White Paper

Symantec
A Division of Broadcom

The Threat Landscape in 2021

Symantec Threat Hunter Team

Table of Contents

Introduction

Ransomware

The Cyber-Crime Ecosystem

Supply Chain Attacks

New Avenues of Attack

Attacks Against Critical Infrastructure

Living off the Land

Attack Tactics, Techniques, and Procedures

Conclusion

Protection

Mitigation

Introduction

The past year has been an eventful one when it comes to the world of cyber security, with new threats emerging and threat actors continually evolving their tactics in order to maintain or improve their position in the threat landscape.

During 2021, ransomware continued to be the most serious threat facing organizations of all sizes. The current template for ransomware attacks – targeted attacks designed to cripple the networks of victim organizations – has been tremendously lucrative for cyber criminals. While there has been some welcome developments, such as the departure of several highly active ransomware operations, these have unfortunately been outweighed by the arrival of new players and the continued refinement of tactics.

Ransomware is now arguably the lynchpin of the entire cyber-crime ecosystem, financing an ever-growing number of affiliated attack groups and providing new income streams for a wide range of attackers such as spammers, financial Trojan operators, and intrusion specialists.

While ransomware continues to be a serious concern, there were several other notable developments during 2021, not least the step up in the scale and ambition of supply chain attacks. While the early part of the year was dominated by the reverberations of the SolarWinds attack, it was followed in July by the Kaseya attack, where ransomware operators found a novel force multiplier for their tools. These attacks will not go unnoticed by threat actors and more may seek to look to the software supply chain as a means of access to high value networks.

Perhaps the single most prominent attack to occur during 2021 was the ransomware attack on the Colonial Pipeline in the U.S. A key piece of infrastructure in the country's energy supply, the Colonial attack was highly disruptive and provided a grave warning about the potential impact of attacks against critical infrastructure. Financially motivated ransomware gangs are not the only threat. Nation states intent on causing disruption and creating panic among their rivals are also a source of concern.

As we look to 2022, organizations need to remain vigilant as they face a broadening range of highly motivated and increasingly well-resourced adversaries.

Ransomware

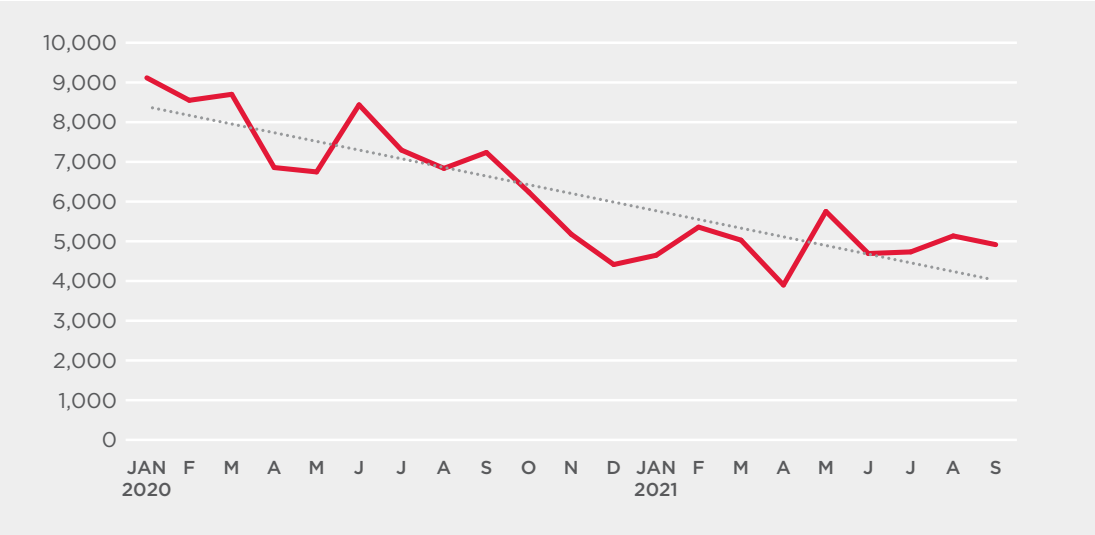
The ransomware problem remained a dominant issue in 2021, with recent developments including ransomware gangs moving towards targeting entities with a broad network of downstream users. These upstream entities included large software developers and organizations involved in critical infrastructure, as seen in the Kaseya and Colonial Pipeline attacks. In addition, targeting managed service providers (MSPs) provides attackers with the opportunity to infect potentially thousands of victims by compromising only one.

Another trend that emerged during the year was ransomware gangs targeting industries that were hardest hit by the COVID-19 pandemic, namely those in the healthcare industry. Attacks such as the one against Ireland's national health service, the Health Service Executive, were carried out when hospital services were under severe pressure, with the attackers likely believing this would work in their favor and force officials to give in to their demands.

Ransomware attacks on critical infrastructure led to U.S. President Joe Biden calling on his Russian counterpart Vladimir Putin to take action against ransomware operators based in Russia. The leaders agreed that they would bring together cyber security experts from their two nations to establish "specific understandings about what's off limits" from cyber activity and how the U.S. and Russia would "follow up" on cyber attacks that "originate in either of our countries". However, months later, the White House National Security Council hosted an international counter-ransomware event with participation from more than 30 nations with the notable exception of Russia.

The persistence of ransomware means Symantec, a division of Broadcom Software, publishes regular reports on the seemingly ever-present threat. Our recent whitepaper, *The Ransomware Threat*, found that, as in previous years, the total number of ransomware attacks detected and blocked by Symantec continued to trend downwards, however, this doesn't necessarily mean ransomware activity is becoming less of a threat. That paper included data up to June 2021 and showed that detected and blocked attacks went from 9,116 in January 2020 to just 4,692 in June 2021. While the number of attacks rose slightly to 4,916 in September 2021, the numbers are still trending downwards overall (Figure 1). This is due to a significant decrease in relatively unsophisticated, indiscriminate ransomware attacks and threat actors focusing on targeting their attacks against large organizations where they can cause more disruption and demand higher ransom amounts.

Figure 1: All Ransomware Detections Jan 2020 to Sep 2021

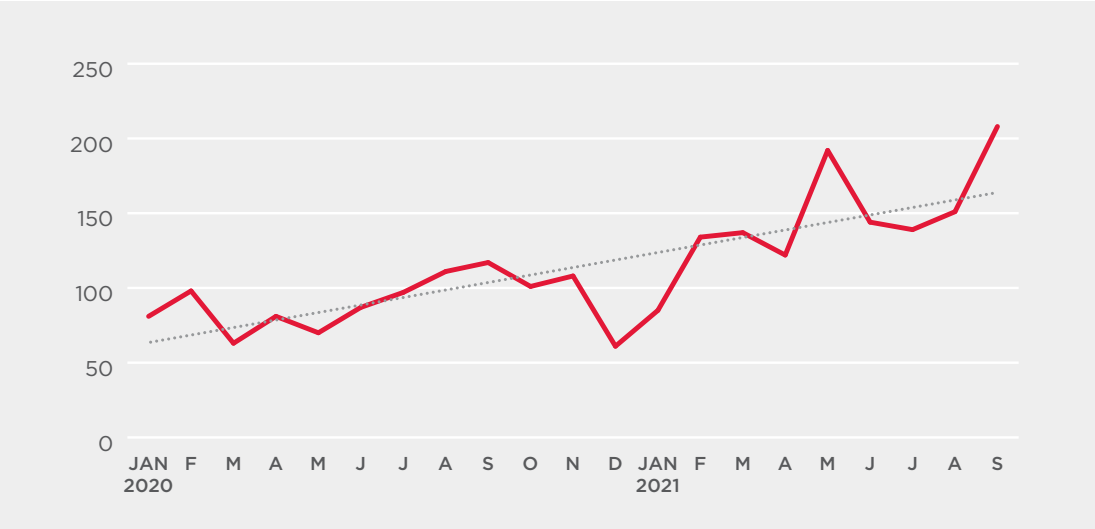


This increase in targeted ransomware threats was also highlighted in a U.S. Treasury Department Financial Trend Analysis report that linked more than $5.2 billion in Bitcoin transactions to ransomware gangs since 2011. The report found that, in the first six months of 2021 alone, these types of transactions totaled $590 million, already exceeding the $416 million in Bitcoin transactions linked to ransomware in the entire 12 months of 2020.

All this is occurring despite law enforcement efforts to stem the tide of targeted ransomware, such as the recent international operation that pushed the REvil (aka Leafroller, Sodinokibi) ransomware offline. REvil's infrastructure was compromised by agents from the U.S. Federal Bureau of Investigation (FBI), U.S. Cyber Command, the Secret Service, and a number of international governments, who gained control of at least some of REvil's servers. This is the second time REvil has shut down. The gang's activities were previously halted following the Kaseya ransomware supply chain attack in July 2021, with rumors that law enforcement had compromised its operations then too. However, REvil returned again in September and is likely to reappear in some form following the most recent takedown effort.

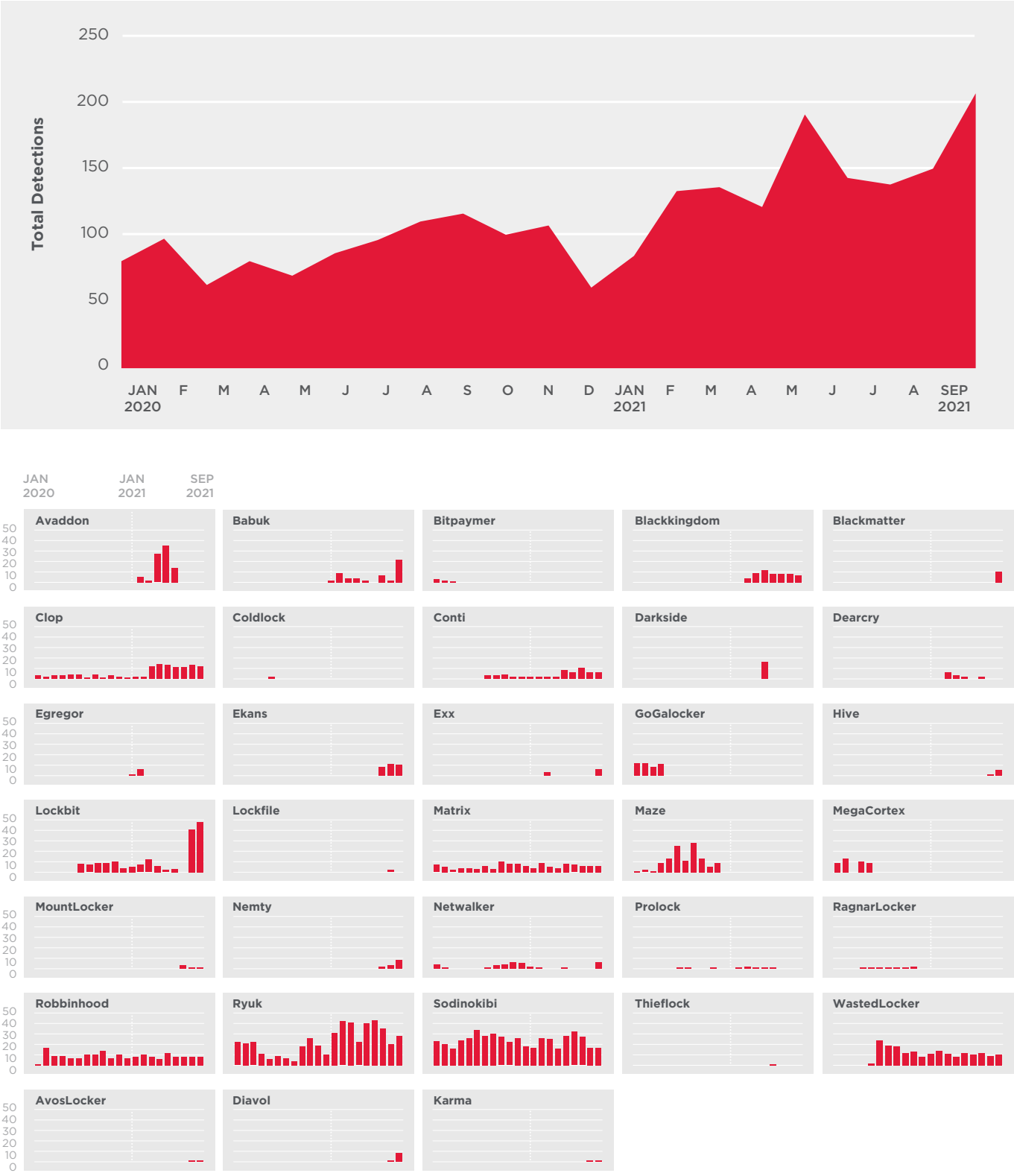
While overall ransomware detections are declining, targeted ransomware attacks are trending upwards (Figure 2). The number of organizations affected by targeted ransomware attacks rose from around 80 in January 2020 to more than 200 in September 2021. This is partly fueled by the rise in ransomware-as-a-service (RaaS), a subscription-based model that lets individuals or gangs known as affiliates use already-developed ransomware threats in their attacks.

Figure 2: Number of Organizations Affected by Targeted Ransomware Attacks, Jan 2020 to Sep 2021



Another trend contributing to the increase in targeted ransomware attacks is the rise of so-called initial access brokers (IABs). These actors have already gained access to networks and sell that access to whoever pays them, which in recent times has increasingly been ransomware operators. IABs allow ransomware operators to avoid the timely process of finding and compromising vulnerable organizations, freeing them up to concentrate on extorting their victims.

Figure 3: Number of Organizations Affected by Targeted Ransomware Attacks, by Family, Jan 2020 to Sep 2021



Another trend we've seen this year is targeted ransomware groups threatening victims in order to prevent them from sharing details of the attack with media or ransomware negotiating firms.

In October, the operators of the Conti ransomware (aka Miner, Wizard Spider) said that they would publish stolen victim data if transcripts or screenshots of ransom negotiations were publicly shared. The announcement was likely prompted by a growing number of media reports containing details of ransom negotiations.

The Grief ransomware gang also warned victims against contacting negotiating companies, threatening to delete victims' decryption keys if their instructions weren't followed. Other threat groups also employed similar tactics, including Ragnar Locker and a new ransomware threat called Yanluowang, which was uncovered by Symantec's Threat Hunter Team.

The Cyber-Crime Ecosystem

Ransomware has had a massive impact on the cyber-crime sector, creating new opportunities for aspiring attackers and bringing greater cooperation between more established actors.

One of the key drivers of change has been the maturation of ransomware-as-a-service (RaaS). From a ransomware developer's perspective, RaaS was the missing piece of the jigsaw. Targeted ransomware attacks are labor intensive and, for any ransomware operator, their revenues were limited by the number of attacks that they could perform. By leasing their tools to other attackers in exchange for a share of the profits, ransomware operators can maximize their revenues and provide an avenue into ransomware attacks for attackers who may not have the skills to create their own ransomware operation from the ground up.

For organizations, this multiplies the number of adversaries they face as, with most ransomware threats these days, there are now different groups all attempting to deliver the same ransomware, but using different tactics, techniques, and procedures (TTPs).

This year has seen an increase in the sophistication and complexity of the RaaS market. Affiliates are now highly mobile and, if a ransomware operator shuts down, many will simply migrate to another ransomware group and begin using their tools instead.

There is also a suggestion of a shift in the balance of power between ransomware operators and affiliates because Symantec has observed affiliates using two different strains of ransomware in a very short space of time and, in some cases, during the same attack. This points to affiliate actors having enough of a reputation to not be locked in to an exclusive agreement with one ransomware operator.

The second notable development is the role that botnets now play in ransomware attacks, providing a new lease of life for many older threats. The majority were originally created for the purposes of financial fraud, but many have been repurposed and the most choice bots, ones inside major organizations, are being sold on to ransomware attackers.

In some cases, it is the same threat actor behind both the ransomware and the botnet. For example, Trickbot is believed to be controlled by the Miner group (aka Wizard Spider) which is also linked to both the Ryuk and Conti ransomware families. The IcedID botnet has also been heavily used by ransomware attackers, whilst other botnets such as Qakbot, Emotet, and Dridex have also featured.

This level collaboration is an unwelcome development as it means that any organization that finds this kind of high-prevalence malware on their network will now have to consider if it is being used as the vehicle for a far more potent type of threat.

Supply Chain Attacks

In our whitepaper *Supply Chain Attacks: Cyber Criminals Target the Weakest Link*, published in February 2021, we discussed how these types of attacks have been taking place for several years but had hits the headlines in late 2020 when the SolarWinds hack occurred.

In a supply chain attack that came to light in December 2020, the update mechanism for SolarWinds' Orion software was compromised and a Trojanized update (Backdoor.Sunburst) was distributed to tens of thousands of SolarWinds customers, including multiple U.S. government agencies.

The Russia-backed Nobelium (aka Hagensia) hacking group, which conducted the SolarWinds attack, has remained active since then. A new backdoor threat likely developed by Nobelium was uncovered in September. Dubbed Tomiris, the malware has similarities to the SUNSHUTTLE second-stage malware used by Nobelium in the SolarWinds attack. Tomiris is deployed via a DNS hijacking attack during which targets attempting to access the login page of a corporate email service are redirected to a fraudulent domain set up with a lookalike interface designed to trick the visitors into downloading the malware under the guise of a security update.

Another backdoor called FoggyWeb was also linked to Nobelium. The post-exploitation backdoor is capable of stealing sensitive data from a compromised Active Directory Federation Services (AD FS) server.

While the SolarWinds attack was significant due to the size and make-up of the company's customer base, supply chain attacks are by no means rare. According to an October 2021 report from the Identity Theft Resource Center (ITRC), supply chain attacks are increasing, with 793,000 more individuals being affected by such attacks in the first three quarters of 2021 than in the entire 12 months of 2020. ITRC recorded 60 entities impacted by 23 third-party or supply chain attacks in the period up to and including September 2021.

One of the entities infiltrated in the course of a supply chain attack was Kaseya, the maker of business IT management and remote monitoring solution Kaseya Virtual System Administrator (VSA). The attack, which was carried out by the REvil (aka Leafroller, Sodinokibi) ransomware gang, impacted multiple managed service providers (MSPs) who used Kaseya VSA software.

The attack exploited a vulnerability in VSA and was carried out during the U.S. July 4 holiday weekend, likely in an effort to keep the attack under the radar until it had achieved its goal, as many employees would have been out of the office. Once the attack was uncovered, Kaseya urged VSA users to shut down their VSA servers to prevent them from being compromised. While the company stated that only a "small percentage" of their customers were impacted by the attack, those customers were MSPs with numerous customers themselves. Kaseya reported that around 60 customers were affected by the attack; however, the number of organizations compromised as a result of the supply chain attack was estimated at 1,500.

In July, Kaseya announced it had obtained a universal decryptor for the REvil ransomware used in the attack. While Kaseya only said that it received the decryptor from a "trusted third party," the REvil gang later revealed that a universal decryptor key for all victims of the Kaseya ransomware attack was accidentally released to victims by one of its coders. REvil had initially demanded $70 million for a universal decryptor, $5 million for a decryptor for each MSP, or $40,000 for each encrypted computer.

Software supply chain attacks, due to their potential to disrupt large sections of society and business, remain a concern for governments and businesses around the world.

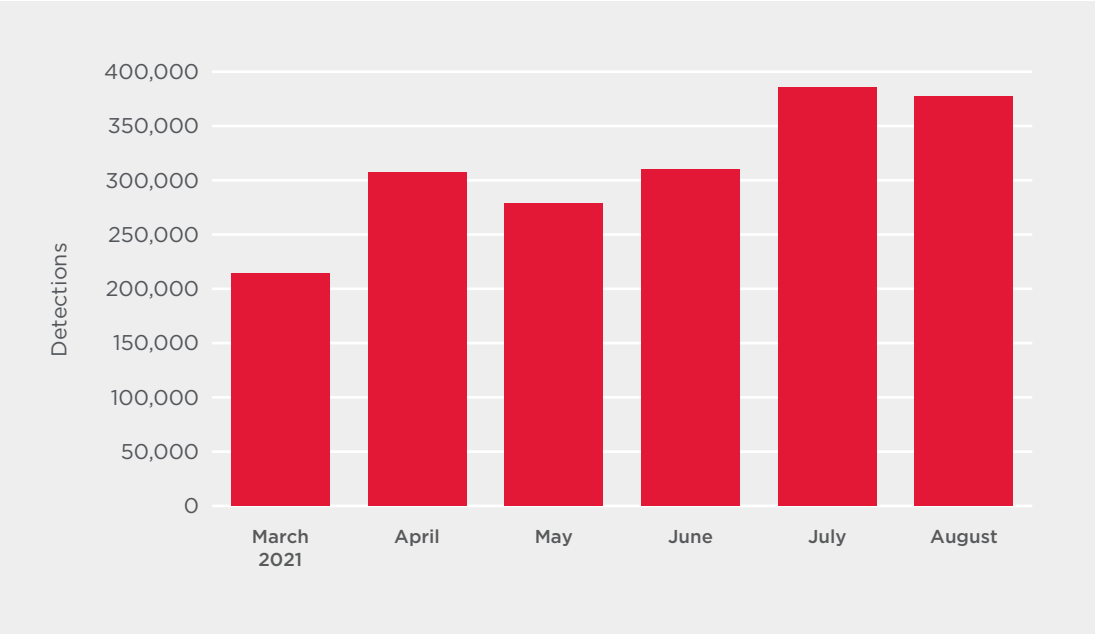
New Avenues of Attack

The past year has seen an upsurge in attackers exploiting vulnerabilities in public-facing applications in order to gain access to organizations' networks. In some cases, they are exploits of zero-day vulnerabilities, but more frequently the focus is on recently patched vulnerabilities and the hunt for unpatched systems.

The most notable example of this followed the discovery of a number of critical vulnerabilities in Microsoft Exchange Server, collectively known as ProxyLogon.

Microsoft issued emergency patches for the vulnerabilities on March 2, 2021. At the time, Microsoft said the vulnerabilities were being exploited by an advanced persistent threat (APT) group it dubbed Hafnium (Symantec tracks this group as Ant) in targeted attacks. However, as soon as the existence of the vulnerabilities became public knowledge numerous other threat actors rushed to exploit them. This was seen in reports at the time and is also visible in our data (Figure 4), which shows exploit attempts against Exchange Server vulnerabilities began in March 2021 and have continued at a consistently high level ever since.

Figure 4: Exploit Attempts Against Microsoft Exchange Server Vulnerabilities, March to August 2021



In August 2021, another string of vulnerabilities in Microsoft Exchange Server, dubbed ProxyShell, were publicly revealed at the Black Hat tech conference. These three flaws (CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207) allow for unauthenticated, remote code execution (RCE) on Microsoft Exchange servers when chained together. Exploit attempts targeting these bugs began immediately, with Symantec data showing more than 200,000 exploit attempts targeting this set of vulnerabilities in August 2021 alone.

Other vulnerabilities in public-facing applications that are frequently exploited by malicious actors include:

- VPN vulnerabilities in Pulse Secure (CVE 2019-11510) and Fortinet (CVE-2018-13379). The Australian Cyber Security Centre (ACSC) published an advisory in mid-2021 warning that LockBit 2.0 ransomware attackers were using CVE-2018-13379 to gain initial access to victim networks. There were also reports in September 2021 that this vulnerability was exploited to steal almost 500,000 VPN login credentials that were then shared on a hacking forum. Both vulnerabilities also featured in the Cybersecurity and Infrastructure Security Agency's (CISA) list of the most exploited vulnerabilities in 2020, despite the fact they had been patched in 2019 and 2018, respectively.
- A zero-day vulnerability in Sonicwall VPN (CVE-2021-20016). Prior to patching, the vulnerability was being exploited by the Canthroid cyber-crime group, which is responsible for the Thieflock ransomware. The vulnerability was patched in February 2021, but Canthroid has continued to attack organizations by exploiting this vulnerability in unpatched versions of the software. Successful exploitation allows the attacker to create their own credentials and join the targeted network.
- Vulnerabilities in Accellion's File Transfer Appliance (FTA) software. Attackers exploited four vulnerabilities (CVE-2021-27101, CVE-2021-27102, CVE-2021-27103, and CVE-2021-27104) to attack FTA servers and install a previously undocumented web shell named DEWMODE. The breach, which was linked to FIN11 and the Clop ransomware gang, gave the attackers access to some Accellion customers' data.

Analysis by Symantec revealed a number of distinct trends emerging around the exploit of vulnerabilities in pubic facing applications:

- How quickly vulnerabilities are exploited by attackers. In most cases, exploit attempts begin as soon as a vulnerability becomes public knowledge. Often this is because these vulnerabilities quickly get integrated into tools such as Metasploit, which can allow relatively unskilled actors to potentially scan and exploit such vulnerabilities on unpatched servers and products.
- Once a vulnerability is targeted by attackers it appears it continues to be exploited for a long time period. Exploit attempts tend not to taper off. In most cases, this is likely due to mass vulnerability scanning that is carried out by multiple actors and cyber criminals.

- Vulnerabilities in public-facing applications can potentially give malicious actors access to a wide variety of applications, and potentially provide them with very comprehensive unauthenticated access to victim networks.

Attacks Against Critical Infrastructure

Symantec's paper *Attacks Against Critical Infrastructure: A Global Concern* was published in June 2021 and focused on cyber attacks against critical national infrastructure (CNI). These attacks can be some of the most impactful as they have the potential to affect everyone in society. CNI attacks have the potential to disrupt utilities people use on a daily basis, such as power, water, transportation etc.

Our reliance on, and the vulnerability of, CNI was highlighted on May 7, 2021 when the Colonial Pipeline, the largest petroleum pipeline in the U.S., suffered a ransomware attack that impacted equipment managing the pipeline.

The Russia-based DarkSide ransomware gang carried out the attack and demanded 75 bitcoin (US$4.4 million at the time) to decrypt Colonial's systems. The gang had also stolen 100 GB of data from the company to use as leverage if the ransom wasn't paid. The ransom was paid just hours after the attack took place; however, the decryption process was slow and the pipeline's operation was halted, causing fuel shortages, price increases, and panic buying across a number of U.S. states.

Due to the poor decryption software provided by the attackers, Colonial's own backups were used to bring the system back online on May 12. Following the attack, which brought major disruption across the southeast of the U.S., President Biden signed an executive order to increase software security standards for sales to the government, tighten detection and security on existing systems, improve information sharing and training, establish a Cyber Safety Review Board, and improve incident response. The Department of Justice also convened a cyber-security task force to increase prosecutions in an effort to deter similar attacks.

Unfortunately, the Colonial Pipeline attack was not a one-off occurrence. In July 2021, it was revealed that Chinese state-sponsored threat actors had targeted 23 U.S. oil and gas pipeline operators in attack campaigns between 2011 and 2013, successfully compromising 13 of them. This information was revealed in a July 20 joint report issued by the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI). The report stated that "these actors were specifically targeting U.S. pipeline infrastructure for the purpose of holding U.S. pipeline infrastructure at risk" and that "this activity was ultimately intended to help China develop cyber-attack capabilities against U.S. pipelines to physically damage pipelines or disrupt pipeline operations."

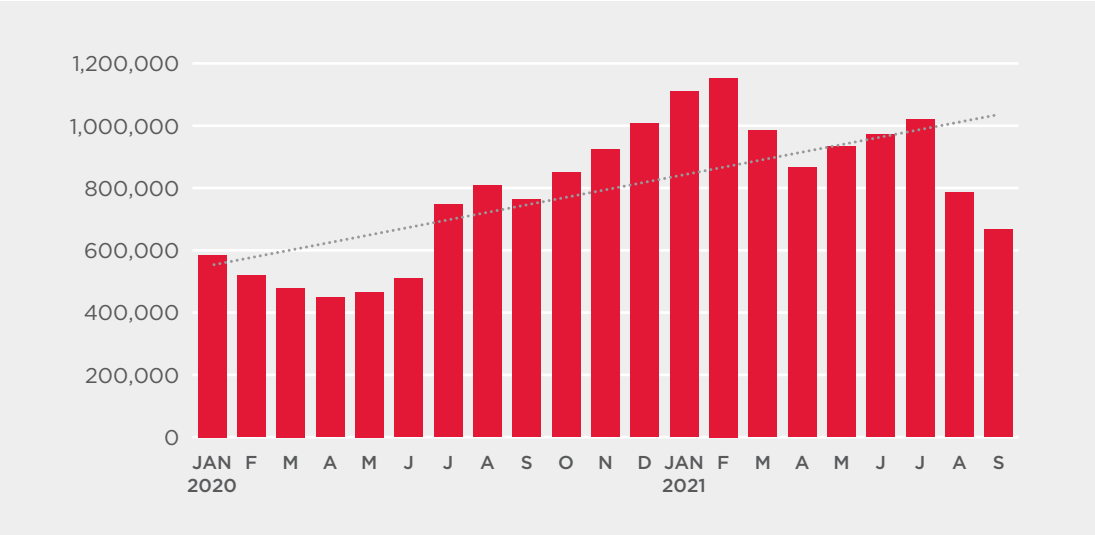
A Continuing Concern

As discussed, attacks against CNI are concerning for many reasons and show no sign of stopping.

While CISA lists a total of 16 different industries that fall under the CNI banner, due to the size of some of these industries our CNI paper, as well as the following updated statistics, concentrate 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

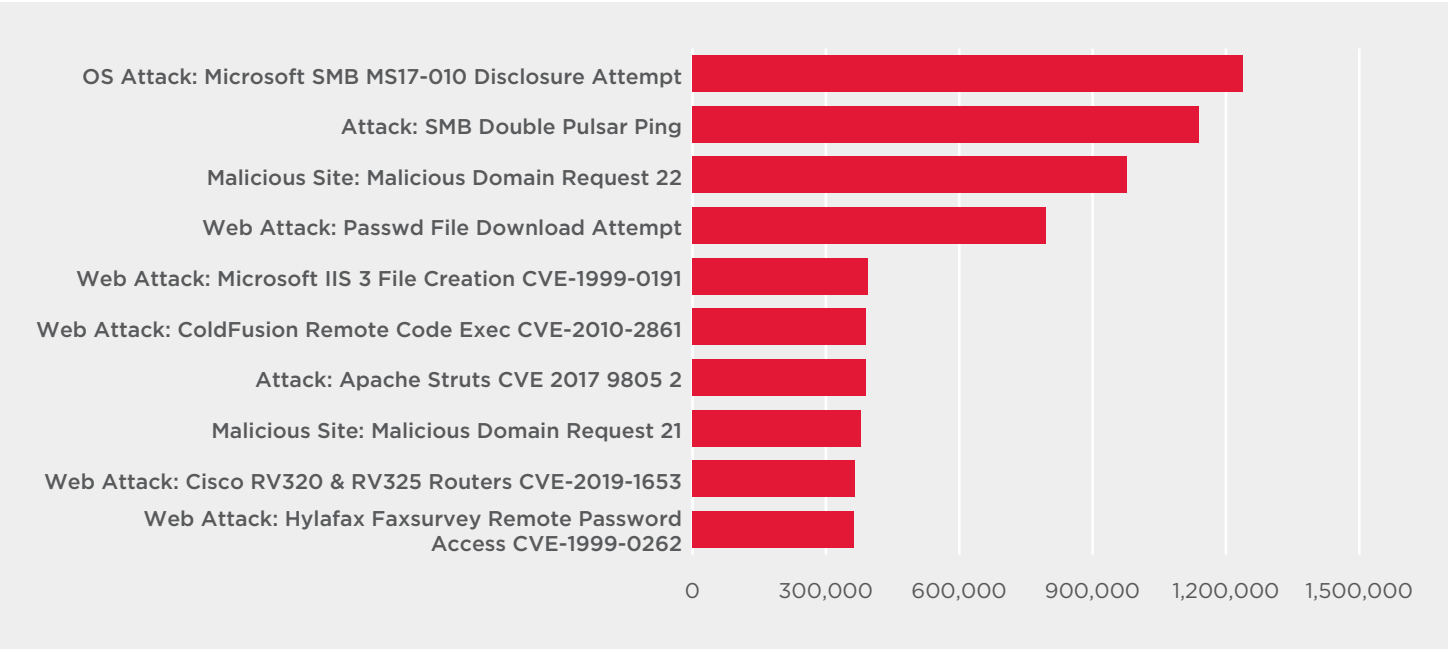
Figure 5: Malicious Activity Blocked on the Network by Month in CNI Customers, Jan 2020 to Sep 2021



The number of network-based detections related to attacks targeting CNI is trending upwards. These attacks are blocked by Symantec's Intrusion Prevention System (IPS) technologies. Malicious activity blocked on the network saw a decline after a peak in July 2021, however, overall the numbers are trending upward.

When it comes to the top blocked IPS signatures on CNI networks the results are similar to what was shown in our CNI paper. The majority are signatures that block attempts to exploit remote code execution (RCE) vulnerabilities, with the top four blocking signatures keeping their positions.

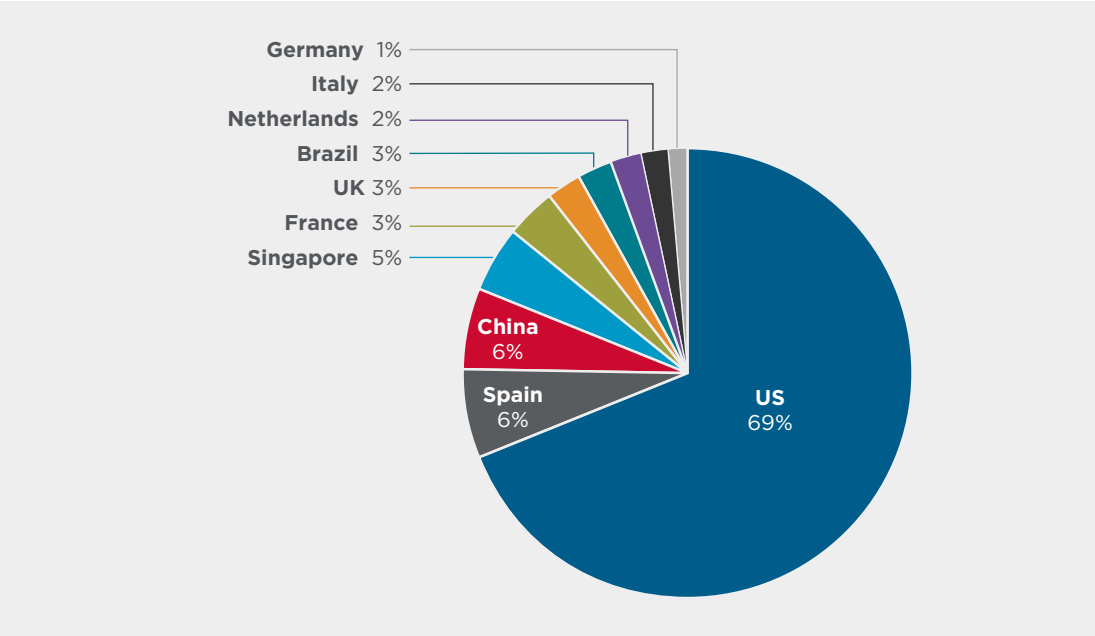
Figure 6: Top 10 IPS Signatures Blocked on the Networks of CNI Customers, Jan 2020 to Sep 2021



In terms of regions that see the most activity targeting the networks of CNI organizations, the U.S. is bounds ahead of others on the list with 69% of all activity seen there. This is the same percentage of activity as reported in out CNI paper which covered data from January 2020 to April 2021.

The next most targeted regions listed in our paper were Singapore (6%), now replaced by Spain (6%), and China, which remains at the number three position (6%).

Figure 7: Top 10 Regions for Network Blocks on the Machines of CNI Customers, Jan 2020 to Sep 2021



Living off the Land

Living off the land has become an increasingly popular tactic used by threat actors in an attempt to fly under the radar and avoid detection. In short, living off the land involves using legitimate tools or leveraging features that already exist in the target environment for malicious purposes. This can help attackers to remain undetected as the use of these legitimate tools and features is not likely to raise any red flags. In addition, the fact that the tools and features already exist and the attackers don't need to spend time and resources developing their own makes living off the land an even more tempting tactic to employ.

During 2020 there was a 29.4% increase in the number of executions of 22 of the most commonly seen dual-use tools in Symantec customer environments, from 5.9 billion executions in 2019 to 7.6 billion in 2020. The numbers for 2021 have already surpassed those from 2020. By the end of September 2021 there was already a 44.9% increase on 2020, with 10.9 billion executions observed so far in 2021 compared to 7.6 billion for the entirety of 2020.

In terms of which dual-use tools are the most commonly seen in customer environments, PowerShell remains at the number one spot with 234% more executions than its nearest rival net.exe.

Table 1: Number of Executions Per Tool for Top 26 Dual-Use Tools, 2019-2021

Tool	2019	2020	2021 (Jan to Sep)
powershell.exe	5,680,737,655	7,248,945,270	7,956,724,935
net.exe	20,603,632	71,106,792	2,384,860,498
schtasks.exe	53,400,817	139,675,323	457,013,261
bitsadmin.exe	9,271,644	39,295,319	116,580,088
psexec.exe	21,061,886	19,000,752	67,091,362
wmic.exe	50,711,927	42,538,858	5,069,305
certutil.exe	16,306,248	19,785,607	2,627,475
sdelete.exe	211,417	248,111	1,258,608
tasklist.exe	925,812	687,823	1,187,194
teamviewer.exe	2,338,302	1,073,812	398,638
systeminfo.exe	365,362	273,187	174,686
wget.exe	455,273	250,821	136,140
gpresult.exe	1,428,498	674,506	91,127
curl.exe	468,414	195,474	81,694
ammyy.exe	123,066	56,086	11,634
rdpclip.exe	122,788	27,444	5,265
procdump.exe	6,603	3,924	3,202
nc.exe	8,309	3,276	2,234
vnc.exe	7,406	3,343	2,100
bloodhound.exe	7,318	1,095	264
wce.exe	338	179	130
nbtscan.exe	2,876	223	95
TOTAL:	**5,858,565,591**	**7,583,847,225**	**10,993,319,935**

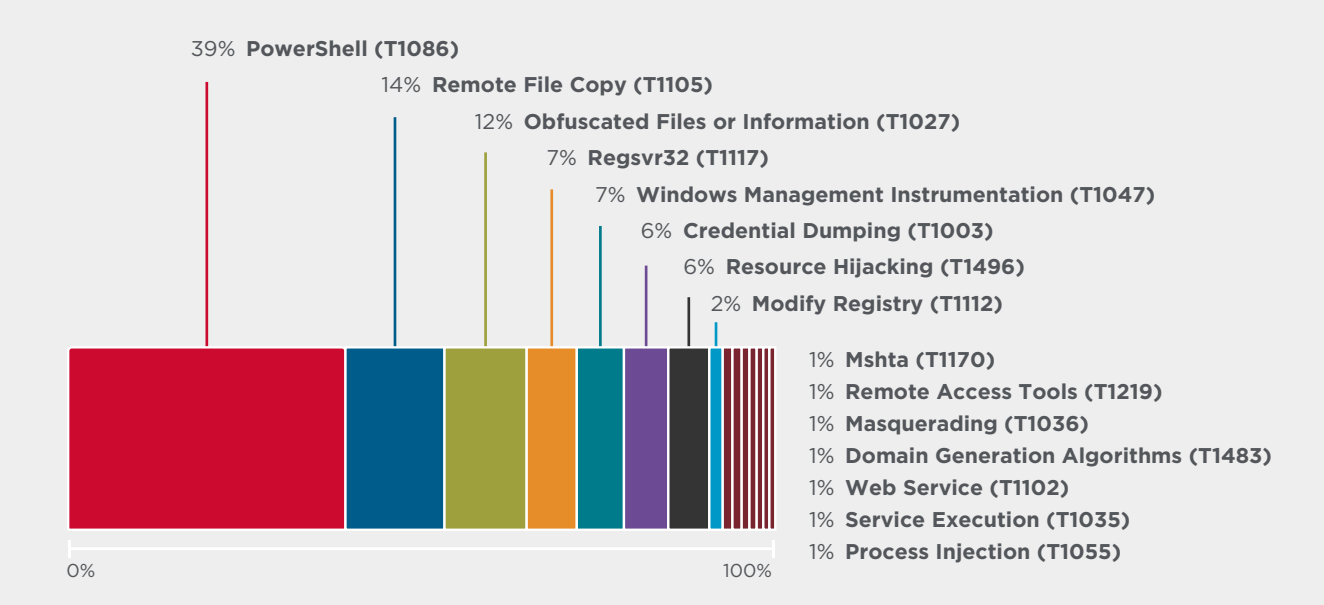
Attack Tactics, Techniques, and Procedures

The MITRE ATT&CK® matrix classifies attack techniques and tactics. It divides attack tactics into 12 main categories, which map to the typical attack chain between vector and payload execution.

- Initial access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact

Within these categories, there are 245 distinct attack techniques. Some may be employed at multiple stages of an attack chain, meaning they can apply to more than one of the above 12 categories. Symantec Cloud Analytics classifies all incidents with a MITRE technique name. With millions of incidents logged each year, it is possible to form a picture of what the most frequently used techniques are. Cloud Analytics draws on intelligence gathered from analyst investigations and leverages advanced machine learning to identify and block patterns of suspicious activity. Because it is designed to identify malicious activity, more so than malicious tools, the vast majority of incidents created relate to living-off-the-land tactics.

Figure 8: MITRE Techniques Associated with Cloud Analytics Incidents, Jan to Sep 2021



Malicious PowerShell usage accounts for 39% of incidents. The other techniques making the top five included:

- **Remote File Copy:** Transferring tools or files from external sources onto a compromised network, either via download from a command and control (C&C) server or through other methods such as FTP.
- **Obfuscated Files or Information:** Attempting to make a malicious file difficult to discover by encoding it or otherwise obfuscating its contents.
- **Regsvr32: Regsvr32.exe** is a command-line program used to register and unregister object linking and embedding controls. Attackers may abuse Regsvr32.exe for proxy execution of malicious code.
- **Windows Management Instrumentation (WMI):** Microsoft command-line tool, which can be used to execute commands on remote computers.

Conclusion

The past year has been an eventful one when it comes to the threat landscape and all indicators point to 2022 continuing this trend. While cyber criminals will no doubt continue to leverage the avenues of attack discussed in this paper, they will also find new opportunities for attack.

Cyber-security threats are not going anywhere anytime soon and organizations should remain aware of the risks, ensure that they have the appropriate solutions in place, and be proactive and leave no part of their attack surface unprotected or unmonitored.

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.

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

Mitigation

Symantec recommends users observe the following best practices to protect against targeted attacks.

Local Environment:

- 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 RDP Services. Only allow RDP from specific known IP addresses and ensure you are using multi-factor authentication (MFA).
- 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.
- Create profiles of usage for admin tools. Many of these tools are used by attackers to move laterally undetected through a network.
- Use application whitelisting where applicable.
- Locking down PowerShell can increase security, for example with the constrained language mode.
- Make credential dumping more difficult, for example by enabling credential guard in Windows 10 or disabling SeDebugPrivilege.
- MFA can help limit the usefulness of compromised credentials.
- **Create a plan to consider notification of outside parties.** In order to ensure correct notification of required organizations, such as the FBI or other law enforcement authorities/agencies, be sure to have a plan in place to verify.
- **Create a "jump bag" with hard copies and archived soft copies of all critical administrative information.** In order to protect against the compromise of the availability of this critical information, store it in a jump bag with hardware and software needed to troubleshoot problems. Storing this information on the network is not helpful when network files are encrypted.

Email:

- Enable MFA to prevent the compromise of credentials during phishing attacks.
- Harden security architecture around email systems to minimize the amount of spam that reaches end-user inboxes and ensure you are following best practices for your email system, including the use of SPF and other defensive measures against phishing attacks.

Backup:

- **Implement offsite storage of backup copies.** Arrange for offsite storage of at least four weeks of weekly full and daily incremental backups.
- **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.
- **Verify and test your server-level backup solution.** This should already be part of your Disaster Recovery process.
- **Secure the file-level permissions** for backups and backup databases. Don't let your backups get encrypted.
- **Test restore capability.** Ensure restore capabilities support the needs of the business.

Symantec™
A Division of Broadcom

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

SES_TTT_WP111 December 17, 2021