REPORT DOCUMENTATION PAGE	*Form Approved* *OMB No. 0704-0188*

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.
PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.

1. REPORT DATE *(DD-MM-YYYY)* 10/14/2022	**2. REPORT TYPE** Technical Paper	**3. DATES COVERED** *(From - To)*

4. TITLE AND SUBTITLE Cyber Risk to Mission Case Study: Norsk Hydro	**5a. CONTRACT NUMBER** W56KGU-18-D-0004
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S) BLAINE JEFFRIES; STEPHANIE SARAVIA; CEDRIC CARTER; ZACHARY ANKUDA;	**5d. PROJECT NUMBER**
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) The MITRE Corporation 202 Burlington Road Bedford, MA 01730	**8. PERFORMING ORGANIZATION REPORT NUMBER** PRS-22-3167
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) The Under Secretary of Defense for Research and Engineering	**10. SPONSOR/MONITOR'S ACRONYM(S)** OUSD(R&E)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

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

13. SUPPLEMENTARY NOTES

14. ABSTRACT

In March 2019, Norsk Hydro, one of the world’s largest aluminum suppliers fell victim to a cyberattack. The cyberattack deployed LockerGoga ransomware across the company’s corporate enterprise and control system networks. While the ransomware attack did not directly affect control systems, the Norsk Hydro incident still serves as a case study for the impact a ransomware attack can have on industrial operations given their reliance on IT systems.

15. SUBJECT TERMS

Network Security; Computer Security; cybersecurity; ATT&CK; malware

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Susan Carpenito
				6	**19b. TELEPHONE NUMBER** *(Include area code)* 781-271-7646

MITRE | SOLVING PROBLEMS FOR A SAFER WORLD®

Cyber Risk to Mission Case Study

BLAINE JEFFRIES, STEPHANIE SARAVIA, CEDRIC CARTER, ZACHARY ANKUDA

Category: Operational Technology
Critical Infrastructure Sector: Critical Manufacturing
Incident: Norsk Hydro

October 13, 2022

Figure 1: Aluminum Casting Process, *Norsk Hydro*

Approved for Public Release; Distribution Unlimited. Public Release Case Number 22-3167

The view, opinions, and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

This technical data deliverable was developed using contract funds under Basic Contract No. W56KGU-18-D-0004

© 2022 MITRE CORPORATION.

Cyber Risk to Mission Case Study

Category: Operational Technology
Critical Infrastructure Sector: Critical Manufacturing
Incident: Norsk Hydro

Executive Overview

In March 2019, Norsk Hydro, one of the world's largest aluminum suppliers fell victim to a cyberattack [1]. The cyberattack deployed LockerGoga ransomware across the company's corporate enterprise and control system networks. The ransomware rendered all Information Technology (IT) systems it encountered useless by encrypting user data, disabling network adapters, and changing login credentials [3]. Norsk Hydro elected not to pay the ransom demanded by the attackers and hired cybersecurity consultants to redesign and recover their networks. The aluminum manufacturer was coerced into operating manually to sustain operations. Uniquely, the company chose to remain transparent throughout their recovery which positively impacted their reputation [4]. While the ransomware attack did not directly affect control systems, the Norsk Hydro incident still serves as a case study for the impact a ransomware attack can have on industrial operations given their reliance on IT systems.

Incident

The Norsk Hydro ransomware attack was an adversarial incident attributed to an organized criminal group. This section provides additional information regarding the target, attribution, malware, and Tactics, Techniques, and Procedures (TTPs) employed. TTP, impact, and mitigation description references can be found within the MITRE ATT&CK® for ICS knowledge base available at the following web address: https://attack.mitre.org/matrices/ics/.

Target

IT systems located within both the enterprise and operational technology networks of Norway's largest public industrial company were targeted by ransomware. Norsk Hydro owns and operates hundreds of facilities across 40 countries and employs more than 36,000 personnel. Their industrial base covers every process required to create aluminum products, to include mining raw materials and operating hydroelectric power stations. The cyberattack targeted their global footprint which most significantly impacted their Extruded Solutions department – responsible for producing aluminum products that are pressed through a die [1].

Attribution

The ransomware attack targeting Norsk Hydro is attributed to the organized crime group FIN6. The group originally gained the attention of cybersecurity experts after deploying card swiping malware to point-of-sale environments. The crime group turns a profit by selling the stolen card information within darknet markets. Mandiant believes they shifted their tactics to target the engineering industry with ransomware. Their motive appears to be strictly financial, even though they are now targeting environments that impact safety systems [5].

Malware

The LockerGoga ransomware strain was employed by the adversary during the cyberattack against Norsk Hydro. In addition to traditional ransomware techniques such as file encryption, LockerGoga takes additional steps to increase the difficulty of system recovery. This ransomware strain logs off all users, disables all network adapters, and changes the local user and administrator passwords following encryption. A computer system infected with LockerGoga ransomware is rendered completely useless [3].

The Norsk Hydro cyberattack was not the first identified sample of the LockerGoga malware. In fact, the strain was linked to three previous cyberattacks targeting other industrial organizations (i.e., Altran Technologies, Hexion, and Momentive) just months earlier. This suggests that Norsk Hydro was one target in a larger criminal campaign focused on industrial organizations [4].

Tactics, Techniques, and Procedures

Spearphishing Attachment (T0865)

Initial access was gained via a weaponized email attachment [4].

Valid Accounts (T0859) & Privilege Escalation (TA0004)

Attackers were able to capture admin credentials to escalate their privileges ultimately to domain admin [4].

Command and Control (TA0011)

With captured domain admin credentials, the attackers were able to deliver and activate the ransomware across the enterprise using Microsoft Active Directory [4].

Response

Operations personnel within Norsk Hydro facilities were the first to detect the cyberattack as their computer systems were rendered unusable. Front line workers notified headquarters of their system faults. Shortly thereafter, the company assessed the extent to which its internal networks were infected with the ransomware. They decided to shut down and isolate their entire IT infrastructure to cut adversary access and prevent further damage. The organization then reverted to conducting operations manually without IT system support, which consequently slowed and even halted operations in some instances. Personnel began pulling reference manuals and documentation out of filing cabinets, calling in retired employees, and doing everything by hand for weeks before they were able to gradually bring IT equipment back online [2].

As previously discussed, Norsk Hydro opted not to pay the ransom demanded by the attackers, but instead hired a range of cybersecurity consultants to redesign and recover their networks from the ground up. Norsk also restructured their security team following the cyberattack to better detect and respond to incidents. Uniquely, the company chose to remain transparent throughout their recovery which positively impacted their reputation [1].

Outcome

Loss of Availability (T0826) & Loss of Productivity and Revenue (T0828)

In total, the cyberattack compromised 160 company sites hosting more than 20,000 systems. The compromised host systems were rendered completely unusable. The LockerGoga ransomware encrypted all user data on the drive, disabled network capabilities, and changed login credentials. Norsk Hydro was able to continue production, but in a limited fashion directly following the cyberattack. Consequently, in their annual report, Norsk Hydro reported an estimated loss of 67-84 million dollars (USD) [1]. Furthermore, sources indicate it took Norsk Hydro several months to regain full operational capability.

Prognosis and Recommendations

The Norsk Hydro ransomware incident serves as a case study for the wide-reaching impacts a ransomware attack can have given an organization’s reliance on Information Technology (IT) systems. Furthermore, Norsk Hydro’s decision to not pay the ransom provides a more realistic timeline to recovery should critical government systems fall victim to a similar cyberattack. While attackers failed to procure direct financial gain from the cyberattack, they have proven that commodity IT malware can have lasting mission impact. Our nation’s adversaries without financial motive could deploy similar capabilities to disrupt critical missions and operations. To that end, this section provides recommendations aligned with the Cyber Risk to Mission Defense in Depth layers.

Defense in Depth Layer 1: Incident Deterrence

Vulnerability Scanning (M0916), Update Software (M0951), Network Intrusion Prevention (M0931), User Training (M0917)

Mission owners can deter adversaries from conducting a ransomware attack on their systems by reducing their attack surface and hardening existing IT infrastructure. Hardening is the process of securing a system by reducing its surface area to attacks and vulnerabilities. Mission owners must understand the different vectors an adversary can exploit to gain initial access and influence those opportunities. They must also be diligent to update and patch existing IT infrastructure in a timely manner. Organizations can reduce the effectiveness of spearphishing and social engineering attacks by spreading awareness through user training. Lastly, victims of a ransomware attack should not pay the ransom. Paying the ransom does not guarantee the systems will be recovered and only emboldens the adversaries to continue to deploy ransomware on vulnerable networks.

Defense in Depth Layer 2: Remediations

Data Backup (M0953), Redundancy of Service (M0811)

Mission owners can reduce the time to recover from a ransomware attack by ensuring redundancy (backups) in operations to recover impacted systems. Backing up critical systems, servers, and data ensures services can be restored in a timely manner. It is vital that backup files are stored in an isolated environment separate from the operational infrastructure, preferably offline. If not, adversaries may access and compromise the backup files as part of their campaign. Depending on the system and its requirements, programs should decide between a hot or cold backup to continue operations.

Defense in Depth Layer 3: Restoration Mitigations

Mission owners need to maintain and regularly exercise recovery plans, ensuring that backups are readily available, verifiable, and current. Local operators and administrators must understand the intricacies of restoring mission critical assets, preferably through on-the-job training and exercises. Proper preparation will ensure services are restored in a timely manner with minimal operational impact.

Defense in Depth Layer 4: Consequence Mitigations

Organizations should be prepared to execute their critical missions and essential tasks with limited or no support from IT infrastructure. While implementing a recovery plan is vital to restore asset functionality after compromise, maintaining mission operations during restoration is equally important. In practice, cyber incident response planning for Operational Technology (OT) environments should include contingency operations for partial and complete IT equipment failure. Operational training plans should include training on primary operational systems as well as redundant systems, manual operations, and alternate operating locations. Training should include simulated loss of control and loss of view scenarios. Manual operations and access to offline documentation were critical to reducing the consequence of the Norsk Hydro cyberattack while restoration activities were ongoing.

Defense in Depth Layer 5: Mission Agility

Mission owners must understand the impact IT system compromise will have on the critical infrastructure supporting operations. In doing so, stakeholders can accurately inform contingency operations through mission dependency analysis. IT systems and supporting critical infrastructure will fail to meet mission requirements due to commodity malware attacks like ransomware. However, by resourcing threat informed scenario development today, decision makers will be able to rapidly adapt to adversary action, increasing survivability and decreasing mission impact during future cyberattacks.

References

[1] Norsk Hydro ASA. (n.d.). *Hydro Annual Report 2019*. https://www.hydro.com/Document/Doc/Annual%20report%202019%20web.pdf?docId=550643

[2] Norsk Hydro ASA. (2019, Apr 2). *Cyber attack on Hydro Magnor* [Video]. https://www.youtube.com/watch?v=S-ZlVuM0we0

[3] Beaumont, K. (2019, Mar 21). *How Lockergoga took down Hydro – ransomware used in targeted attacks aimed at big business*. DoublePuslar. https://doublepulsar.com/how-lockergoga-took-down-hydro-ransomware-used-in-targeted-attacks-aimed-at-big-business-c666551f5880

[4] Hotter, A. (2019, Aug 22). *How the Norsk Hydro cyberattack unfolded*. American Metal Market. https://www.amm.com/Article/3890250/How-the-Norsk-Hydro-cyberattack-unfolded.html

[5] McKeague, B., Ta, V., Fedore, B., Ackerman, G., Pennino, A., Thompson, A., & Bienstock, D. (2019, Apr 5). *Pick-Six: Intercepting a FIN6 Intrusion, an Actor Recently Tied to Ryuk and LockerGoga Ransomware*. Mandiant. https://www.mandiant.com/resources/pick-six-intercepting-a-fin6-intrusion

Additional Reading

Slowik, J. (2020). *Spyware Stealer Locker Wiper: LockerGoga Revisited*. Dragos. https://www.dragos.com/resource/spyware-stealer-locker-wiper-lockergoga-revisited/

Briggs, B. (2019, Dec 16). *Hackers hit Norsk Hydro with ransomware. The company responded with transparency*. Microsoft News. https://news.microsoft.com/transform/hackers-hit-norsk-hydro-ransomware-company-responded-transparency/

Harbison, M. (2019, Mar 26). *Born This Way? Origins of LockerGoga*. Palo Alto. https://unit42.paloaltonetworks.com/born-this-way-origins-of-lockergoga/

Austin, P. (2021, Jul 14). *This Company Was Hit with a Devastating Ransomware Attack—But Instead of Giving In, It Rebuilt Everything*. Time Magazine. https://time.com/6080293/norsk-hydro-ransomware-attack/

Related Incidents

Colonial Pipeline (May 2021)

In May 2021, the Colonial Pipeline Company halted all pipeline operations to limit the effect of a ransomware attack that compromised its IT systems. It took 5 days before Colonial Pipeline was able to safely restart their pipeline system. 10 days following the halt they reported that had regained full operational capability. The company admitted in submitting to attacker demands, paying a ransom of roughly $4.5 million USD.

Sources

Colonial Pipeline. (2021, May 17). *Media Statement Update: Colonial Pipeline System Disruption.* Colonial Press Release. https://www.colpipe.com/news/press-releases/media-statement-colonial-pipeline-system-disruption

Parfomak, P. & Jaikaran, C. (2021, May 11). *IN11667 Colonial Pipeline: The DarkSide Strikes.* Congressional Research Service. https://crsreports.congress.gov/product/pdf/IN/IN11667

Belarusian Railway (Jan 2022)

In January 2022, a group of political activists breached a national railway network and deployed ransomware. The group self-identified as Belarusian Cyber-Partisans and demanded the release of 50 political prisoners as ransom payment. The railway was actively being used by the Russian military in preparations for a potential invasion of Ukraine. A former employee of the Belarusian Railway detailed that the attack had a serious impact on their automated systems ranging from "*payroll to cargo manifests to timetables*".

Sources

Hurnievic, D. (2022, Jan 29). *'It was a Serious Blow': Ex-Belarusian Railways Worker says Officials Downplaying Consequences of Cyberattack.* RFERL. https://www.rferl.org/a/belarus-railways-cyberattack-consequences/31677443.html

Greenberg, A. (2022, Jan 25). *Why the Belarus Railways Hack Marks a First for Ransomware.* Wired. https://www.wired.com/story/belarus-railways-ransomware-hack-cyber-partisans/