Prepared Statement
Charles Carmakal, Senior Vice President and Chief Technology Officer
FireEye-Mandiant
Before the United States House Committee on Homeland Security
June 9, 2021

Introduction

Chairman Thompson, Ranking Member Katko, and Members of the House Homeland Security Committee, 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 Committee for holding this hearing to further examine the recent ransomware attack against Colonial Pipeline. Both governmental and corporate responses to the attacks continue to evolve, and the Committee plays an important role in overseeing these efforts.

As requested, I am going to share our observations of the threat actor associated with the ransomware attack against Colonial Pipeline and discuss the cybersecurity threats to organizations in the United States.

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 over 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 tens of thousands of security incidents. It is unfortunate, but we receive calls almost every single day from organizations that have suffered a cybersecurity breach. For every security incident we respond to, our mission is to help our clients investigate the attack, contain the incident, eradicate the attackers, guide our clients through the recovery of their environments, and help them become more resilient to future attacks.

The Cyber Intrusion into Colonial Pipeline

On the early morning of May 7, 2021, Mandiant was engaged by Hunton Andrews Kurth LLP, on behalf of Colonial Pipeline, to help respond to the ransomware event that was discovered earlier that day. Prior to that date, Mandiant had not provided cybersecurity consulting services to Colonial Pipeline. Shortly after being called on the morning of May 7th, we mobilized a team of experienced incident responders and information technology and operational technology security experts to help Colonial Pipeline investigate and contain the incident, eradicate the threat actor, and further enhance the security posture of the network to facilitate the safe restart of the pipeline. Additionally, Mandiant is advising Colonial Pipeline on ways to become more resilient to cyber attacks in the future.

The earliest evidence of compromise that we have identified to date occurred on April 29, 2021. On that date, the threat actor had logged into a virtual private network (VPN) appliance using a legacy VPN profile and an employee's username and password. The legacy VPN profile did not require a one-time passcode to be provided. The legacy VPN profile has since been disabled as part of Colonial Pipeline's remediation process.

The Evolution of Disruptive Intrusions: Ransomware to Multifaceted Extortion

Cyber intrusions have become increasingly disruptive over the past decade. Every year, Mandiant publishes an annual report, M-Trends, which covers the cybersecurity trends we observed from our breach investigations.[1] 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 malicious software that encrypts data on systems, commonly referred to as ransomware. Threat actors asked for ransom payments in exchange for the software that would enable victim organizations to recover their encrypted data.

In late 2019, a hacking group by the name of Maze changed the way threat actors would conduct their intrusions. Prior to deploying ransomware across victim environments, they would look for and steal sensitive corporate information. They launched a website where they would publicly shame the victim organizations that they compromised and publish the data that they stole. 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. Extortion demands were often in the six- and seven-figure ranges, but sometimes went up to eight-figures.

Last October, the cyber threat in the United States reached an unprecedented level. Hospitals across the United States 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.

The majority 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 7 to 8-figure range. Some threat actors will convince news and media organizations to write embarrassing stories about victims. They may call and harass

[1] M-Trends, https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html

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 help organizations defend their networks.

The DarkSide Threat Group

DarkSide is a ransomware service that enables a network of different groups to conduct cyber intrusions under the name "DarkSide." Like many other financially motivated threat actors, the criminals affiliated with the DarkSide service conduct multifaceted extortion schemes to coerce victims into paying large extortion demands. They exfiltrate victim data, deploy DarkSide ransomware encryptors, and threaten to publish stolen data to their victim shaming website. Since initially surfacing in August 2020, they have launched a global crime spree affecting organizations in more than 15 countries and multiple industry verticals.

DarkSide operates as a ransomware-as-a-service (RaaS) wherein profit is shared between its owners and partners, or affiliates, who provide access to organizations, steal sensitive victim data, and deploy the ransomware encryptors. Mandiant currently tracks multiple threat groups that have conducted these intrusions, some of whom have also worked on behalf of ransomware services besides DarkSide. These groups demonstrate varying levels of technical sophistication throughout intrusions.

Mandiant has identified multiple DarkSide victims through our incident response engagements and from reports on the DarkSide victim shaming website. Most of the victim organizations were based in the United States and span across multiple sectors, including financial services, legal, manufacturing, professional services, retail, and technology.

Following the security incident at Colonial Pipeline and the FBI's public attribution to DarkSide, Mandiant has observed multiple actors cite a May 13, 2021 announcement that appeared to be shared with DarkSide RaaS affiliates by the operators of the service. This announcement stated that they lost access to their infrastructure, including their blog, payment, and content distribution network (CDN) servers, and would be closing their service. The post cited law enforcement pressure and pressure from the United States for this decision. Multiple users on underground forums have since come forward claiming to be unpaid DarkSide affiliates, and in some cases privately provided evidence to forum administrators who confirmed that their claims were legitimate. We have not seen evidence suggesting that the operators of the DarkSide service have resumed operations.

Operational Technology (OT) and Industrial Control Systems (ICS) Security

Operational Technology (OT) and Industrial Control Systems (ICS) are responsible for managing and monitoring the industrial equipment, machines, and processes. They facilitate the generation and distribution of power, operations of manufacturing plants, and transportation of people and products. To mitigate the risks associated with OT environments, organizations segment their OT environments from IT environments (i.e., the environment that supports email, web browsing, and other business processes).

There have been relatively fewer publicly disclosed intrusions of OT environments as compared to IT environments, but the impact can be exponentially more significant. Some of the most notable incidents include the disruption of power distribution in Ukraine in 2015 and 2016, the development of malware that could manipulate safety control systems that was used against an organization in the middle east in 2017, and an attack on a Florida water treatment plant in 2021.

Conclusion

On behalf of Mandiant, I thank you for this opportunity to testify before the Committee. 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.