DM20-0957

Script: Ransomware: Evolution, Rise, and Response
SME: *Marisa Midler and Tim Shimeall*
Moderator: *Suzanne Miller*
Interview Conducted*:* Thursday, October 15, 2020 at 11 a.m. ET

Suzanne Miller: [At Camera] Hi, my name is Suzanne Miller. I am a principal researcher here at the Software Engineering Institute. Today I am joined by Marisa Midler and Tim Shimeall, both analysts within the SEI's CERT Division.

Today we are here to discuss their latest work in ransomware, which we have seen a spike in over the last year, both in the number of ransomware cases and their severity.

Welcome to Marisa and Tim.

Marisa and Tim: Respond. (Brief Hello)

- Hello, my name is Marisa Midler and I am an analyst in the Situational Awareness team within the SEI's CERT division.

1. **Suzanne:** Tell us a little bit about yourselves and the work that you do here at the SEI. What forces led you down the path to studying ransomware?

   Marisa and Tim: **Respond.**
   - **The CERT Situational Awareness team (in brief)**
   - Analyzing current data and supporting network security in organizations: traffic analysis, security technique development and application, threat assessment
   - Diverse background on the team to provide multifaceted expertise

- Marisa's Background
  (I worked as a software engineer for a bit and went back and got my master's from CMU in Information Security Policy and Management. I'm a bit of a generalist and I've worked on an assortment of projects during my time here at the SEI from developing web applications using Django and Docker

to iOS security research to some operations and virtualization work and of course research on ransomware.

- **Ransomware interest came from awareness of the impact it has on a large variety of organizations**
  Concern both for specific organizations and for the impact this malware is having in general

  - As Tim mentioned, Situational Awareness explores a diverse set of areas. The drive behind this research is the fact that organizations are still being affected by ransomware attacks and the impact of these attacks is significant.
  - Additionally, the ransomware attack behaviors have also changed over the past years and it's important to get information out on the new behaviors.

2. **Suzanne:** It's not an understatement to say that ransomware cases are on the rise.

   The New York Times reported earlier this month [October 2020] that a woman died from treatment delays after a hospital in Germany that was hit by a cyberattack was forced to turn away emergency patients. A coronavirus vaccine trial was also bogged down in recent weeks when researchers were locked out of their data.

   In your own SEI blog posts published in recent weeks on ransomware, you have talked about the spike in cases.

What’s going on? What’s behind this increase in ransomware attacks?

Marisa and Tim: Respond.

- **The motivation behind ransomware attacks is predominantly financial.** The cyber criminals are looking for the easiest way to make money and ransomware attacks have proven to be an effective means.
- **This past April at RSA 2020, Supervisory Special Agent Joel DeCapua presented research that tracked Bitcoin wallets associated with ransomware variants and found victims paid over $140 million in ransoms from 2013-**2019. This is just in ransoms and does not include incident response and recovery costs. Ryuk was at the top of the list and collected $61 million in ransoms.
  - **It’s also worth noting that the actual ransom payment amounts are actually higher because the FBI did not have access to all the ransom notes and Bitcoin wallets.**
- That being said, over the past year the ransoms demanded have significantly increased. The average ransom payment in Quarter 3 of 2019 was roughly $42,000 and in Quarter 1 2020 the average ransom payment jumped to roughly $112,000. Which is about $70,000 more.

- The number of attacks increased by 25% from Quarter 4 2019 to Quarter 1 2020 and we expect that ransomware attacks are going to continue to increase.
- Ransomware has proven to be a lucrative means for the cyber criminals to make money and they are only increasing their efforts and evolving their strategies.

3. **Suzanne:** Marisa, in one of your blog posts, you explored the evolution of Ransomware-as-a-Service. Explain for us what Ransomware-as-a-Service is and the role that it has played in this recent spike in the number of attacks.

Marisa and Tim: Respond.

- **Ransomware as a Service is a new business model for ransomware developers.** The ransomware developers sell or lease their ransomware variants to other cybercriminals who then use the ransomware to perform attacks. This lowers the risk for ransomware developers since they no longer need to perform attacks to make money and Ransomware as a Service makes ransomware usable by non-technical people.
- **The appeal to use ransomware to make money is already established. Potential ransomware attackers can see the payoff by how many organizations end up paying the ransoms. Ransomware as a Service lowers the barrier to entry and cyber criminals no longer need to develop their own ransomware variants to perform attacks; they can pay to use an already existing ransomware variant.**

- **Making ransomware accessible to non-**technical cybercriminals drastically increases the threat landscape by increasing the number of potential attackers. And more attackers typically means more attacks.

4. **Suzanne:** Federal agencies, including the FBI, do not support paying ransom in the event of a ransomware attack, which has been hard for many victims who feel like they have limited options. What steps can organizations take both to prevent a ransomware attack and, worst case scenario, respond to one once it has been executed?

   Marisa and Tim: Respond.
   Tim: paying ransom is a poor response, since it both rewards the attackers and about 60% of the time does not result in organizations getting their data back. However, after a successful compromise some organizations may have little choice. If an organization is prepared for these attacks, much more attractive options are available: pre-emptive options that make common entry options less available for attackers (specifically, phishing defenses and RDP security), damage mitigation defenses (such as encrypting data at rest, so that attackers cannot easily threaten disclosure of confidential data), and recovery (such as using your own validated backups, instead of paying the ransom).

I think it's also worthwhile to mention the data exfiltration behavior of ransomware. In November 2019, criminals using the Maze ransomware exfiltrated data from Allied Universal and sent a ransom demanding payment or they would publish the data online. The payment deadline came and went, and the attackers followed through with the threat and published 700MB of Allied Universal's data online. And more ransomware variants have adapted to this tactic and published victim data online.

- **Orgnaizations should know what their High Value Assets and Data are.**
- At this time, the only reasonable mitigation against this data exfiltration ransomware behavior is to strongly encrypt data at rest. If your organization might justify paying a ransom for specific data, you should probably encrypt it.

5. **Suzanne:** As a federally funded research and development center, our role is to serve as an honest broker of information. We anticipate and try to solve these hard problems and then convey these solutions to the government.

   What is the SEI doing to try to solve the problem of ransomware? What resources have you developed, and where can our audience locate them?

   Marisa and Tim: **Respond. (Series of reports; situational awareness tools; insider threat insight into fighting**

phishes; ongoing engagement)

Technical report: Current Ransomware Threats
Blog posts: The blog posts are great because the also link to both SEI resources as well as external sources to get additional information depending on your interest.

- **Ransomware as a Service Threats**
- Ransomware Prevention Defense Priorities

6. **Suzanne:** What is next for you both in this arena? How do you see ransomware evolving?

Marisa and Tim: Respond. (Further tracking and information, advanced tooling and more targeted detection techniques, exploiting multi-sorted data collection) Ransomware is persistent. As long as it is making money for the attackers, they will use it. The affiliate structure allows developers to innovate with little risk. Evolving will likely focus on clouds, common storage technologies, and in defeating defensive protection of data.

Something of interest is there are some cloud organizations that are beginning to support data immuntable backups so the backup cannot be modified, deleted, or encrypted.

Suzanne: Thanks for being here and talking about this work. [Turns to Camera] And to our listeners, we will include links in our transcript to all resources mentioned in this podcast. Thanks for joining us today.

Pre-recorded Outro.