Prepared Statement
Charles Carmakal, Senior Vice President and Chief Technology Officer
FireEye Mandiant
Before the United States House Committee on Energy and Commerce
Subcommittee on Oversight and Investigations
July 20, 2021

Introduction

Chairwoman DeGette, Ranking Member Griffith, and Members of the Subcommittee, thank you for the opportunity to share our observations and experiences regarding this important topic, as well as for your leadership on cybersecurity issues. My name is Charles Carmakal and I am a Senior Vice President and Chief Technology Officer at FireEye Mandiant ("Mandiant").

We commend the Subcommittee for holding this hearing to further examine recent ransomware and multifaceted extortion events. Both governmental and corporate responses to these attacks continue to evolve, and the Subcommittee plays an important role in overseeing these efforts.

As requested by the Subcommittee, I am going to discuss the ransomware landscape, including the threat actors, motivations, general aspects of this criminal enterprise, and recommendations for what organizations should do to mitigate this threat.

Background

In my role at Mandiant, I oversee a team of security professionals that help organizations respond to complex security breaches orchestrated by foreign governments and organized criminals. My team and I have had the opportunity to help organizations across the globe deal with some of the most significant and catastrophic cybersecurity incidents in history.

Mandiant employees are on the front lines of the cyber battle, actively responding to computer intrusions at some of the largest organizations on a global scale. We employ more than 1,000 cybersecurity experts in over 25 countries, with skills in digital forensics, malware analysis, intelligence collections, threat actor attribution, and security strategy and transformation. Over the last 17 years, we have responded to thousands of security incidents. It is unfortunate, but we receive calls almost every single day from organizations that have suffered a cybersecurity breach. For the security incidents we respond to, our mission is to help our clients investigate the attack, contain the incident, eradicate the attackers, guide them through the recovery of their environments, and help them become more resilient to future attacks.

Ransomware Overview

Ransomware is the most prolific cybersecurity threat today. Financially motivated threat actors primarily monetize their cyber intrusions by deploying ransomware and conducting multifaceted extortion. Organizations across all sectors and sizes are impacted. In the earlier days of ransomware, around 2013, ransom demands were low, often under $1,000. As the years progressed, around 2015, a threat group by the name of SamSam started asking for ransom demands around $20,000. Today, victim organizations are often coerced to pay six, seven, and

eight-figure extortion demands to recover business operations and mitigate the disclosure of stolen sensitive information. Many high-profile cyber intrusions over the past few years have involved ransomware and multifaceted extortion.

The term ransomware refers to the software used by threat actors to encrypt data on victim computers. It is also called a "ransomware encryptor." However, the industry often uses the term "ransomware" to describe any cybersecurity incident that involves extortion or destruction, even when ransomware encryptors were not used.

Many ransomware operations are run as a "Ransomware as a Service." This means there are different groups responsible for different functions. As an example, one group may be responsible for building ransomware encryptors and maintaining the victim shaming websites. Another group may be responsible for phishing employees and obtaining the initial access into a victim environment. Another group may be responsible for conducting the hacking actions within a company network, stealing data, and deploying the ransomware encryptor. The extortion payments are divided up between the groups involved. Ransomware as a Service lowers the barrier to entry for criminals that want to get started in ransomware.

The Evolution of Disruptive Intrusions: Ransomware to Multifaceted Extortion

In 2015, Mandiant observed a notable surge in disruptive intrusions in which threat actors deliberately destroyed critical business systems, leaked confidential data, taunted executives, and extorted organizations. We anticipated that intrusions would become more disruptive over time given the high impact and low cost to threat actors. Over the next few years, financially motivated threat actors began shifting away from stealing payment card information to deploying ransomware. Threat actors asked for ransom payments in exchange for the key to decrypt their data.

In late 2019, a hacking group by the name of Maze changed the way financially motivated threat actors would conduct their intrusions. Maze would find and steal sensitive corporate and customer information in addition to encrypting data on systems. They launched a website to publicly shame the victim organizations that they compromised and publish the stolen information. They would demand money in exchange for tools to recover the data that they encrypted, a promise to not publish the data they stole, and details of how they compromised the organization. The shaming site served as a warning to those who did not comply. Extortion demands were often in the six- and seven-figure ranges, but sometimes went up to eight-figures. Shortly after, many other cyber-criminal groups followed suit. There is a distinct upward trend in both the number of victims that have appeared on these victim shaming sites and the number of groups using this methodology to pressure victims.

Last October, the cyber threat in the United States reached an unprecedented level. Hospitals across the U.S. were disrupted by a group of eastern European threat actors. Hospital technology systems were taken offline, and medical professional and administrative staff had to rely on paper and pen to record data. Many hospitals had to divert patients and ambulances to emergency departments at other hospitals. The impact of cyber intrusions to human lives has never been more dire.

Most of today's intrusions by financially motivated threat actors involve multifaceted extortion. Threat actors will apply immense pressure to coerce victims to pay substantial extortion demands – often in the seven to eight-figure range. Some threat actors will convince news and media organizations to write embarrassing stories about victims. They may call and harass employees. They may notify business partners that their data was stolen due to a breach of their partner, creating friction in business relationships. They may also conduct denial of service attacks to create further chaos and disruption.

Ransomware and multifaceted extortion events have reached an intolerable level and we must come together as a community to defend our nation.

Extortion Payments – Considerations for Paying

Mandiant does not negotiate with threat actors or pay extortion demands on behalf of our clients. Nor do we make recommendations or provide advice on how to respond to such demands. However, we are often asked to help executives and board members evaluate their options with respect to recovering from disruptive intrusions. We advise our clients to discuss with their outside counsel and to think through several considerations before deciding whether or not to comply with extortion demands.

Some of the considerations are outlined below:

1. **How quickly can you recover your systems and data on your own?**
   Organizations may not be able to recover their systems and data on their own. This could be due to not having mature backup processes or the threat actor destroying their backups. Often, organizations have good backups, but the restoration process is slow due to the volume of systems that were encrypted and need to be recovered.

2. **How reliable is the threat actor?**
   Many threat actors recognize their business model requires them to be reliable and credible. If a victim paid a threat actor, and the threat actor did not provide a working decryption tool or published stolen data anyway, the threat actor would develop a negative reputation. This would decrease the likelihood of them being paid by other victims in the future.

3. **Did the threat actor steal data before they deployed their encryptors? How sensitive is the data that they stole?**
   Nowadays, most threat actors steal large volumes of sensitive data from victim organizations. Many organizations feel compelled to pay not because they need tools to recover their data, but because they feel obligated to do everything they can to protect their customer and partner data.

4. **Does the threat actor still have active access to your network?**
   Threat actors almost always establish multiple backdoors into victim environments, enabling them to escalate their attacks if they do not get paid.

5. **Will cybersecurity insurance cover the claim?**
   Cybersecurity insurance helps many organizations recoup some of the cost associated with the painful decision of paying threat actors.

6. **Is the threat actor sanctioned by the U.S. Department of Treasury?**
   Paying sanctioned threat actors is illegal and organizations need to take appropriate actions to ensure that they do not pay a sanctioned entity. This usually requires support from firms or third party experts and law enforcement.

Extortion Payments – What Have we Observed When Victims Pay?

There are many assumptions about what happens when a victim organization pays a threat actor. Here is a summary of observations based on hundreds of incidents that Mandiant has investigated:

1. **Threat actors usually deploy multiple backdoors within victim environments**.
   Unless the backdoors are removed and incident containment and remediation steps are taken, the threat actor may have the ability to re-compromise the environment. If a victim chooses to pay the threat actor, they must also take steps to block their access and eradicate them from the environment. This may require investments in cybersecurity tools, processes, and people.

2. **Many threat actors provide working decryption tools when they are paid.**
   Threat actors realize their business model requires them to provide positive outcomes to victim organizations, or they would develop a negative reputation and they would not be paid in the future. Threat actors often provide decryption tools that work, however, the decryptors often have unintentional bugs that may not effectively decrypt every single file. Additionally, many decryptors are slow.

3. **Many threat actors do not publish stolen data when they are paid.**
   Some threat actors may provide proof that they discarded the data they stole if they are paid, however, there is no guarantee that the proof was authentic, or they don't have other copies of the data. Prior to 2019, we observed many threat actors that publicized stolen data and re-extorted victims after being paid. Over the next 24 months, Mandiant anticipates some threat actors will re-extort victims and publish stolen data at a later time, despite being paid.

4. **Many threat actors don't re-compromise entities that paid them.**
   Today, threat actors can opportunistically compromise other organizations easily. They often move on to the next target when they are paid.

Recommendations for Organizations to Mitigate the Risk of Ransomware and Multifaceted Extortion Events

In September 2019, Mandiant published a technical whitepaper[1] outlining the most common and high priority steps Mandiant incident responders use to help organizations respond to and contain ransomware events. The document provides detailed recommendations that organizations should implement immediately following a ransomware event – or ideally before a ransomware event – to limit the impact. It includes detailed tactical recommendations for endpoint hardening, credential exposure and usage hardening, Windows domain controller isolation and recovery planning, and Windows Group Policy Object (GPO) permissions and monitoring.

Conclusion

On behalf of FireEye Mandiant, I thank you for this opportunity to testify before the Subcommittee. The ransomware and multifaceted extortion challenge has become so prolific and dire, that we should no longer view it as a mere nuisance or business risk—we should consider it a significant threat to global security. The number of attacks continues to rise at an alarming rate. We stand ready to work with you and other interested parties to devise effective solutions to deter malicious behavior in cyberspace and to build better resiliency into our networks.

[1] https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/wp-ransomware-protection-and-containment-strategies.pdf