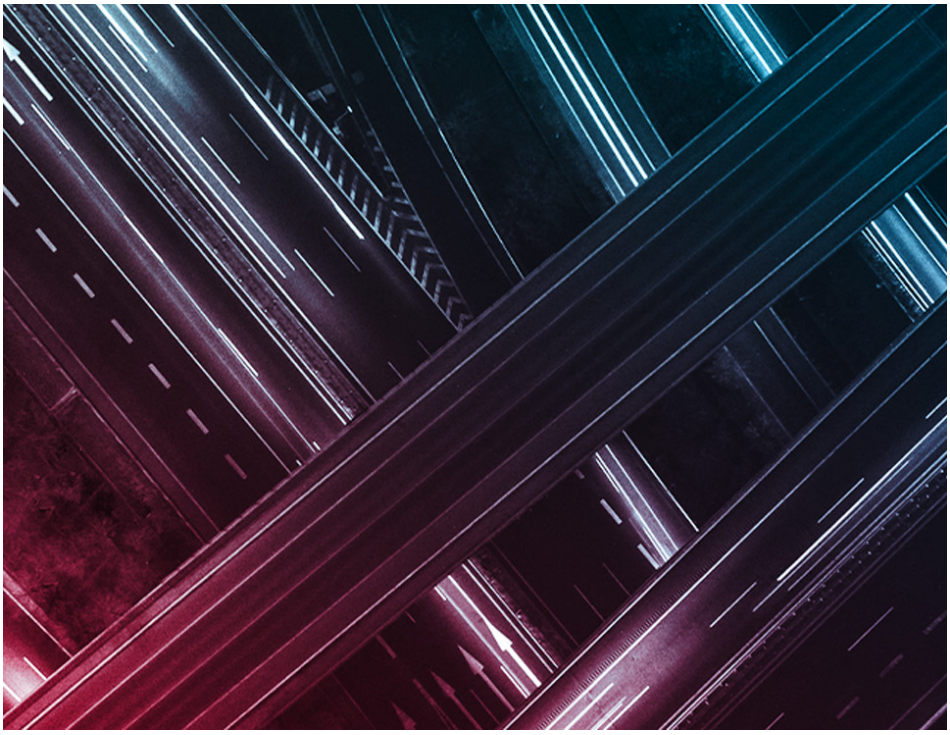
White Paper

Symantec
A Division of Broadcom

Attacks Against Critical Infrastructure: A Global Concern

By Threat Hunter Team

Table of Contents



Introduction

Cyber attacks on Critical National Infrastructure (CNI) have always been a major concern due to the immense disruption they have the potential to cause. The interruption of power, water, or transportation systems can have a major impact on ordinary citizens and put huge pressure on organizations and governments to restore systems quickly.

The Stuxnet attack on the Iranian nuclear enrichment program that was discovered in 2010, an attack on the power grid in Ukraine in 2015, and the recent attack on the Colonial Pipeline in the U.S., are just some of the high-profile incidents affecting CNI that have been publicly reported. Cyber attacks on power grids can cause anxiety due to the potential negative impacts they can have on ordinary citizens: the attack in Ukraine occurred in December, cutting out power and heat for citizens in the middle of Europe's winter. Thankfully, in that case, power was restored reasonably quickly, but the fact that attackers were able to gain access to the power grid to shut it down in the first place was a cause for significant concern.

The recent Colonial Pipeline attack in the U.S. also caused a huge reaction, leading to people stockpiling gasoline amid fears of a fuel shortage. In a world where almost all systems are internet connected to some degree, good cyber security in CNI has never been more important.

This paper will look at some of the most high-profile cyber attacks on CNI we have observed, including the Colonial Pipeline attack, and some previously unpublished research into an attack campaign aimed at some CNI infrastructure in a South East Asian country.

We will also look at what Symantec data tells us about malicious activity aimed at the CNI sector, and the steps you can take to help protect your organization.

Some of the key points covered in this paper:

- The Colonial Pipeline incident and other recent attacks have underlined the disruptive potential of ransomware for CNI and the pressure that can be exerted on organizations to pay ransoms in an effort to restore essential services quickly, making them a prime target for ransomware criminals.
- Attacks on CNI are a global issue, with high-profile incidents having occurred in the U.S., Europe, and the Middle East.
- Symantec data indicates that an increasing number of malicious actors are attempting to attack CNI organizations, but the number of attackers successfully installing malware on the endpoint in the sector is trending down.
- Attacks on CNI can be hard to contain or keep under wraps for affected businesses, leading to potential damage to business reputation as well as major effects on ordinary citizens. This was demonstrated in both the Colonial Pipeline and Ukraine power grid attacks.
- A comprehensive cyber security strategy with the implementation of policies like network segmentation, Zero Trust, and multi-factor authentication is essential for businesses in this sector, particularly in order to keep production networks safe even if corporate networks become infected.
- Malicious actors targeting this sector use living-off-the-land tools and techniques, as well as malware, to target and infect victims.
- Though rare, we have seen both destructive attacks and attacks with physical impact aimed at organizations in the CNI sector, so this is something companies in this sector need to be aware of. Due to the wide impact disruption of organizations in this sector can have, organizations need to be aware they could be the subject of attacks from highly skilled, nation-state-backed malicious actors.

Methodology

Critical National Infrastructure (CNI) is a broad sector that encompasses a number of different industries. The Cybersecurity and Infrastructure Security Agency (CISA) lists 16 critical infrastructure sectors "whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof." This includes the following:

- Healthcare and Public Health
- Financial Services
- Food and Agriculture
- Transportation Systems
- Information Technology
- Government Facilities
- Emergency Services
- Dams
- Communications
- Chemical
- Commercial Facilities
- Critical Manufacturing
- Defense Industrial Base
- Energy
- Nuclear Reactors, Materials, and Waste
- Water and Wastewater Systems

However, given the size of some of these sectors, for the purposes of this paper we will be concentrating primarily on a subset of these sectors, including the following:

- Energy Sector
- Dams
- Chemical
- Nuclear Reactors, Materials, and Waste
- Water and Wastewater Systems
- Critical Manufacturing
- Transportation Systems
- Commercial Facilities

Colonial Pipeline: U.S. Infrastructure Under Attack

On May 7, 2021, Colonial Pipeline, one of the biggest fuel pipelines in the U.S., providing 45% of the fuel consumed on the East Coast, was forced to shut down operations following a ransomware attack.

The finger of blame for this incident was quickly pointed at a group called Darkside (aka Coreid), a ransomware-as-a-service operation that is widely believed to operate from Eastern Europe. This attack attracted a huge number of headlines in the U.S. and around the globe, a response from the White House, and, seemingly, the shutdown of the operations of the ransomware gang responsible.

The Attack

The Colonial Pipeline is 5,500 miles long, travels through 14 states and is responsible for providing almost half of the fuel supply of the East Coast of the U.S. Its shutdown caused alarm among residents of eastern and southeastern states of the U.S., with fears that a prolonged shutdown could lead to fuel shortages and price hikes. The level of panic was such that there were reports of gas stations running out of fuel, and people going so far as to fill plastic bags with gasoline.

In a statement about the attack, Colonial said it temporarily shut down all its pipeline operations after learning it had been hit by a cyber attack on some of its "information technology" systems. The firm said it "proactively took certain systems offline to contain the threat."

The seriousness of the attack was underlined when the government invoked emergency powers in response to the hack. The Department of Transportation issued an emergency declaration on May 9 in response to the incident to relax regulations for drivers carrying gasoline, diesel, jet fuel, and other refined petroleum products in 17 states and the District of Columbia. It allowed them to work extra or more flexible hours to make up for any fuel shortage related to the pipeline outage.

Thankfully, Colonial was able to restart the pipeline five days after it had shut it down, although it did say it would take "several days for the product delivery supply chain to return to normal."

While it wasn't initially clear whether or not Colonial had paid a ransom to the attackers, *Bloomberg News* reported on May 13 that the company had paid a ransom of $4.4 million. The company reportedly paid the ransom within hours of the attack occurring, and received a decryption key from the attackers. However, the decryption process was reportedly so slow that the company also continued to use its own backups to recover from the attack.

Speaking in front of the U.S. Senate Homeland Security and Governmental Affairs Committee on June 8, Colonial Pipeline's CEO Joseph Blount defended his decision to pay the ransom to the attackers, stating that he had "put the interests of the country first." He also revealed that the attackers gained initial access to the company's network through a "legacy VPN" account that the company's IT team did not know existed. The account was protected with only a password and did not have multi-factor authentication enabled.

The Attackers

Darkside, which Symantec tracks as Coreid, is a ransomware-as-a-service operation that works with affiliates to conduct ransomware attacks and takes a share of the profits. Coreid develops the malware and affiliates carry out the attacks. Like most ransomware actors these days, Coreid carries out what are known as "double extortion" attacks, where they steal victims' data and threaten to publish it to further pressure victims into paying the ransom demand. An unusual aspect of Coreid's operation is that it claims to prohibit affiliates from attacking certain organizations, including hospitals, hospices, schools, universities, non-profit organizations, and government agencies.

The group was first seen in August 2020, but a new level of interest was drawn to the group in the wake of the attack on Colonial Pipeline. Coreid had been noted for the level of "professionalism" employed by the group since it emerged, with the gang reportedly even providing a phone number and a help desk to facilitate negotiations with victims. This "professionalism" was evident in the wake of the Colonial attack too, with the group issuing a press release after it was named as the perpetrator of this attack. The group said it was "apolitical" and not associated with any government, and also stated that its goal was to make money, and not create problems for society. It said that in the future it would introduce moderation and check each company that its partners want to encrypt to avoid "social consequences."

Coreid is believed to be a financially-motivated cyber crime group, and is not thought to be nation-state-backed or interested in cyber espionage. While Symantec cannot definitively say where Coreid is based, public reports state the group is based in Eastern Europe, with Russia considered to be its most likely base. The group does check for the language used on infected machines and does not proceed with an attack if Russian or several other languages spoken in former Soviet bloc nations are installed on the machine.

Coreid is thought to be a very profitable ransomware group, having reportedly taken in around $90 million. Blockchain analysis firm Elliptic found and analyzed payments made to Coreid from 47 different Bitcoin wallets, with the payments totaling $90 million, which would mean the average ransom paid to Coreid was approximately $1.9 million. This would put Coreid at the high end of ransomware earners that we have seen, with this amount of money also collected in a reasonably short period of time, considering the group only emerged in August 2020. The Coreid operators are believed to keep 10% to 25% of the profits of attacks, with the rest going to affiliates, so the malware developers themselves are estimated to have made approximately $15.5 million. Nevertheless, it is difficult to determine exactly how much money is made by ransomware actors, so the true figure may be even higher.

However, it appears the Colonial Pipeline attack may have been an attack too far for the group, with Darksupp, an admin for the Coreid group, announcing on an underground forum on May 14 that the group had lost access to its data leaks site, payment servers, and content delivery network (CDN) servers following law enforcement action in the wake of the Colonial attack. This news came after U.S. President Joe Biden announced that countries harboring ransomware networks must take action to shut them down. "We have been in direct communication with Moscow about the imperative for responsible countries to take decisive action against these ransomware networks," he said.

The group was paid $9.4 million in ransoms—from Colonial Pipeline ($4.4 million) and German chemical company Brenntag ($5 million)—in the weeks before it shut down, causing speculation that the group may have decided to cash out and keep those profits rather than sharing with affiliates. However, on June 7 it was announced that authorities in the U.S. had recovered 63.7 of the 75 bitcoins Colonial had paid to Coreid. The Department of Justice said the FBI recovered the money after they gained access to one account's private key.

There is no doubt the increased attention on the group following the Colonial attack put it under pressure, but whether this is in fact the last we see of these ransomware actors remains to be seen.

Impact

As well as the obvious and immediate impact of this attack on Colonial itself, and the disruption to fuel supplies, the attack was also followed by some political pronouncements.

U.S. President Biden signed an executive order (EO) on May 12 aimed at modernizing U.S. defenses against cyber attacks, and allowing more timely access to information needed for law enforcement to conduct investigations. The 34-page EO followed several attacks targeting U.S. interests over the preceding few months, including the attack on Colonial, and the SolarWinds supply chain attacks.

The *Executive Order on Improving the Nation's Cybersecurity* called for a number of actions, including:

- Removing barriers to threat information sharing between government and the private sector
- Modernizing and implementing stronger cyber security standards in the federal government
- Improving software supply chain security
- Establishing a cyber security safety review board
- Creating a standard playbook for responding to cyber incidents
- Improving detection of cyber security incidents on federal government networks
- Improving investigative and remediation capabilities

The White House said the EO was the "the first of many ambitious steps the Administration is taking to modernize national cyber defenses."

In the wake of the Colonial attack, the U.S. Department of Homeland Security also issued a Security Directive for the oil and gas pipeline industry. The Directive, which will be administered by the Transportation Security Administration (TSA) and Cybersecurity and Infrastructure Security Agency (CISA), was published on May 27, 2021, and replaced voluntary guidelines that had been in place for more than a decade.

The Directive requires critical pipeline owners and operators to report any confirmed or potential cyber security incidents to CISA. They are also required to have a designated cyber security coordinator who is available 24/7. The Directive also stipulated that pipeline owners and operators needed to review their practices to identify any gaps and related remediation measures, and report the results to TSA and CISA within 30 days. TSA said it would also consider follow-on mandatory measures in the future that would "further support the pipeline industry in enhancing its cyber security." When announcing the directive, Secretary of Homeland Security Alejandro N. Mayorkas referenced the Colonial attack, stating: "The recent ransomware attack on a major petroleum pipeline demonstrates that the cyber security of pipeline systems is critical to our homeland security." He also said the DHS would work closely with the private sector to "increase the resilience of our nation's critical infrastructure."

The Department of Justice (DoJ) also established a Ransomware and Digital Extortion Task Force in the wake of the attack, which it said was "established to investigate, disrupt and prosecute ransomware and digital extortion activity." The DoJ also said that ransomware incidents would be given a similar priority as investigations into acts of terrorism.

The Colonial attack also had an impact outside of the U.S., with the South Korean government ordering a review of the cyber security preparedness of its energy infrastructure. South Korea's Minister of Trade, Industry and Energy, Moon Seung-wook, said that in the wake of the disruption at Colonial it was "necessary to thoroughly examine whether cyber security preparations and countermeasures for our energy-related infrastructure are properly in place." He ordered all operators of oil pipelines, power grids, gas pipelines, and emergency response systems to check the status of their systems and report back on their findings.

The Japanese government also announced it would introduce new regulations for 14 critical infrastructure sectors to bolster cyber defenses, in the wake of the Colonial attack. The sectors included areas like telecommunications, electricity, railroads, government services, and healthcare. The government will require operators of such key infrastructure to address national security concerns when procuring foreign-made equipment.

The wide-ranging impact of the Colonial attack is interesting. It appears to have raised awareness worldwide of the dangers posed by potential cyber attacks on companies involved in CNI, and has led to authorities in the U.S., particularly, showing a determination to crack down on ransomware attackers to a degree we hadn't previously seen.

Case Study: Concerted Attacks on CNI in South East Asia

Symantec researchers observed attacks on a number of organizations that were part of the CNI sector in a South East Asian country. These attacks were ongoing since at least November 2020, and continued right up to March 2021. Intelligence gathering was thought to be the likely motivation in these attacks.

Victims were seen in multiple organizations that all fall under the umbrella of CNI, including in the areas of water, power, defense, and communications. There are some indications that the attacker is based in China, but the activity cannot be attributed to any one particular group.

There are numerous indications that the attacks on the different organizations were carried out by the same attacker, including:

- The geographic and sector links of the affected organizations
- The presence of certain artifacts on machines in the different organizations, including a downloader (found in two of the organizations), and a keylogger (found in three of the organizations)
- The same IP address is also seen in attacks on two of the organizations

Credential theft and lateral movement on victim networks seemed to be a key aim of the attacker, who made extensive use of living-off-the-land tools in this campaign. While we do not know what the initial infection vector used by the attacker to get onto targeted networks was, we do see how they moved through infected networks.

Water Company

The first activity we saw in the attack on this organization was suspicious use of Windows Management Instrumentation (WMI); there is no indication of what infection vector was used to gain initial access to the machine. A legitimate free multimedia player called PotPlayer Mini was exploited by the attackers to load a malicious DLL. FireEye has previously published research about how this player was susceptible to DLL search order hijacking. DLL search order hijacking is not a new technique, but we do still see it frequently leveraged by attackers to insert malicious files onto victim machines. We saw PotPlayer Mini added as a service to launch a file called potplayermini.exe, we then saw multiple dual-use and hacking tools launched, including:

- ProcDump
- PsExec
- Mimikatz

ProcDump was used for credential theft by abusing the LSASS.exe process, and domain shares were enumerated using net view. We then observed a suspected tunneling tool being launched on the system. The machine targeted by the attackers in this instance had tools on it that indicate it may have been involved in the design of SCADA systems.

Power Company

Similar activity was seen in a company in the power sector. In that instance too, PotPlayer Mini was exploited to carry out DLL search order hijacking and ProcDump was deployed alongside another payload that we suspect was malware. We also saw the attacker once again carrying out credential theft by using ProcDump of the LSASS.exe process. There were indications here too that this machine may also have been involved in engineering design.

There was some file overlap between the attacks on both the water and power company as well as similar tactics used—pointing to the same actor being behind both events.

Communications Company

An interesting aspect of this attack was that the attacker appeared to have exploited a different legitimate tool, Google Chrome Frame, with suspicious files appearing where chrome_frame_helper.exe was the parent file. Google Chrome Frame is a plugin for Internet Explorer that enables rendering the full browser canvas using Google Chrome's rendering engine.

It wasn't clear if Google Chrome Frame was already present on the machine or if it was introduced by the attacker, however, it was the parent file of legitimate as well as suspicious files. PotPlayer Mini also appeared to be exploited on this machine by the attacker for malicious purposes.

PAExec, a tool similar to PsExec, launched at.exe (a Windows task scheduler) in order to schedule execution of chrome_frame_helper.exe as a task. WMI was used to run chrome_frame_helper.exe and perform credential theft by dumping LSASS. PsExec and WMIC were also used for lateral movement and to launch chrome_frame_helper.exe against an internal IP address. PsExec also launched it to schedule execution of an unknown batch file as a daily task, and chrome_frame_helper.exe was also used to launch the SharpHound domain trust enumeration tool and other suspicious files. PsExec was also seen executing what appeared to be Mimikatz for suspected credential theft.

WMI was used to run chrome_frame_helper.exe to execute a net.exe command to connect a hidden C$ share. This type of share is not visible when viewing another computer's shares. However, it is still accessible if the name of the hidden share is known. Persistence was created for chrome_frame_helper.exe as a scheduled task—GoogleUpdateTaskMachineCore4f23—with the file disguised as chrome_proxy1.exe.

Defense Organization

In the defense organization we once again saw PotPlayer Mini exploited for DLL search order hijacking, as well as seeing some file overlaps between this organization and the communications and water companies.

Conclusion

While we cannot definitively say what the end goal of the attacker was in these attacks, information stealing seems like the likeliest motive, given the activity we did see (credential stealing, lateral movement), and the types of machines targeted in some of the organizations (those involved in design or engineering). The ability of the attacker to maintain a stealthy presence on the targeted networks for a number of months indicates they were skilled. Certain artifacts found on the victim machines indicate the attacker may be based in China, though it is not possible with the information we have to definitively attribute these attacks to a named actor.

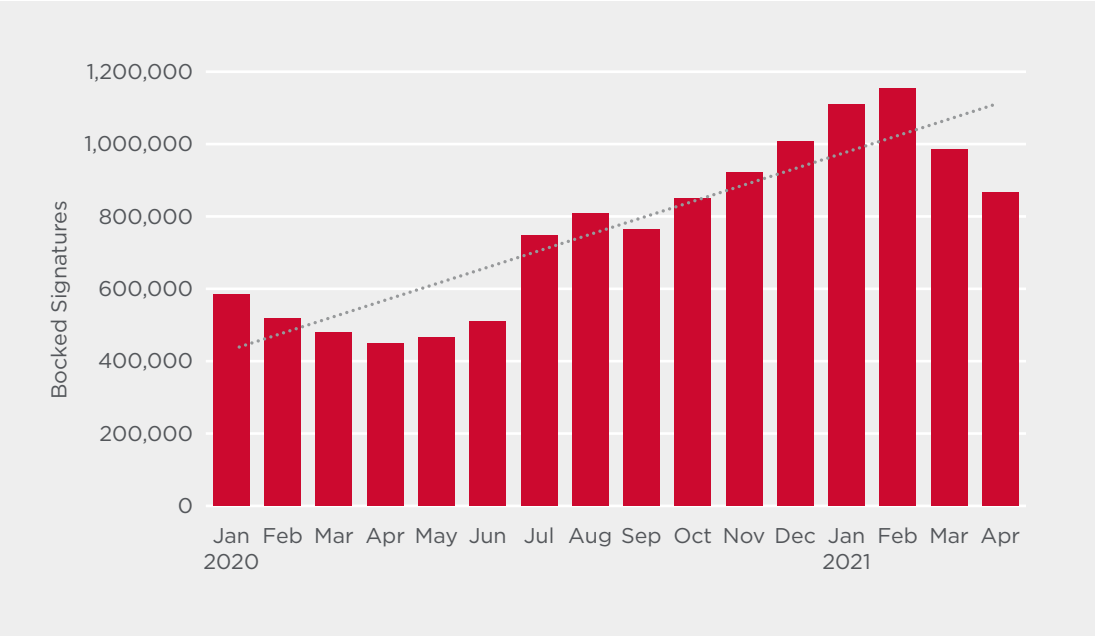
What the Data Tells Us

When we examine the malicious activity targeted at our CNI customers, it would appear that an increasing number of attackers are attempting to attack CNI organizations, but the number of attackers successfully gaining access and installing malware on the endpoint in this sector is trending down.

Network-based detections indicate that malicious activity targeted at CNI organizations is on the rise. Attacks blocked on the network by our Intrusion Prevention System (IPS) technologies help reveal information about the extent of malicious activity on organizations' networks. If a machine on a network becomes infected, the malware is likely to attempt to contact a command and control (C&C) server, which can also trigger these detections. Looking at the number of network detections attempting to contact a C&C server gives an indication of the number of infected machines on a network and a picture of the extent of malicious activity in a sector.

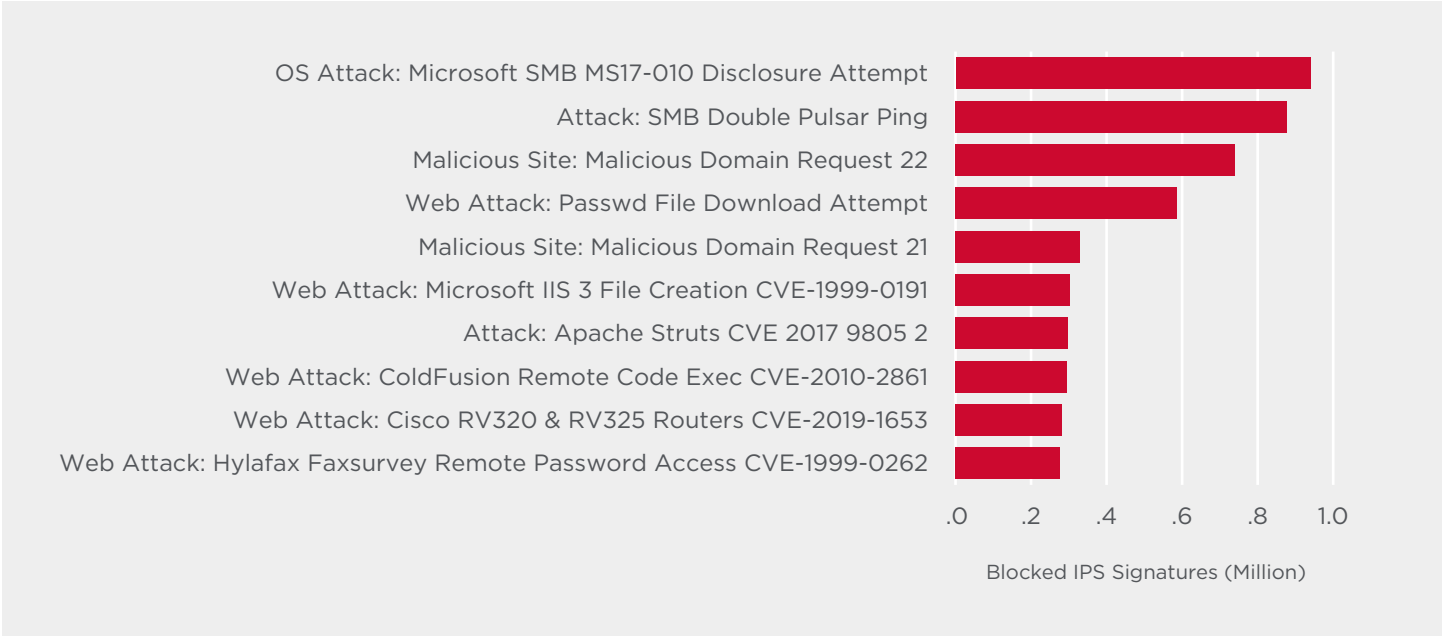
Network-based activity trended upwards over the time period we looked at, with an increase in June 2020 carrying through to February 2021. While these detections dropped slightly in March and April 2021, the overall trend is still increasing.

Figure 1: Malicious Activity Blocked on the Network by Month in CNI Customers, January 2020 to April 2021



The top 10 signatures blocked are primarily signatures that block attempts to exploit remote code execution (RCE) vulnerabilities that allow attackers to execute attacks on target organizations from wherever they are in the world.

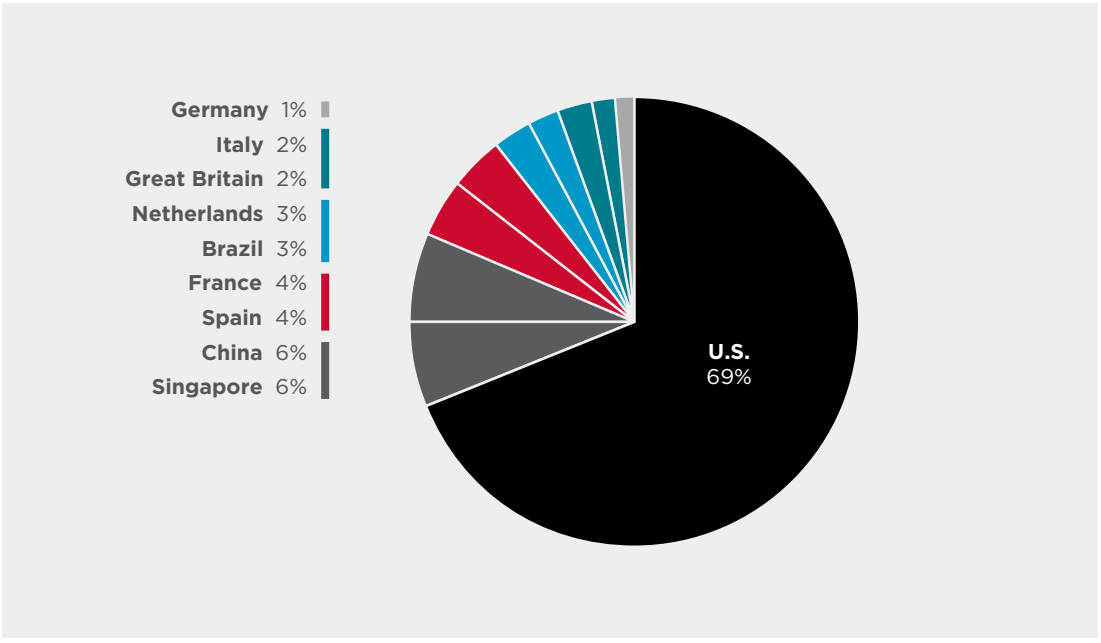
Figure 2: Top 10 IPS Signatures Blocked on the Networks of CNI Customers, January 2020 to April 2021



The most commonly seen blocking signature—OS Attack: Microsoft SMB MS17-010 Disclosure Attempt—detects attempts to exploit a RCE vulnerability in Microsoft Windows SMB Service, which was famously used in the disruptive WannaCry ransomware attack in 2017.

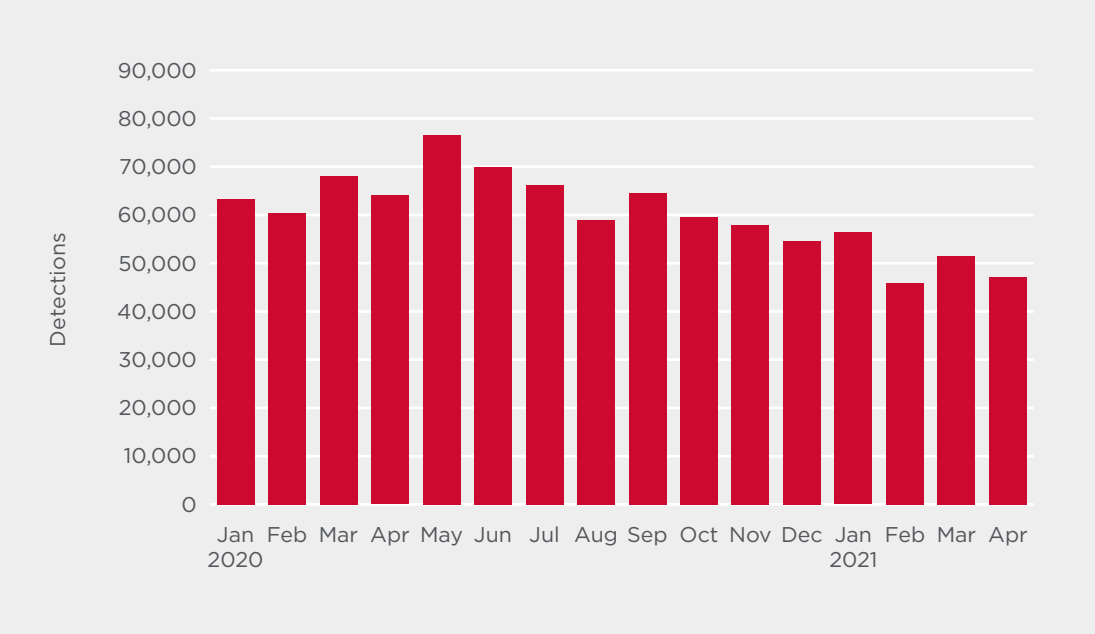
The U.S. is the country that sees by far the most activity targeting the networks of CNI organizations, with it accounting for 10-times as many network blocks as Singapore and China—the countries in second and third position in the top 10. Despite the concentration of malicious activity on the network of CNI customers in the U.S., overall the top 10 is a global picture, featuring countries from Europe and South America as well as Asia and the U.S.

Figure 3: Top 10 Countries for Network Blocks on the Machines of CNI Customers, January 2020 to April 2021



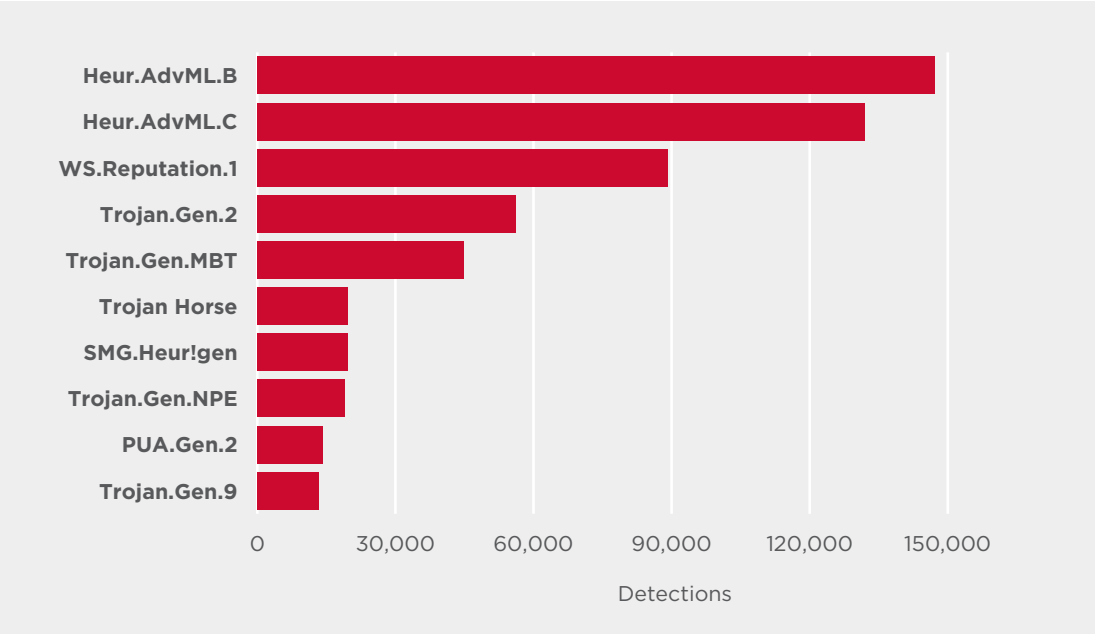
However, in something of a contrast, reviewing the data for malware activity on the endpoint in the CNI sector since the beginning of 2020 to April 2021 doesn't reveal any particularly dramatic trends. Malware activity on the endpoint in the sector has remained reasonably steady in that time period. We saw something of a spike in May 2020, but after that, activity returned to a fairly steady level, even declining slightly.

Figure 4: Malware Detections by Month for CNI Customers, January 2020 to April 2021



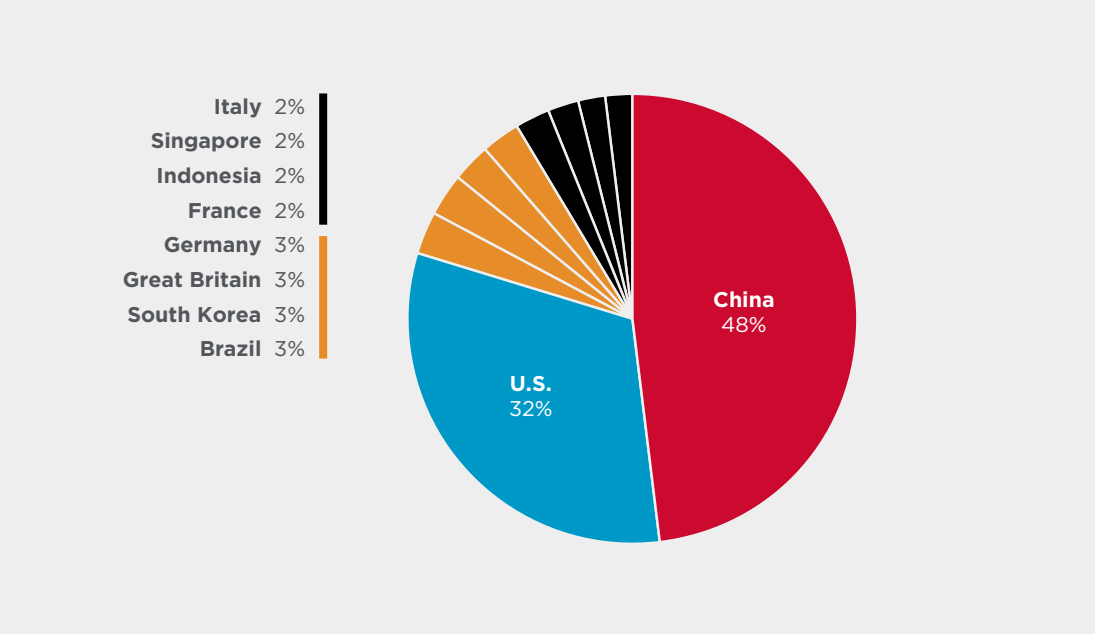
When we look at the top 10 detections being triggered by CNI customers, a lot of those detections are heuristic detections, which detect and block a wide range of different malware. This could include ransomware, crypto mining software, information stealers, or other backdoors that could give attackers a grip on the targeted network.

Figure 5: Top 10 Malware Blocked on the Machines of CNI Customers, January 2020 to April 2021



China and the U.S. were the countries where we saw the highest number of endpoint malware detections in the CNI sector, with those two countries combined accounting for 80% of the top 10 detections. However, the presence of countries in other parts of Asia and also Europe in the top 10 does further demonstrate that malware attacks aimed at CNI are a global issue.

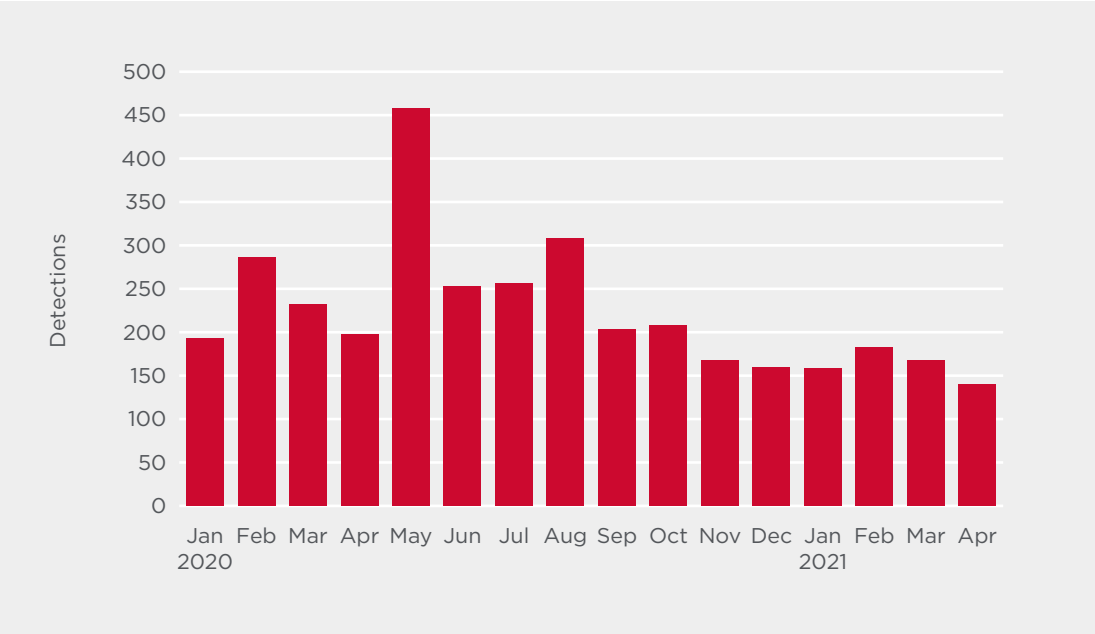
Figure 6: Top 10 Countries for Malware Detections on the Machines of CNI Customers, January 2020 to April 2021



Ransomware

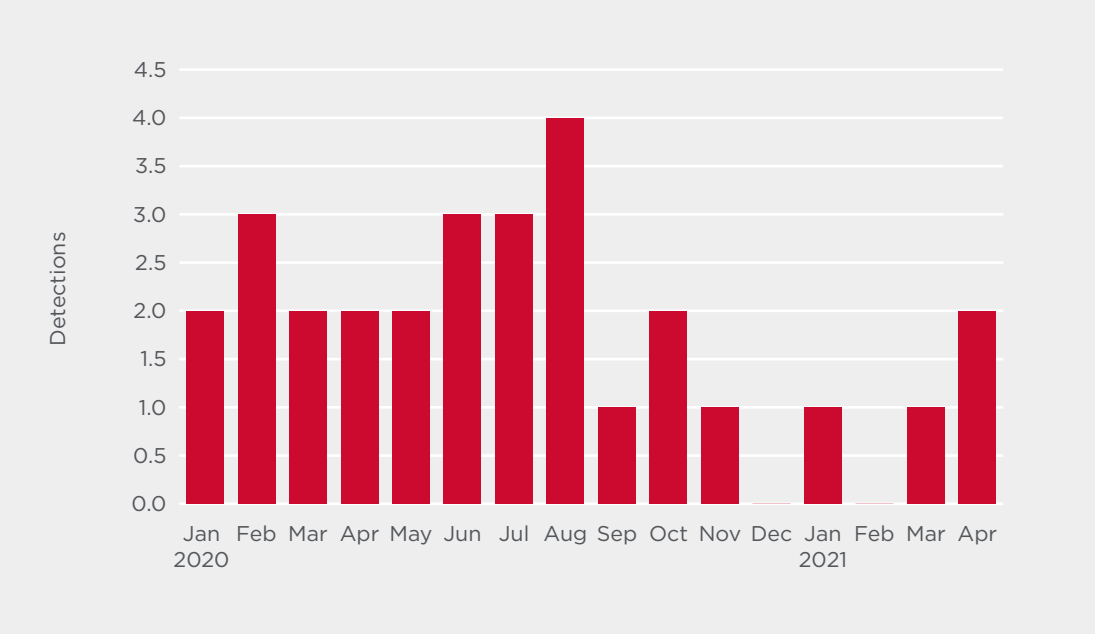
Ransomware activity aimed at organizations in the CNI sector remained reasonably steady over the period examined, although there was a spike in May 2020, with ransomware numbers somewhat elevated for several of the middle months of 2020. While we did see a small drop in malicious activity in general at the very beginning of the COVID-19 pandemic, as threat actors presumably also adjusted to a new way of working and targeting victims, this drop did not last long, and malicious activity did, in many cases, return to and even exceed pre-pandemic levels. It is possible the May spike was a return to activity for actors after a small decline in March and April.

Figure 7: Ransomware Detections by Month for CNI Customers, January 2020 to April 2021



While the ransomware numbers may not appear to be huge, ransomware attacks now are a lot more targeted, with the days of mass spamming ransomware campaigns largely a thing of the past. Most ransomware groups these days spend a long time planning attacks, potentially spending a long time on compromised systems carrying out reconnaissance and exfiltrating data before deploying ransomware. Due to the large paydays offered by ransomware attacks now, malicious ransomware actors tend to carry out fewer attacks for greater rewards.

Figure 8: Targeted Ransomware Detections by Month for CNI Customers, January 2020 to April 2021



While the number of targeted ransomware attacks aimed at organizations in the CNI sector over the period we examined may seem low—averaging at around two per month—just one attack every few weeks can easily give attackers the outcome they want. It should also be noted that the data shown in *Figure 8* is only a representative sample of the overall number of attacks involving targeted ransomware. Most targeted ransomware operators recompile their payloads for every new attack. This means that the variant of the ransomware used in an attack may be blocked by a generic or machine learning-generated detection signature rather than a detection linked to that ransomware family.

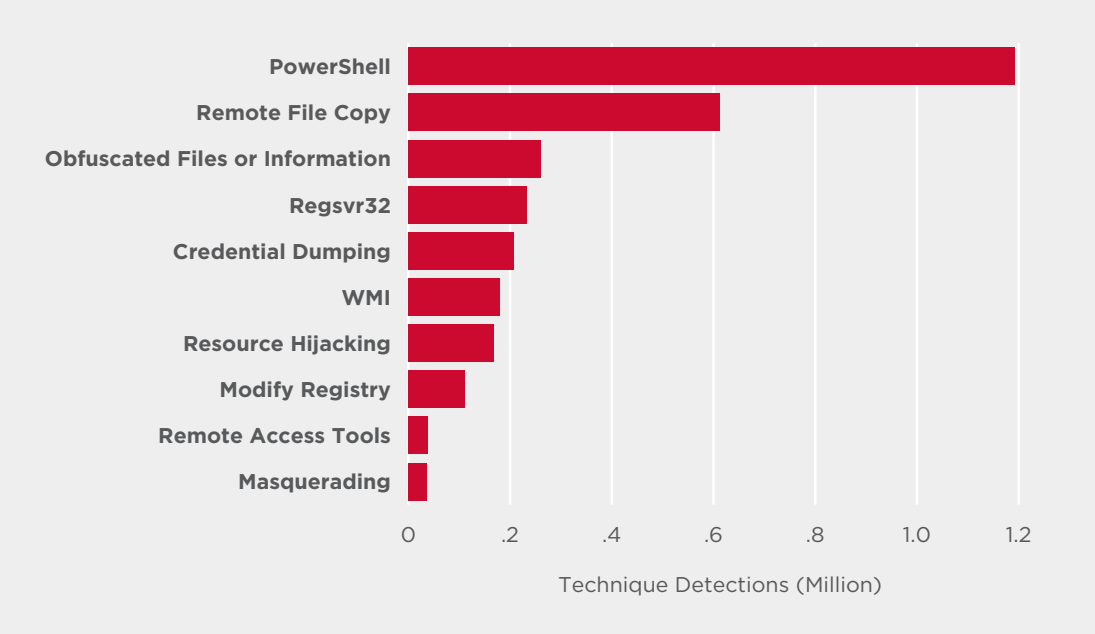
The Colonial Pipeline attack demonstrated that just one ransomware attack on a key organization can lead to wide-ranging disruption, and potentially a big payday for attackers. JBS Foods, one of the world's largest meat producers, paid $11 million to the REvil ransomware gang on June 1, 2021, after a ransomware attack on the company encrypted some of its operations in North America and Australia, leading to significant disruption. REvil had also threatened to leak data it said it had stolen from the company.

For organizations that become infected with ransomware—particularly when they are in critical sectors like energy, food production, or health—trying to balance the risks of not paying with the knowledge that paying only encourages attackers to continue carrying out these kinds of attacks can be a difficult balancing act. An organization's desire and sometimes need to avoid long-term disruption, and potentially recovery costs significantly greater than the cost of paying a ransom, can lead to big paydays for ransomware criminals.

Attack Tactics, Techniques, and Procedures

In 2021, malware detections tell only part of the malicious activity story, with the popularity of living-off-the-land techniques among malicious actors these days meaning that a lot of malicious activity can occur without any malicious tools being deployed. For this reason, Symantec Cloud Analytics doesn't just detect malicious tools, but rather it draws on intelligence gathered from analyst investigations and leverages advanced machine learning to identify and block patterns of suspicious activity. It then classifies all incidents with a MITRE ATT&CK® technique name. With millions of incidents logged each year, it is possible to form a picture of what the most frequently used techniques are.

Figure 9: Top 10 MITRE Techniques Used in Attacks Against CNI Customers, January 2020 to April 2021



The top 10 MITRE techniques used in attacks against CNI customers are familiar names that we frequently see leveraged by malicious actors in a wide range of attacks. PowerShell, for example, the technique we see leveraged most often by attackers, is by far the most popular dual-use tool used by attackers. It is a powerful and versatile tool for malicious actors, but it is also widely used for legitimate purposes. Malicious usage still only accounts for a small percentage of overall PowerShell usage, meaning that attackers abusing it are often able to hide in plain sight on victim machines.

Living-off-the-land techniques allow attackers to minimize malware usage, deploying it only when necessary and sometimes, as often in the case of ransomware, at such a late stage in the attack that the victim has little or no time to respond and stop the attack. The popularity of living-off-the-land tools for attackers is demonstrated in the case study earlier in the paper, where the attackers made wide use of living-off-the-land tools and techniques in their attack chain.

Activity like that is why having protection in place that can spot suspicious activity before malware is deployed is important for organizations striving to keep their networks safe.

Other Noteworthy Attacks on CNI

While extremely high-profile, the attack on Colonial Pipeline was not the first impactful attack on CNI infrastructure we have seen.

Stuxnet and the Threat of "Cyber-Physical" Attacks

Probably one of the most famous cyber attacks to ever occur, the Stuxnet attack is believed to have begun in late 2007 when the digital weapon was deployed against centrifuges at a uranium enrichment plant. That attack was discovered and widely reported on in 2010. The immense sophistication of the attack meant that the presumption was that a nation state was behind it, with the Stuxnet attack now widely believed to have been powered by a cyber weapon developed over the course of a number of years in a collaborative effort between the U.S. and Israel.

Stuxnet was the first example of a cyber attack having a physical impact, damaging, as it did, centrifuges at a nuclear enrichment facility in Natanz, Iran. Stuxnet worked by modifying the centrifuge speeds, causing them to speed up and become damaged or destroyed. The output at the nuclear plant was reported as dropping by a third during the time it was infected with Stuxnet. Stuxnet was a highly targeted attack that was only ever intended to infect the targeted networks but an error in the code meant it spread to a computer that had been connected to the centrifuges and then made its way onto the internet to spread further. However, as Stuxnet was specifically programmed to target Siemens Step7 software on computers controlling programmable logic controllers (PLCs), it caused little damage outside of the targeted networks.

Stuxnet showed for the first time in real life that it was possible for "cyber" attacks to cross over and become "physical" attacks with a real-world impact. The possibility of this occurring was—and remains—a major fear for governments and corporations worldwide. The sophistication of Stuxnet showed that, while not easy to execute, it was possible to carry out attacks like this.

For a long time Stuxnet appeared to be an outlier, and we didn't see another cyber attack causing physical damage to infrastructure until 2014. Just before Christmas that year, a report was released revealing that hackers had struck an unnamed steel mill in Germany. They manipulated and disrupted the control systems in the mill so much that a blast furnace could not be properly shut down, resulting in what was described as "massive" damage. Germany's Federal Office for Information Security (BSI), which issued the report about the incident, indicated that the attackers gained access to the steel mill through the plant's business network, then successively gained access to the production network, which allowed them to access systems controlling plant equipment. The attackers were believed to have gained initial access to the corporate network through a spear-phishing email. Once they had an initial foothold they were able to explore the company's networks and eventually compromise a "multitude" of systems, including industrial components on the production network. The report said that as a result of this unauthorized access the plant was "unable to shut down a blast furnace in a regulated manner" which resulted in "massive damage to the system."

Authorities in Germany did say at the time that the attackers appeared to possess knowledge of industrial control systems, however, it is not clear if causing destructive physical damage to the steel mill was part of the attacker's plan, or if the incident was collateral damage of their presence on the network.

If it was accidental, it demonstrates that it isn't just extremely sophisticated attackers like those behind Stuxnet that organizations need to worry about causing physical damage. It is unlikely that all the malware used to infiltrate ICS and other networks will be as well designed as Stuxnet, leading to the possibility that incidents that lead to real-world damage could be unintentionally caused as collateral damage.

While Stuxnet took elaborate steps in order to gain access to air-gapped networks, the attackers who targeted the German steel mill appear to have been able to jump from the corporate network to the production side of the plant. Incidents like this serve to underline the importance of good cyber practices like network segmentation and Zero Trust policies, so that if attackers compromise one part of your network they do not gain access to the entire system.

Blackout: The Dangers of Power Grid Attacks

The attack on the Ukraine power grid took place on December 23, 2015, and was the first confirmed hack to bring down a power grid. Such an attack had been long feared given the immense disruption such an outage could cause. That this attack took place in the depths of Europe's winter underlined the seriousness of the situation, with the average temperature in Ukraine in December often dipping below 32 degrees Fahrenheit (zero degrees Celsius).

The attack on the Ukrainian power grid was very sophisticated, with the attackers thought to have been on the power grid systems for several months before they deployed the malware. The attack began with a spear-phishing campaign targeting IT staff and system administrators working for multiple companies responsible for distributing electricity throughout Ukraine. The email had an attachment that contained malicious macros; if this was opened a malicious backdoor called BlackEnergy was downloaded onto the corporate network. However, this only gave hackers access to the corporate network, and it is understood that the targeted power distribution companies in Ukraine did have network segmentation in place, with a firewall separating the corporate network from the SCADA network that controlled the power grid. However, the attackers explored the corporate network, conducting reconnaissance and eventually gaining access to the Windows Domain Controllers, where they were able to harvest worker credentials for the VPNs used to remotely log in to the SCADA network. As workers logging remotely into the SCADA network weren't required to use multi-factor authentication, once the attackers had access to those credentials they were able to log in to the SCADA network.

This shows the importance of having all the different facets of your organization's cyber security strategy implemented. While the power grid companies in Ukraine were doing the right thing by having their networks segregated, the fact they didn't have multi-factor authentication set up for all workers logging remotely into the SCADA network meant that attackers were ultimately able to overcome that hurdle to gain access to the SCADA network anyway.

Once on the SCADA network, the attackers went to the trouble of replacing the legitimate firmware on Serial-to-Ethernet converters in order to prevent the operators from sending remote commands to re-close breakers once a blackout occurred. They were then ready to carry out their attacks, opening circuit breakers to plunge tracts of Ukraine into darkness. They also flooded the power companies' customer call centers with phone calls to take them offline when customers wanted to contact them. The attackers also deployed a wiper malware called KillDisk to wipe files from operator stations to render them inoperable.

Ultimately in this incident, the attackers hit three power distribution centers, took around 60 substations offline, and left almost a quarter of a million Ukrainians in darkness. In this instance, authorities were able to get the lights turned back on quickly—with the longest outage lasting six hours—but the impact of the attacks were felt in the power distribution centers for several months as several actions could no longer be performed remotely. Given the skill levels of the actors in this attack and the access they achieved on the network, the consequences of this attack could have been a lot more serious than they were, and it certainly served as a warning to power companies of the level of destruction attackers could deploy on power grids.

While this attack occurred in a European country, and not the U.S., similar environments are likely to exist in U.S. power distribution centers, meaning the threat of such an attack is there wherever in the world your organization may be located. While we have not yet seen U.S. electricity disrupted by a cyber attack, an AP investigation in the same year the Ukraine attack took place showed that the U.S. power grid was certainly of interest to foreign adversaries, a fact that is unlikely to have changed in the last few years.

Shamoon: Destructive Attacks Threaten Oil Industry in Middle East

The threat widely known as Shamoon (W32.Disttrack) first appeared in 2012, when it was used in a targeted attack against at least one organization in the energy sector in Saudi Arabia. Shamoon is notable because it is a wiper malware that corrupts files on an infected machine and overwrites the Master Boot Record (MBR) in order to make the computer unusable. Those deploying Shamoon appear to have destruction as their goal, as opposed to espionage or financial gain, the more common motives for cyber attacks.

Shamoon was seen again in 2016, when a slightly modified version of the malware was once again used in destructive attacks aimed at the Saudi energy sector. In the 2012 attacks, infected computers had their MBRs wiped and replaced with an image of a burning U.S. flag. The 2016 attacks instead used a photo of the body of Alan Kurdi, a three year-old Syrian refugee who drowned in the Mediterranean Sea in 2015. The attacks appeared timed to cause maximum destruction. The malware was configured to trigger on Thursday night, local time, on November 17, 2016. The Saudi working week runs from Sunday to Thursday, meaning computers were wiped after most staff had left for the weekend, minimizing the chance of discovery before the attack was complete. It also appeared the attackers had done a significant amount of preparatory work for the operation, as the malware was configured with credentials that appear to have been stolen from the targeted organizations, allowing it to move laterally across machines on the network.

Shamoon reappeared again in 2018, again focusing on targets in the Middle East, with victims that time in the United Arab Emirates (UAE), as well as Saudi Arabia. Once again, the victims operated in the oil and gas sector. However, these attacks were slightly different from prior incidents as they involved a new, second piece of wiping malware (Trojan.Filerase). This malware would delete and overwrite files on the infected computer, while Shamoon itself erased the computer's MBR. The addition of the Filerase malware made the attacks even more destructive as deleting the files before erasing the MBR meant they could not be recovered.

Although attacks involving destructive malware such as Shamoon are relatively rare, they can be highly disruptive for the targeted organization, potentially knocking mission-critical computers offline and leading to the loss of important files. The fact that Shamoon seems to reappear every few years means that corporations, particularly any that have operations in the Middle East, need to be aware of this threat and prepared, with comprehensive backups and a robust security strategy in place.

Shamoon attacks are believed to be associated with malicious actors operating out of Iran, with the attacks often tending to coincide with periods of heightened instability in the region. The fact the attackers also seemed to have been evolving their attacks, with the addition of the Filerase malware in the most recent wave of attacks, should also be a cause of heightened vigilance against attacks of this type.

Iranian hackers were also linked to an intrusion at the Bowman Avenue Dam, a small dam in New York State, in 2013. Media reports said the hackers were believed to have gained access to the dam through a cellular modem. The hackers reportedly didn't take control of the dam but probed the system, possibly discovering information about how the computers running the flood control system worked. This intrusion occurred in 2013, but information about it didn't emerge until 2015. While no damage was caused during this attack, it serves to demonstrate the interest foreign adversaries have in U.S. critical infrastructure organizations.

Conclusion

The Colonial Pipeline attack underlined that ransomware, with its ability to shut down operations and cause significant business impact, can be just as disruptive a threat as the so-called "destructive" malware that we saw deployed in, for example, the Shamoon and Stuxnet attacks. A recent Conti ransomware attack on the Irish Health Service Executive (HSE), the country's national healthcare service, also demonstrated how disruptive ransomware attacks can be. The attack on the HSE led to the cancellation of many services and major disruption, with authorities there vowing not to pay a ransom and predicting it would take many weeks for the service to recover from the attack. Targeted ransomware attacks that also steal data and demand large ransoms are one of the biggest cyber security threats for all sectors at the moment, and CNI is no exception.

The impact on the public that can be caused by cyber attacks on CNI industries, such as essential services being forced offline for a period, also means that attacks on organizations in this industry can be hard to keep from the public and media, potentially leading to awkward questions and possible damage to businesses' reputations.

Meanwhile, a somewhat unique challenge faced by CNI is the effect cyber-physical attacks could have on the sector, with the prospect of attackers being able to destroy equipment or gain control of things like dams or electricity substations a particular danger that this sector has to deal with.

We have seen companies in the CNI sector from the U.S. to Europe to the Middle East targeted with serious and disruptive attacks, so there is no region in which CNI organizations can assume they are not under threat of a serious cyber attack. All these threats underline that organizations operating in this sector need to have a robust cyber security strategy in place in order to keep their networks, equipment, and customers, safe.

Mitigation

Symantec security experts recommend users observe the following best practices to protect their networks:

- Look to deploy an integrated cyber defense platform that shares threat data from endpoint, email, web, cloud apps, and infrastructure.
- Ensure multi-factor authentication is enabled for all accounts using your network.
- Monitor the use of dual-use tools inside your network.
- Ensure you have the latest version of PowerShell and you have logging enabled.
- Restrict access to Remote Desktop Protocol (RDP) services by only allowing RDP from specific known IP addresses.
- Implement proper audit and control of administrative account usage. You could also implement one-time credentials for administrative work to help prevent theft and misuse of admin credentials.
- Ensure any legacy applications that are no longer in use are removed from all machines on your network so they cannot be misused.
- Create profiles of usage for admin tools. Many of these tools are used by attackers to move laterally undetected through a network.
- Use application allow lists where applicable.
- Implement offline backups that are onsite. Make sure you have backups that are not connected to the network to prevent them from being encrypted by ransomware.
- Test restore capability. Ensure restore capabilities support the needs of the business.
- Educate staff to ensure they understand cyber security principles and do not engage in any behaviors that may put network security at risk.

Protection

How Symantec Solutions Can Help
The Symantec Enterprise Business provides a comprehensive portfolio of security solutions to address today's security challenges and protect data and digital infrastructure from multifaceted threats. These solutions include core capabilities designed to help organizations prevent and detect advanced attacks.

Symantec Endpoint Security Complete
Symantec Endpoint Security Complete (SESC) was specifically created to help protect against advanced attacks. While many vendors offer EDR to help find intrusions, as does Symantec, there are gaps. We call these gaps blind spots and there are technologies in SESC to eliminate them.

Symantec recommends that customers ensure that IPS technology is running on all endpoints for superior protection against network-based attacks. Additionally, Adaptive Protection and TDAD technologies should be implemented to harden systems against living-off-the-land attacks and to prevent lateral movement.
LEARN MORE

Privileged Access Management (PAM)
PAM is designed to prevent security breaches by protecting sensitive administrative credentials, controlling privileged user access, proactively enforcing security policies and monitoring and recording privileged user activity.
LEARN MORE

Symantec Web Isolation
Symantec Web Isolation eliminates web threats and solves the challenge of providing access to unknown, uncategorized and potentially risky web sites by creating a remote execution environment between an agency's enterprise systems and content servers on the web.
LEARN MORE

Symantec Secure Web Gateway (SWG)
SWG delivers high-performance on-premises or cloud secure web gateway that organizations can leverage to control or block access to unknown, uncategorized, or high-risk web sites.
LEARN MORE

Symantec Intelligence Services
Symantec Intelligence Services leverages Symantec's Global Intelligence Network to deliver real-time threat intelligence to several Symantec network security solutions including Symantec Secure Web Gateway, Symantec Content Analysis, Symantec Security Analytics, and more.
LEARN MORE

Symantec Content Analysis with Advanced Sandboxing
Within the Symantec Content Analysis platform, zero-day threats are automatically escalated and brokered to Symantec Malware Analysis with dynamic sandboxing for deep inspection and behavioral analysis of potential APT files and toolkits.
LEARN MORE

Symantec Security Analytics
Symantec Security Analytics delivers enriched, full-packet capture for full network traffic analysis, advanced network forensics, anomaly detection, and real-time content inspection for all network traffic to arm incident responders for quick resolution.
LEARN MORE

Symantec™
A Division of Broadcom

For product information and a complete list of distributors, visit our website at: broadcom.com

SES-AACI-WP108 July 1, 2021