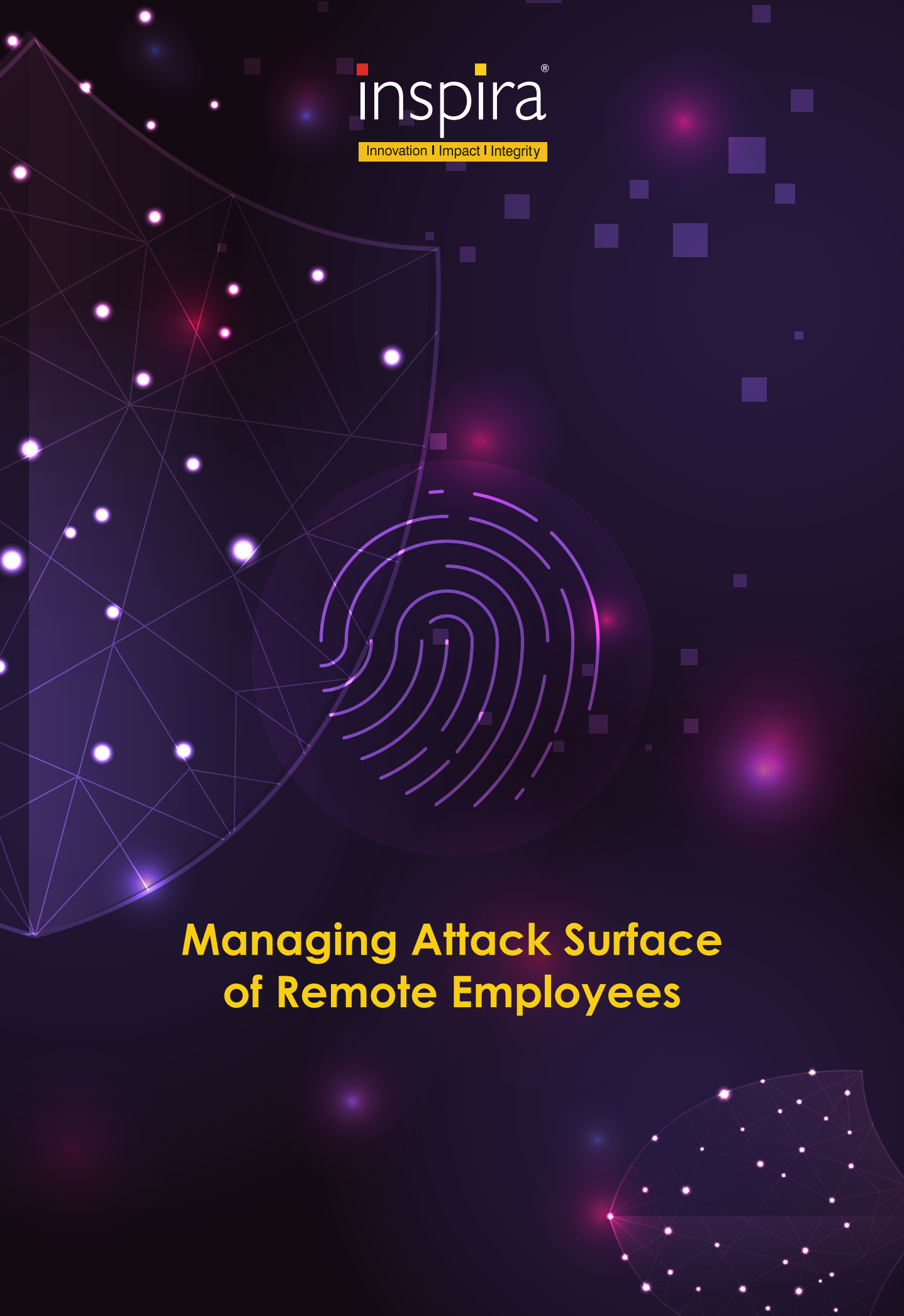
inspira®

Innovation I Impact I Integrity



Managing Attack Surface of Remote Employees

Globally organisations have had to shift their employees to work from home for the foreseeable future due to the COVID-19 pandemic. This means that organizations will have a largely (or entirely) remote workforce for the first time, instead of a few privileged employees who had this benefit till now.

This creates a situation that is ripe for cybercriminals and nation-state actors to exploit. There have been a rapid adoption of COVID-19 themed phishing scams, threat actors — both nation-state and cybercriminal — are quick to exploit new and evolving situations. Since the beginning in late January 2020, the volume of data increases, with larger spikes occurring as the number of COVID-19 infections increased through the month of February and March.

Some of the incidents identified were:

- In late January 2020, IBM X-Force researchers found cybercriminals using coronavirus as a phishing lure to distribute Emotet in a campaign primarily targeting Japan. The phishing emails claimed that the attached Microsoft Word documents contained health information and updates, but in reality contained a malicious VBA macro that installs a PowerShell script, which then downloads the Emotet trojan.

- Kaspersky issued an advisory about phishing emails that emulated the CDC (USA), in particular from emails containing the domains cdc-gov[.]org and cdcgov[.]org. In one instance, the URL contained within a phishing email led to a fake Microsoft Outlook login page, designed to convince victims to input their credentials. In another instance, victims were asked to donate Bitcoin to the CDC to aid in the pursuit of a vaccine.

- The AZORult malware observed by Proofpoint researchers was being delivered via email by phishing word documents that used COVID-19 as a lure in early February 2020. These attacks involved emails that contained Microsoft Office document attachments designed to lure victims and exploit a Microsoft Office vulnerability, tracked as CVE-2017-11882, which allows attackers to run arbitrary code in the context of the current user. The malicious documents contained what is purported to be an advisory on the impact of the virus on the shipping industry. Once the malicious document is opened, it installs the information-stealing malware "AZORult." The AZORult strain observed in the campaign did not download ransomware, as it has done in previous attacks.

Some other notable sophisticated phishing campaigns were with the below subject line

- "COVID-19 — Now Airborne, Increased Community Transmission" that appears to originate from the address CDC-Covid19[@]cdc[.]gov. (Confense research)

- "Attention: List Of Companies Affected With Coronavirus March 02, 2020", contained a malicious attachment that dropped Agent Tesla Keylogger. (Confense research)

- "Coronavirus: informazioni importanti su precauzioni", targeting Italian email addresses.

Phishing campaigns have been launched using the names of both corporates such as Fedex, Dongwoo Fine-Chem Corporation (South Korea) and Government agencies like WHO, Public Health Center of the Ministry of Health of Ukraine, Ministry of Health in the People's Republic of China, Office of Vietnamese Prime Minister Nguyen Xuan Phuc, etc.

The security teams have had to manage this sudden change in the organization's network topology which has resulted in a vastly expanded attack surface with little time to adapt to the new reality. For employees, generally, it means having to be even more vigilant of potential attacks. In this expanded, remote working environment, there are two focus areas of attack that need to be addressed by defenders: technical and organizational.

Teleworking Applications being exploited

The network baseline of the organisations has radically altered due to sudden rise in the remote working facilities being given to employees. Instead of an environment where 80% or more of the employees at an organization spent most of their time at a desk in an office, everyone is now accessing the same systems, but remotely. Besides the change in the network topology, this shift has also created challenges for user and entity behaviour analytics (UEBA) tools.

Employees will suddenly be accessing systems at unusual times, and they may be accessing systems they didn't regularly access previously. It will also be a challenge for organizations that built their security tools to primarily monitor the edge of the network, rather than the core. Employees, especially those using their own devices to connect to a VPN, may be introducing new malware into the heart of the network, and if the organization is not monitoring for malicious activity there, it may be missed.

Common remote working applications such as Zoom, Citrix, Slack, Skype, and Google Suite are already frequent targets of attackers, but when the usage of these tools was kept primarily behind a firewall, there was better control over the risk. Now that users will primarily be using these tools outside of the firewall, there is more risk of exploitation, especially if users are forced to use their own laptops, desktops, and smart phones to connect into the office.

In the last 90 days alone, there have been several published vulnerabilities exploited by malicious threat actors against these common teleworking tools. There has also been an uptick in DDoS attacks against some VPN providers.

While there has been a notable uptick in attacks against VPNs and other telework applications in recent months, these tools have been the target of cybercriminals and nation-state actors for much longer than that. The new reality of expanded telework simply gives these threat actors a chance to capitalize on the techniques they have already been developing for years.

Both nation-state threat actors and cybercriminals have been exploiting these vulnerabilities across technologies like Fortinet, Citrix, Palo Alto, Pulse Secure, etc.

Chaos Management

Net week weeks will overwhelm the help desks at many organizations with a sudden responsibility for keeping the network up for the remote users, using these to an extent that has not been seen before at this organization.

One of the challenges the help desk team need to address is the misconfiguration of services, which is a top risk to cloud services, thus increasing an organization's risk. Many of these remote work setups were designed and implemented in a short time span at a large scale, often with little documentation. This can leave users confused and unsure what to do, but still with a job to carry out.

This type of scenario is ripe for workarounds that may inadvertently expose sensitive information. For example, if an organization requires that all internal video conferences be conducted over the VPN, but users are having trouble configuring their VPNs, they may opt to hold those meetings outside of the VPN or switch to a different, unauthorized, video conferencing system.

Similarly, if users cannot reach internal file sharing systems, they may decide to share sensitive documents using consumer file-sharing solutions. It's common for individuals to reuse passwords between different accounts and applications, so it is likely that at least some people would sign up for these services using passwords already exposed on marketplaces in the criminal underground. Without the proper security controls in place, it may be impossible to know where all of these sensitive files are stored.

Threat actors will manipulate the fear around COVID-19 to scam individuals and organizations increasing the level of confusion and uncertainty. This will user more susceptible to phishing attacks — especially well-crafted ones. Given the potential for chaos, it is likely that users will be more likely to click on a fake tech support email or open a Word document that purports to be "VPN Instructions."

During this transition of remote working, employees will be regularly receiving inputs from helpdesk or the IT Team. Threat actors will try to exploit this expectation and make users fall for phishing emails, as seeing other users' personal email accounts in use could become more common during this transition period. Threat actors on dark web forums are openly advertising and discussing phishing content related to COVID-19. For example, FalosOfTanos, a member of a dark web forum, is selling a phishing method using an interactive COVD-19 map to deliver a malicious payload.

Another potential problem could be the influx of more commodity malware into your organization. As more users are connected to your network, often using their own computers that don't have the same security profile as an organization's systems, they could introduce new malware to your network via VPN. Even if your normal defences could easily squash these new attacks, the introduction of so many new machines, along with the increase in potential threats, could lead to threats being missed by an overwhelmed SOC.

Combating attacks on Remote devices

Combating these attacks requires planning and awareness on the part of everyone in the organization. We recommend the following steps:

- IT and security teams should have a well-documented policy and plan for working from home, as well as backup solutions if the primary solutions don't work. This documentation should include a minimum security profile (fully patched operating system, antivirus protection, and so on) for any system connecting to the organization.
- Security teams need to plan to ensure parity of security controls between the remote workforce and the on-premise workforce.
- Incident detection tools should work equally well with remote and on-premise systems.
- Both incident response and security controls should be tested regularly to ensure they are working as expected.
- Helpdesk support should ramp up, perhaps recruiting more technically savvy users to assist.
- Approved remote working applications need to be prioritized for patching and configuration changes, and monitored closely for announcements about vulnerabilities, proof-of-concept (PoC) exploit code, and configuration vulnerabilities in those applications.
- Monitor password dumps for employee email addresses
- Monitor for VPN activity from strange locations. Especially with all the travel restrictions in place, there should be more homogeneity in VPN connections.
- Test IR team capability on effective remediation of attacks remotely
- Create virtual Security Awareness sessions to make employees more vigilant about incoming email. There will be a spike in phishing and whaling emails, so be suspicious of everything and don't hesitate to pick up the phone and call someone if you suspect an email is fraudulent.
- Plan simulated phishing and social engineering attacks
- Keep in mind that your security and IT teams are going to be under even more pressure than usual during this time, management should be sure to provide for the emotional wellbeing of the team to help reduce stress levels as much as possible.

+91 9920335957 | +91 22 40569999

info@inspiraenterprise.com | inspiraenterprise.com

Follow Us