Legal landscape

MITRE

40

Reference(s):

- Global Risks Report 2023, World Economic Forum’s (WEF), https://www.weforum.org/reports/global-risks-report-2023/digest, 11 January 23.
- Global Perspectives on Threat Intelligence, Mandiant now part of Google, Global-Perspectives-on-Threat-Intelligence-2-08-23.pdf, https://www.mandiant.com/global-perspectives-on-threat-intelligence, 8 February 2023.
- 2023 Global Threat Report, CrowdStrike, CrowdStrike2023GlobalThreatReport.pdf, https://go.crowdstrike.com/rs/281-OBQ-266/images/CrowdStrike2023GlobalThreatReport.pdf, 28 February 2023.
- 2022 Identity Fraud Study: The Virtual Background, Javelin, https://javelinstrategy.com/2022-Identity-fraud-scams-report, 28 March 2022.
- Report on Securing and Growing the Digital Economy, Commission on Enhancing National Cybersecurity, https://nsarchive.gwu.edu/document/22389-document-12-commission-enhancing-national, 1 December 2016.
- Better Identity in America: A Blueprint for Policymakers, Better Identity Coalition, https://static1.squarespace.com/static/5a7b7a8490bade8a77c07789/t/5d07cd2eca832a0001656624/1560792371066/Better_Identity_Coalition%2BBlueprint%2B-%2BJuly%2B2018.pdf, July 2018.
- H.R. 4258, the Improving Digital Identity Act, by Representatives Bill Foster, John Katko, James R. Langevin, and Barry Loudermilk, https://www.congress.gov/bill/117th-

congress/house-bill/4258?s=1&r=47, Introduced 30 June 2021.

- H.R. 8322 - 117th Congress (2021-2022): STOP Fraud Act, The Strengthening Tools to Obstruct and Prevent Fraud Act of 2022, introduced by Chairman Gerald E. Connolly, https://www.congress.gov/bill/117th-congress/house-bill/8322, Introduced on 11 July 2022.
- Lawmakers grill ticketing industry after Taylor Swift concert fiasco, Aditi Sangal and Brian Fung, CNN, https://www.cnn.com/business/live-news/ticketmaster-taylor-swift-senate-hearing/index.html, 24 January 2023.
    - “hit with three times the amount of bot traffic than we had ever experienced, and for the first time in 400 Verified Fan on sales they came after our Verified Fan access code servers
    - While the bots failed to penetrate our systems or acquire any tickets, the attack required us to slow down and even pause our sales. This is what led to a terrible consumer experience that we deeply regret.
- Public Law No: 114-274, Better Online Ticket Sales Act of 2016 or the BOTS Act of 2016, Sec. 2, https://www.congress.gov/bill/114th-congress/senate-bill/3183, 14 December 2016.
    - This bill prohibits the circumvention of a security measure, access control system, or other technological measure on an Internet website or online service of a ticket issuer that is used to enforce posted event ticket purchasing limits or to maintain the integrity of posted online ticket purchasing order rules for a public event with an attendance capacity exceeding 200 persons
- Cyber Threats, What types of cyberattacks and operations and which actors pose the greatest threat, https://cyberconflicts.cyberpeaceinstitute.org/threats, Last updated 29 June 2023.

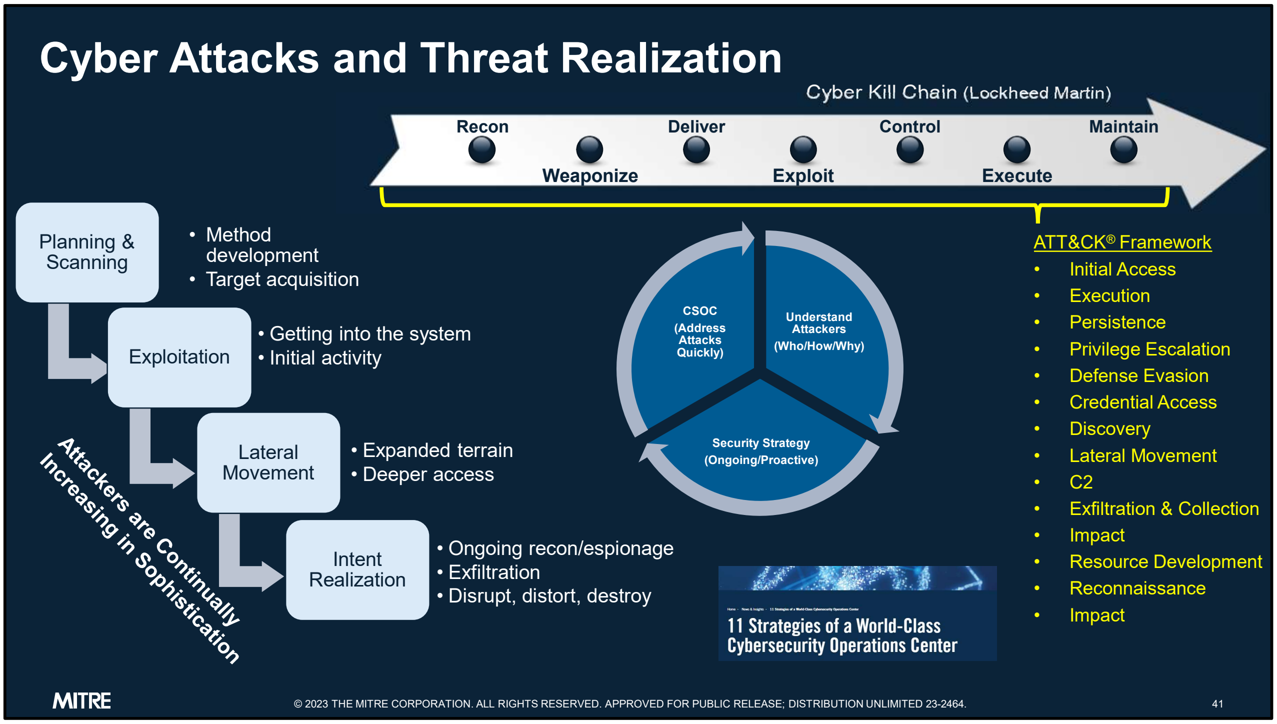
Note(s):

- Technology - Security must parallel technology innovation
- New policies & laws are being implemented - New laws expanding existing one
- Public Law No: 114-274, Better Online Ticket Sales Act of 2016 or the BOTS Act of 2016, Sec. 2, https://www.congress.gov/bill/114th-congress/senate-bill/3183, 14 December 2016.
    - H.R. 4258, the Improving Digital Identity Act, by Representatives Bill Foster, John Katko, James R. Langevin, and Barry Loudermilk, https://www.congress.gov/bill/117th-congress/house-bill/4258?s=1&r=47, Introduced 30 June 2021
        - Experts have recognized the need for a streamlined approach across federal, state, and local governments, in coordination with the private sector, to strengthen the country’s digital identity infrastructure against this threat.
    - The Strengthening Tools to Obstruct and Prevent Fraud Act of 2022 was introduced by Chairman Gerald E. Connolly on July 11, 2022. The bill seeks to foster a federal government focus on the reduction of improper payments and fraud by removing unnecessary compliance requirements and incentivizing use of

data analytics and other tools to proactively prevent waste, fraud, and abuse.

        - Despite rigorous annual reporting requirements related to identifying improper payments and their causes, they have steadily risen from $35 billion in 2004 to $281 billion in 2021, according to the Government Accountability Office. The STOP Fraud Act would establish a dedicated antifraud office, known as the Federal Real Antifraud Unified Directorate (FRAUD), within the Office of Management and Budget. The Office would assist agencies in using best practices to prevent and reduce fraud and provide technical support to all agencies to help them create outcome-focused initiatives that save taxpayer dollars. It would also establish an online, public dashboard to tracks cost savings, cost avoidance, and burden reduction those who qualify for federal program funding.

- Regulators:
    - The Financial Conduct Authority
    - European Securities and Markets Authority
    - Prudential Regulation Authority
    - Securities and Exchange Commission
- Revised Payment Services Directive (PSD2) - Directive (EU) 2015/2366
    - European Union (EU) Directive, administered by the European Commission
    - Regulates payment services & providers
    - Throughout the EU & European Economic Area (EEA)
    - Key elements to reduce and manage fraud without negatively impacting customer experience & improve consumer choice
        - Strong Customer Authentication (SCA)
        - Two types of new regulated payment providers/Third Party Providers (TPPs) expected to drive payments innovation and competition



## Cyber Attacks and Threat Realization

Cyber Kill Chain (Lockheed Martin)

Recon · Weaponize · Deliver · Exploit · Control · Execute · Maintain

Planning & Scanning
- Method development
- Target acquisition

Exploitation
- Getting into the system
- Initial activity

Lateral Movement
- Expanded terrain
- Deeper access

Intent Realization
- Ongoing recon/espionage
- Exfiltration
- Disrupt, distort, destroy

Attackers are Continually Increasing in Sophistication

CSOC (Address Attacks Quickly)

Understand Attackers (Who/How/Why)

Security Strategy (Ongoing/Proactive)

11 Strategies of a World-Class Cybersecurity Operations Center

ATT&CK® Framework
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- C2
- Exfiltration & Collection
- Impact
- Resource Development
- Reconnaissance
- Impact

MITRE

Reference(s):

- The Top 5 Cyber Attack Vectors, Arctic Wolf, https://arcticwolf.com/resources/blog/top-five-cyberattack-vectors/, 26 May 2023.
- ATT&CK® Framework, MITRE, https://attack.mitre.org/, Last accessed 16 March 2023.
- 11 Strategies of a World-Class Cybersecurity Operations Center, The MITRE Corporation, Kathryn Knerler, Ingrid Parker, Carson Zimmerman, https://www.mitre.org/news-insights/publication/11-strategies-world-class-cybersecurity-operations-center, 31 March 2022.
- Gartner Report: The Urgency to Treat Cybersecurity as a Business Decision, https://www.gartner.com/doc/3980891, Refreshed 2 August 2021, Published 12 February 2020.

Note(s):

- Mitigations
    - 24×7 Monitoring
        - Scan for & detect misconfigurations across devices and networks
        - Ongoing compromise monitoring and threat detection
    - Ongoing network & system management
        - Vulnerability scanning

    - Patching (at a minimum on software & systems that pose the biggest risks),
- Security strategy to eliminate gaps, misconfigurations, and vulnerabilities that attackers could exploit
- Cloud security, specifically cloud security posture management (e.g., to help detect misconfigurations in real time as well as map configurations to a security framework)
- User education & security awareness training
- Address successful attack actions quickly
    - Address successful phishing attack quickly and have next level / subsequent defenses in effect (e.g., multi-factor authentication, monitoring and detection software)
- Email filters (e.g., anti-spam to stop phishing emails from reaching inboxes)
- Enact credentials management
    - Enforce strong password requirements
    - Adopt Multi-Factor Authentication (MFA) across the IT environment
    - Limit user privileges based on roles
    - Monitor user behavior to spot unusual activity
    - Implement strict controls for admin accounts, Establish countermeasures specifically designed to thwart brute-force attacks, like limiting attempts before locking out an account or requiring manual CAPTCHA input
- Supply Chain exposure minimization, such as:
    - Require suppliers to maintain certain cybersecurity standards through your service agreements
    - Validate the suppliers’ security posture through audits, metrics, and other tools
    - Implement policies that require scanning and monitoring your vendors’ devices once they’re connected to your network
    - Use a threat detection and response solution to monitor your environment for anomalies
- Other
    - Vulnerability
    - Vulnerability scanning
    - Patching (at a minimum on software & systems that pose the biggest risks),
    - 24×7 monitoring and threat detection
    - Security misconfigurations
    - Proactive security strategy to eliminate gaps, misconfigurations, and vulnerabilities that attackers could exploit. Cloud security, specifically cloud security posture management, can help detect misconfigurations in real time as well as map configurations to a security framework. In addition, 24×7 monitoring software can scan for, and detect misconfigurations across devices and networks
    - Compromised Credentials – Enforce: Enforce strong password

requirements , Adopt MFA across the IT environment, Limit user privileges based on roles, Monitor user behavior to spot unusual activity, Implement strict controls for admin accounts, Establish countermeasures specifically designed to thwart brute-force attacks, like limiting attempts before locking out an account or requiring manual CAPTCHA input

- Supply Chain - Minimize your exposure through proactive measures:
- Require suppliers to maintain certain cybersecurity standards through your service agreements
- Validate the suppliers' security posture through audits, metrics, and other tools
- Implement policies that require scanning and monitoring your vendors' devices once they're connected to your network
- Use a threat detection and response solution to monitor your environment for anomalies

- MITRE developed ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) model to quickly identify and categorize behavior post-network infiltration
  - Persistence
  - Privilege Escalation
  - Defense Evasion
  - Credential Access
  - Discovery
  - Lateral Movement
  - Execution
  - Collection
  - Exfiltration
  - Command and Control
- Provides a common lexicon to understand, detect, mitigate, and share information about adversary activities
- FireEye threat techniques / findings now mapped to the MITRE ATT&CK framework

Report by Threat Horizon - cyber threats under three key themes:

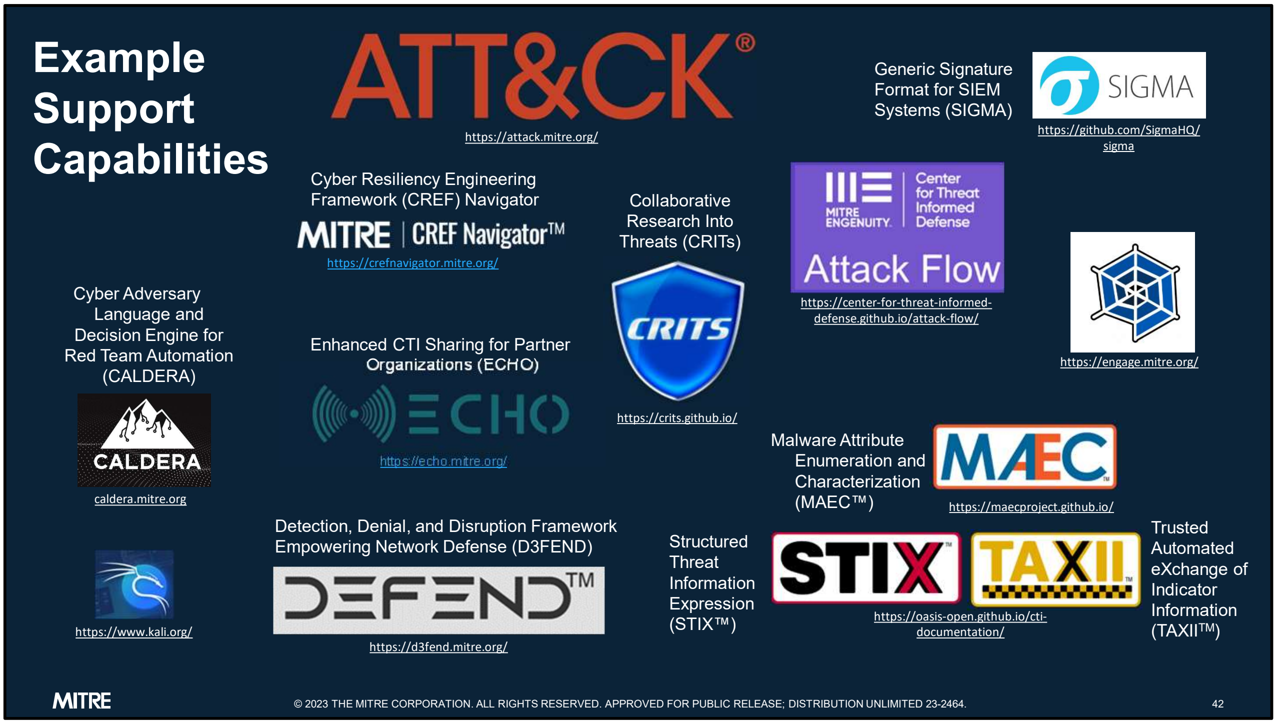
- Disruption: Over-dependence on fragile connectivity will increase the risk of premeditated internet outages that compromise business operations. Cybercriminals will use ransomware to hijack the Internet of Things (IoT).
  - 1.1 Premeditated internet outages bring trade to its knees
  - 1.2 Ransomware hijacks the Internet of Things
  - 1.3 Privileged insiders coerced into giving up their crown jewels
- Distortion: Spread of misinformation by bots and automated sources will cause compromise of trust in the integrity of information.
  - 2.1 Automated misinformation gains instant credibility
  - 2.2 Falsified information compromises performance
  - 2.3 Subverted blockchains shatter trust
- Deterioration: Rapid advances in smart technologies and conflicting demands posed by

evolving national security will negatively impact an enterprise's ability to control information. When controls are eroded by regulations and technology

  - 3.1 Surveillance laws expose corporate secrets
  - 3.2 Privacy regulations impede the monitoring of insider threats
  - 3.3 A headlong rush to deploy AI leads to unexpected outcomes.

- Risks – Geopolitical / Socioeconomic
  - Disrupt – premeditated internet outages compromise business operations / hijack IoT
  - Distort – deterioration/compromise of information/entity trust
  - Destroy – result in info, property, $ losses

- 2020 Information
  - Cost of cyber attacks
  - $26 billion global losses 2016 – 2019 (FBI IC3)
  - Cyber-crime (Cyber Security Stats Guide 2020)
  - Business Email Compromise (BEC) / Email Acct Compromise (EAC) scams (over $1.7 billion 2019)
  - Confidence/romance fraud (over $475 million 2019)
  - Spoofing (over $300 million 2019)
  - Brand Impersonations
  - Online Payment Fraud to cost E-Commerce over $25 Billion Annually by 2024 (Security Boulevard)



# Example Support Capabilities

ATT&CK®
https://attack.mitre.org/

Generic Signature Format for SIEM Systems (SIGMA)
https://github.com/SigmaHQ/sigma

Cyber Resiliency Engineering Framework (CREF) Navigator
https://crefnavigator.mitre.org/

Collaborative Research Into Threats (CRITs)
https://crits.github.io/

https://center-for-threat-informed-defense.github.io/attack-flow/

https://engage.mitre.org/

Cyber Adversary Language and Decision Engine for Red Team Automation (CALDERA)
caldera.mitre.org

Enhanced CTI Sharing for Partner Organizations (ECHO)
https://echo.mitre.org/

Malware Attribute Enumeration and Characterization (MAEC™)
https://maecproject.github.io/

Detection, Denial, and Disruption Framework Empowering Network Defense (D3FEND)
https://d3fend.mitre.org/

https://www.kali.org/

Structured Threat Information Expression (STIX™)

Trusted Automated eXchange of Indicator Information (TAXII™)

https://oasis-open.github.io/cti-documentation/

© 2023 THE MITRE CORPORATION. ALL RIGHTS RESERVED. APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED 23-2464.

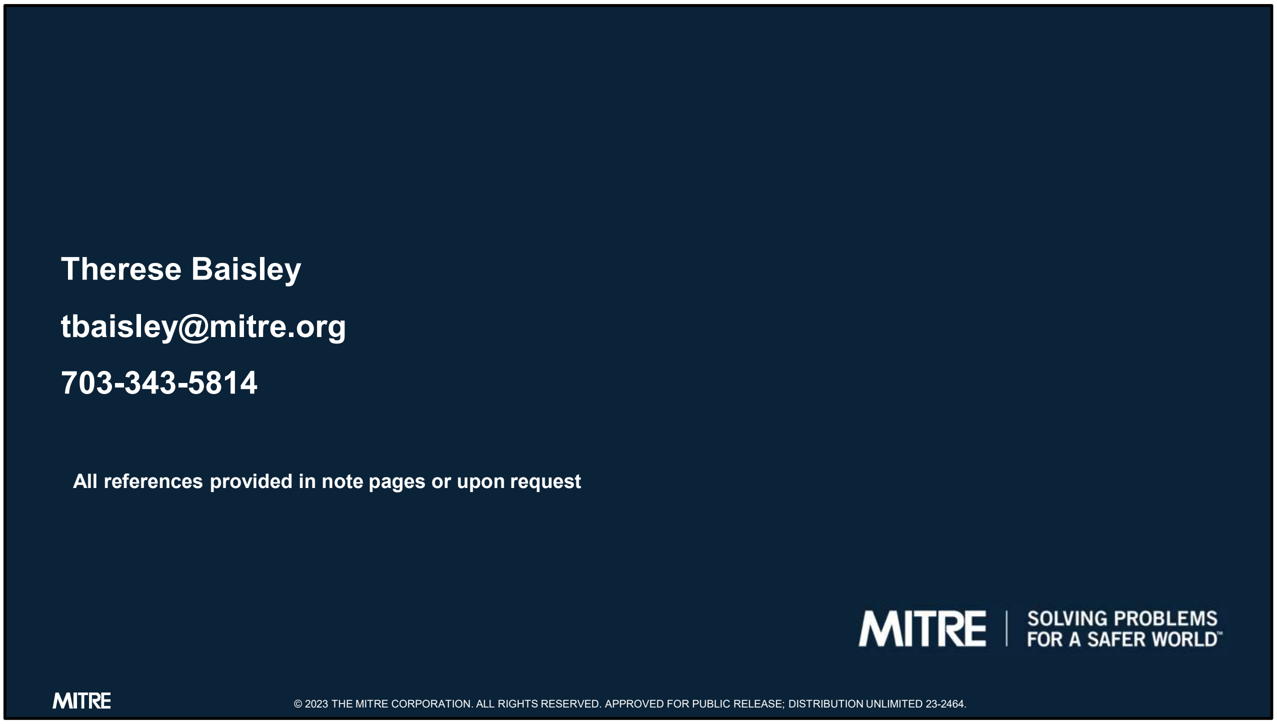
42

Reference(s):

- 11 Strategies of a World-Class Cybersecurity Operations Center, The MITRE Corporation, Kathryn Knerler, Ingrid Parker, Carson Zimmerman, 31 March 2022.
- Analytic Coverage Comparison, MITRE CAR, https://car.mitre.org/coverage/, Generated 30 December 2022.
- ATT&CK® Analytic Coverage, https://mitre-attack.github.io/attack-navigator/#layerURL=https://raw.githubusercontent.com/mitre-attack/car/master/docs/coverage/es_analytic_coverage_12_30_2022.json, Generated 30 December 2022.
- Cyber Adversary Language and Decision Engine for Red Team Automation (CALDERA), caldera.mitre.org, Last accessed June 2023.
- CREF Navigator, MITRE, https://crefnavigator.mitre.org/about, Last accessed 20 April 2023.
- CRITs, MITRE, https://crits.github.io/, Last accessed 20 April 2023.
- CVE Page, MITRE, https://cve.mitre.org/, Last accessed 20 April 2023.
- Cyber Analytics Repository (CAR), https://car.mitre.org/, Last accessed, 6 June 2022.
- Detection, Denial, and Disruption Framework Empowering Network Defense (D3FEND™), MITRE, https://d3fend.mitre.org/faq/, Last accessed 20 April 2023.
- Diamond Model in Cyber Threat Intelligence, Chad Warner, https://warnerchad.medium.com/diamond-model-for-cti-5aba5ba5585, 17 December

2021.

- OASIS Cyber Threat Intelligence Technical Committee, OASIS Open STIX Version 2.1., https://docs.oasis-open.org/cti/stix/v2.1/os/stix-v2.1-os.html, Last accessed 17 June 2023.
- National Vulnerability Database, CVE Program, NIST, https://nvd.nist.gov/general/cve-process, Last accessed 20 April 2023.
- Structured Threat Information eXpression (STIX™) & Trusted Automated eXchange of Indicator Information (TAXII™), https://oasis-open.github.io/cti-documentation/, Last accessed June 2023.
- Kali, https://www.kali.org, Last accessed June 2023.
- Malware Attribute Enumeration and Characterization (MAEC™), https://maecproject.github.io/, Last accessed June 2023.
- MITRE Engage™ framework for planning and discussing adversary engagement operations that empowers you to engage your adversaries and achieve your cybersecurity goals, https://engage.mitre.org, Last accessed 20 April 2023.
- Enhanced CTI Sharing for Partner Organizations (ECHO), https://echo.mitre.org/, Last accessed June 2023.
- Sigma, a Generic Signature Format for SIEM Systems, SigmaHQ, https://github.com/SigmaHQ/sigma, Last accessed June 2023.



Therese Baisley

tbaisley@mitre.org

703-343-5814

All references provided in note pages or upon request

SOLVING PROBLEMS FOR A SAFER WORLD™