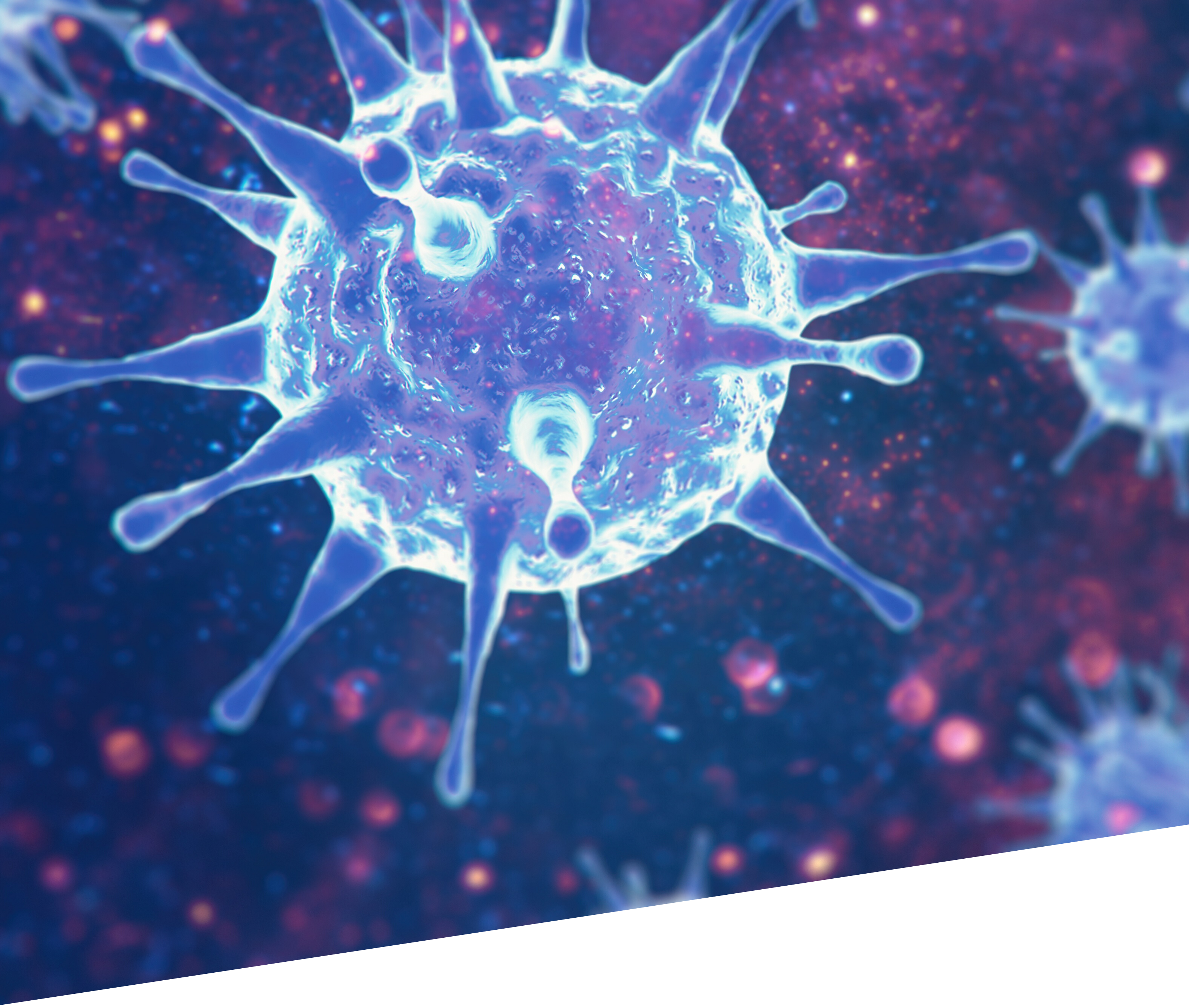

IT-ISAC

COVID-19 CHALLENGES AND LESSONS LEARNED

REPORT

JULY 2020 // PREPARED BY THE IT-ISAC OPERATIONS TEAM

20TH ANNIVERSARY OF THE

IT-ISAC

FOUNDED 2000

The mass, unplanned imperative to enable employees to work from home has resulted in one of the biggest IT and cybersecurity challenges in years. Even companies who have promoted work from home and thus have established policies and procedures for managing work from home security issues, have been impacted due to the scale and suddenness of the switch, as 90% or more of their employees quickly transitioned to remote work.

This paper seeks to document some challenges experienced by companies and to offer lessons learned. In creating this white paper, the IT-ISAC team incorporated input from both members and independent, public sources. While our members generally participated with the promise of non-attribution, we have provided citations to all publicly sourced content.

CHALLENGE - SECURITY THREATS

Threat actors have leveraged the COVID-19 virus's notoriety to target victims across all sectors. We have seen financially motivated actors taking advantage of the pandemic, as well as nation-state actors.

Fake Installers: We have seen threat actors pushing fake Zoom installers and VPN solutions to install malicious software on machines. Often these applications function as normal but include malicious content: trojans, crypto miners, adware, and more. Pirated VPN software or “free” versions of popular VPNs have also been compromised.

Malicious COVID domains: Thousands of COVID-19 domains have been purchased for use in malicious campaigns, or as place holder domains to potentially resell at a later point. The IT-ISAC operations team was able to locate 55,000 malicious COVID domains that were uploaded into TruSTAR, our threat intelligence platform. “According to Mimecast, during the first 100 days of the coronavirus pandemic, there was “a 33.5% rise in malicious activity—especially spam and impersonation attacks. Unsafe clicks have increased by more than 55%as malicious actors exploit a perfect storm of risk factors. These include: coronavirus-related chaos and uncertainty, users’ desire for information, and the increase in working from home.” [1].

Spoofed Email Addresses: To make phishing emails more successful, threat actors have spoofed health organizations including the World Health Organization (WHO).

Ransomware: Threat actors have tuned ransomware strains to use the coronavirus pandemic fears as a lure. A few organizations claimed to have stalled attacks against hospitals during the pandemic, but attacks against healthcare facilities have continued to occur. According to Mimecast, "Hospitals and other medical providers are facing a growing volume of ransomware attacks initiated via coronavirus us-themed phishing emails" [2]. Ransomware attacks are not unique to the Healthcare sector, they remain a threat across all industries. "Many recent ransomware attacks have been linked to the Emotet malware, which operates via a botnet of infected machines" [2].

CHALLENGE - SECURITY CONTROLS

Securing home offices can be difficult and since work from home decreases a company's visibility into how employees are utilizing their devices. Supplying and maintaining corporate-approved remote devices can be costly and time-consuming. Permitting employees to use their own devices comes with significant risks. Existing malware on an employee's device may be distributed into the corporate network. Opportunities for data theft could also arise from employees using devices on unsafe networks. These devices may be lost or stolen, possibly without safeguards in place to remote wipe or recover.

The risk of insider threats is also a concern. It can be difficult to monitor data without leveraging extensive Data Loss Prevention (DLP) technologies. The use of technologies like cloud-based web proxies, next-gen endpoint security, cloud identity providers, and CASB can help alleviate some of these visibility and control gaps.

Lastly, is the challenge of balancing security with usability. As employees are forced to work remotely, security measures may temporarily be lowered to allow employees to function effectively. Members have had to assume some risk to ensure productivity is not compromised.

CHALLENGE - VPN LIMITATIONS

Companies use VPNs to authenticate valid users and secure data in transit to and from their internal networks. VPN technology uses encryption and secure tunneling to protect data so that it is not intercepted. The use of VPNs is essential when data from a private network is shared across a public network, or from a less secure home office. They allow remote employees to access sensitive corporate data from a remote location that is less secure.

As the COVID-19 pandemic forced people to leave the office and work from home, the demand for VPNs rose sharply. Many companies needed to upgrade or invest in additional VPN technologies to manage the influx of remote workers. According to Top VPN.com, "Global VPN demand rose 41% over the last two weeks of March compared to the first half of the month. While overall demand would soften in April, it remains significantly elevated at 22% higher than it was before the pandemic was declared. Even in huge mature markets like the US, we have seen daily demand peak at 65% above the previous average" [3].

Companies have also struggled with allowing or disallowing split tunneling. With split tunneling, employees can connect to resources on a corporate network through the VPN connection. However, when the user wants to connect to websites outside the corporate network, the local network they have connected to will be used instead. Split tunneling can help avoid bottlenecks and conserve bandwidth on the corporate network. With remote workers accessing a variety of websites and streaming services, it is essential to separate that traffic from corporate VPN traffic. The disadvantage of split tunneling is that when enabled, users may potentially bypass gateway level security that may be in place within the company infrastructure. Employees will find themselves with fewer restrictions, opening the door for security incidents.

As employees move to new VPN services, the network security monitoring and control systems may see an increase in false positives and impossible travel detections. This can cause a strain on technicians who must scramble to whitelist and monitor these new connection points.

VPN challenges caused companies to explore alternatives to VPNs. One such technology is called Software-Defined Perimeter (SDP). SDP aims to provide employee with an on premise like environment. The key is to grant access only to the resources the user will need, following the principle of least privilege. SDP focuses heavily on zero trust technology to enhance the security of the remote connection. Because there are no open ports, companies can avoid snooping and scanning attacks on their network. Typically, there are no additional hardware or network integrations required, and employees can have the same experience remotely that they would have in the office. A lightweight client can be installed on the remote machine. Administrators can control access to applications regardless of whether they are on the remote machine or in the cloud. One of the largest areas of value is SDP's ability to provide security without bogging down the network. VPN traffic can cause bandwidth issues, especially as the entire workforce moves to remote locations.

CHALLENGE - TECHNICAL LIMITATIONS

Some employees with highly technical skills and responsibilities have been unable to work efficiently due to the closure of corporate offices and laboratories. Malware researchers for example, have had trouble experimenting with technical investigations such as reverse engineering from their home offices. Some specific machines and technologies can only be used from the corporate office and are often not feasible to use from home. The implementation of these technologies can be costly and logistically impossible for some employees due to power requirements and necessary storage capacity. There is often expensive licensing for certain software or costly hardware implementations that may be too large for a home office or require specific power/ventilation requirements.

CHALLENGE - NEW HIRES AND SEPARATIONS

Remote work has created many policy and logistical challenges to new employee hiring and employee separations. With new hires, training on corporate policies, including security, must now be done through video conferencing technology, videos, or other remote tools.

There are also the challenges of deploying secured devices to new employees. Internal technology departments no longer have access to corporate machines in storage. They now must order these products online and send machines to the employees, sometimes after they have been configured by the security team. However, there are often shipping delays and a shortage of high demand products such as laptops. Allowing a new employee to access the corporate network before they have been properly trained and vetted can cause the company to bear additional risk. As such, remote work has disrupted the entire onboarding process--from hiring to training, to providing them secure devices.

In the same way, the process for managing employee separations has also been disrupted and stressed. For example, there are challenges having machines returned from those who have been separated from the company. As such, former employees may retain access to sensitive corporate information even after they no longer work for the company. This also pertains to disconnecting access to corporate credentials. When a small minority of employees are working from home, managing remote access credentials is easier than when a small minority are working in the office. Therefore, disabling credentials as employees are separated becomes a larger challenge.

CHALLENGE - EMPLOYEE HEALTH AND SAFETY

With over 100,000 confirmed COVID-19 deaths confirmed in the U.S. schools, businesses, and government offices shuttered, and daily reports of new COVID-19 cases, the pandemic has created a sense of worry, panic, and anxiety. Fears about catching the virus, concerns over the well-being of loved ones, and extended periods of isolation can become a mental drain for many people. As such, managers have had to ensure the mental health of their team.

This stress and anxiety are even greater for those who cannot work from home. In many cases, these employees may operate some of the most critical parts of a company's business. COVID-19 has presented unique challenges in supporting those who are responsible for operating the most important parts of critical infrastructure.

Members of the IT-ISAC include manufacturers and producers of goods, from components for computers to farms and plants that underpin the global food supply. As such, many members have had to adjust to challenges surrounding employee safety. This has caused companies to change manufacturing or plant processes and procedures to implement to the greatest extent possible, social distancing, and providing employees with personal protective equipment. Extra cleaning procedures are implemented in a manner that minimizes disruption to essential operations.

Additionally, companies have encountered issues with employees getting trapped in foreign countries. Some employees were overseas when the pandemic struck, leaving them stranded and unable to get home.

CHALLENGE - MANAGING MORALE AND PRODUCTIVITY

As employees vanished from the office to work from home, managing the human element as well as securing corporate assets, became paramount. It also has impacted how people work. Where some people started the work from home push with great enthusiasm, after being under restriction for weeks their energy faded. In contrast, some people prefer working in an office setting and made the transition to work from home poorly. The rapid forced transition to work from home impacts people in different ways. While some employees may enjoy working from home, others might miss the in-person interaction and collaboration. While the production of some employees may have increased, the production of others has suffered.

Many managers are also adjusting to the new work environment. Managers must help their team members adjust to working remotely, even when the “new normal” may not fit their management style. In addition, as the stress and new life pressures on individual employees increase, managers must be more cognizant of these circumstances and their impact on productivity. It thus becomes vital to create and evangelize the context for the tasks at hand, take time to listen, be available for the many teleconferences that characterize the new norm, and give a little extra time for some one-on-one conversations.

How does this relate to Information Security? Disaffected employees tend to comply less with information security policies and methods.

They may cease to care as disaffection grows worse, or as worries about the pandemic overshadow their normally good behavior. At worst they may even go rogue. It is important managers communicate, maintain trust, and lean toward empathy in these challenging times. The trust you build now will pay dividends when your group returns to the office.

In sum, the forced transition to remote working has impacted employee health, morale, and productivity. This, in turn, creates new management challenges and pressures. These challenges will continue as companies build and implement “re-opening” work strategies.

CONCLUSION

COVID-19 marks an important chapter in the battle between network defenders and their attackers. The forced migration to remote work has expanded the attack surface, reduced network visibility, stressed security policies, practices, plans and personnel. The adversaries continue to deploy attacks that are known to be successful but are customizing them with COVID-19 themed lures. However, enterprises are fighting back by upgrading capabilities, investing in new tools and technologies, and ensuring the welfare of their employees.

SOURCES

1. **Mimecast Blog:** *Healthcare providers on the front line of the COVID-19 pandemic now also face the threat of catastrophic ransomware attacks delivered via coronavirus-themed emails*, by Mike Faden. Posted April 21, 2020. https://www.mimecast.com/blog/2020/04/healthcare-organizations-attacked-by-coronavirus-related-ransomware/

2. **Mimecast Blog:** *Spam and impersonation attacks have surged to the top of the list of cyberattack vectors driving a significant increase in overall malicious activity and unsafe user behavior, based on Mimecast's analysis of cyberthreats during the first 100 days of the coronavirus pandemic. Unsafe behavior may increase even more unless organizations take steps to ensure that users working at home create a secure environment and remain alert to the threats,* by Dr. Kiri Addison. Posted April 16, 2020. https://www.mimecast.com/blog/2020/04/threat-intelligence-briefing-surging-spam-impersonations-drive-increasing-coronavirus-cyber-threats/

3. **Top10VPN:** *COVID-19 VPN Demand Statistics* by Simon Migliano, March 27, 2020 updated April 20, 2020. https://www.top10vpn.com/news/vpn/covid-19-vpn-demand-statistics/