VPN TUNNELING AND REMOTE WORK CYBER THREAT PROJECT

(VT-RW-CTP)

REPORT CLASSIFICATION: UNCLASSIFIED

The primary objective with this project is to create a paper covering how virtual private networks (VPNs) can be compromised, the most popular attack vectors being used to compromise networks during this crisis, how security operations center (SOC) analysts are coping with the situation, and recommendations on how to better secure one's corporate network and personal computer. Particular focus is given to the compromising of encrypted tunnels, and how users could be exploited when working remotely.

30 April 2020

Project Manager: **Susanne Bitter,** CSFI
Chief Editor: **Aaron Ostrovsky**, Researcher
Senior Editor: **Maril Vernon**, Penetration Tester
Reviewers: **Paul de Souza**, CSFI Founder and **Christine de Souza**, CSFI Director

WWW.CSFI.US

The Cyber Security Forum Initiative (CSFI) is a non-profit organization headquartered in Omaha, NE, and operating in the Washington, DC, area with a mission "to provide Cyber Warfare awareness, guidance, and security solutions through collaboration, education, volunteer work, and training to assist the US Government, US Military, Commercial Interests, and International Partners."

TABLE OF CONTENTS

1. CSFI PROJECT TEAM PARTICIPANTS

The Cyber Security Forum Initiative (CSFI) thanks all the participants who volunteered their time, effort, and expertise in contributing to this effort. The diversified team of leaders, information security professionals, intelligence analysts, engineers, offensive testers, and project managers volunteered and collaborated in the CSFI portal contributing to this deliverable. CSFI thanks them for their contribution and hard work. Special thanks and credit to the following CSFI volunteers:

Name	Title	Country	Project Role
Susanne Bitter	CSFI - Head of Regional Strategic Alliances United Kingdom	United Kingdom / Czech Republic	Project Manager / Contributing Author
Aaron Ostrovsky	Researcher	USA	Chief Editor / Contributing Author
Maril Vernon	Penetration Tester	USA	Senior Editor / Senior Author
Arvin Verma	CSFI Fellow and Cyber-Risk Thought Leader	USA	Senior Author / Assistant Editor
Marek Hajn	SVP for Business Development IT-CNS, Inc.	USA / Czech Republic	Author
Baha Haktanir	Level II SOC Analyst	Turkey / Netherlands	Author
Ensar Seker	Cyber Advisor - NATO	Turkey	Supporting Author
Richard Guedes	Cyber Intelligence Analyst	Brazil	Supporting Author
Ashraf Aljammal	Associate Professor Computer Science and Applications Department The Hashemite University	The Hashemite Kingdom of Jordan	Contributor
Brandon Bates	Global Network Operations	USA	Contributor
Eric C. Kim	Graduate Student American University	USA	Assistant Editor
Matthew T. Dean	M.A. Candidate American University USAF	USA	Assistant Editor

2. KEY FINDINGS

The best things users and organizations can do to secure their virtual private networks (VPNs) and remote working environments include the following:

- Implementing strong password and lockout policies;
- Using multi-factor authentication (MFA) on all authentication portals;
- Using the most secure encryption algorithms;
- Implementing an intrusion detection system (IDS) with vigorous logging and monitoring; and
- Utilizing lock screens, log-off functionalities, and closing active browsing sessions even at home to terminate sessions.

3. ANALYSIS

3.1 Introduction to Secure Remote Working

3.1.1 COVID-19 Changes: Remote Workforce

The emergence of the novel coronavirus known for causing coronavirus disease 2019 (COVID-19) has led to the sudden upheaval of daily norms for companies and employees. Many companies' Business Continuity Plans (BCPs) either did not exist or did not account for the entire workforce and majority of operations going completely remote. When faced with the choice to shut down business operations or rapidly convert to a remote workforce, the pressure was put on information technology (IT) teams across the globe to mass deploy endpoint devices, migrate to cloud-based infrastructure, and/or quickly configure and support massive virtual private network (VPN) traffic. Many remote workers do not benefit from the enterprise-level controls of their robust corporate networks until they are connected via VPN.

A VPN extends an organization's private network in an encrypted tunnel across an unsecured public network, such as the Internet. However, as the extended arm of the network, VPNs are often the target for network cyberattacks. Additionally, many on-premises networks were not designed to cope with extreme demand for remote connectivity while maintaining high security standards. In parallel, the COVID-19 self-isolation deadline continued to extend, resulting in a perpetual user mindset of panic and uncertainty, leaving a perfectly set stage for new and creative cyberattacks against both VPN infrastructure and its end users.

VPN technology operates by "tunneling" through a public network connection between devices, which ensures the communication path is protected from public access, i.e. encryption. VPN requires authentication, which adds an additional layer of defense increasing its popularity with organizations and users.

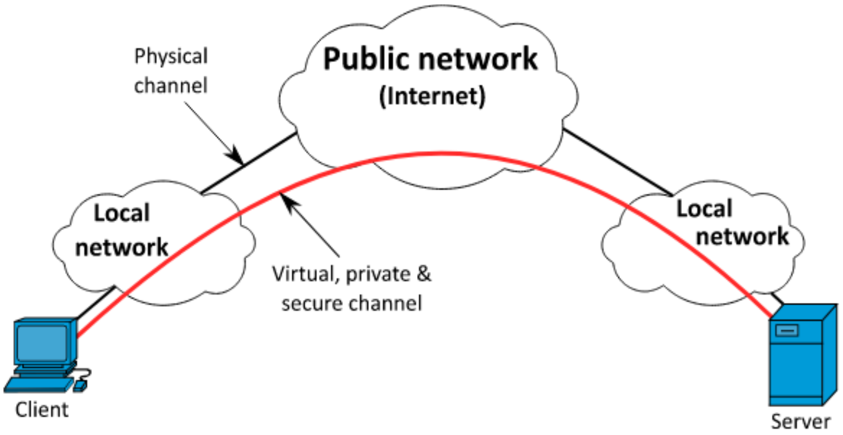

Figure 1: High-level VPN architectural diagram

3.1.2 Information Security During COVID-19

Information security professionals work to secure the confidentiality, integrity, and availability (CIA) of information, including a person or entity's personally identifiable information (PII), protected health information (PHI) or payment card industry (PCI) data as well as an organization's corporate data/intellectual property. Those are a lot of acronyms, which convey the collective effort to enforce users to select strong passwords and use VPNs to protect the privacy and accessibility of personal information, which could be used to steal one's identity or perform other unauthorized actions without the user's knowledge.

Some would like to approach most cyber related issues with the mindset that attackers have a default "type," but the truth is any person, at any time, using widely available and easily accessible tools, can successfully compromise a target if it is profitable for him/her to do so. Hackers range in skill, funding, and end goal from script kiddies to advanced persistent threat (APT) groups. A script kiddie is someone who can download open-source tools and easily perform basic script attacks. On another level, Hacktivists are part of a thought-lead group with a common ideological goal. Finally, APT groups, which are usually nation-state backed, have much more funding, large teams with decades of experience, and a specific goal in mind, such as compromising a country's industrial control systems (ICS). Hacker motivation is what determines the target and dedication to compromising that target. Occasionally, security is enough of a deterrent for a hacker to seek poorly-configured, low-hanging fruit elsewhere; in other cases, attacks will be attempted no matter the security measures.

Crises usually bring about an uptick in cyberattacks and security breaches. According to MoneyControl, "several global reports indicate that cybercriminals are capitalizing on the crisis to commit fraud and steal private and confidential information, including payment card data through phishing and social engineering schemes" (Bhatnagar, 2020).

3.2 Possible Ways of Compromise During Remote Working

Although several tactics are well-known, classified, and heavily evidenced by organizations such as MITRE in their Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework, no particular attack is more popular from one attack group to the next. Each will have its strategy combining tactics in new ways against previously unexploited vulnerabilities ("zero day" exploits) depending on whom they target and what traditionally works on those targets. Being supposedly well-guarded against one vector (and not knowing how well-guarded without conducting a thorough penetration test) is woefully inefficient against an advanced hacking method. What is important is implementing controls that head off the key things a hacker needs to go right to be successful vs protecting against one specific tactic over another.

What many may think of as the most "popular" attack methods gain notoriety due to the levels of effort and motivation. If motivation is high and level of effort is low, then there is a strong likelihood the hacker will pursue an attack. Conversely, if motivation is low and level of effort is high, chances are the hacker will not pursue an attempt. Automated toolsets such as Metasploit and Kali Linux have helped lower the level of effort involved for hacking system vulnerabilities, VPN vulnerabilities included, which will also drive higher motivation efforts for hacking attempts and thus causing an increase in service disruptions.

3.2.1 VPN Attacks

Understanding why VPNs are attacked requires understanding where they fall in a hacker's process. It is important to note that the end-goal of a hacker is often to remain undetected and maintain a persistent network presence. But first, s/he needs to gain initial entry into a system, establish a listening session, duplicate that session, and erase evidence of entry in order to maintain a persistent presence and continuously steal data. VPNs represent one avenue of entrance into a corporate network that is far-reaching and extends well away from the network "body;" this is why they are targeted.

The hacking Kill Chain, as demonstrated below, shows the paths an attacker can take to gain a foothold and establish a presence in a network. Payoffs increase as the duration of persistence increases, affording attackers more time to steal information while evading both intrusion detection systems (IDS) and intrusion detection response (IDR).

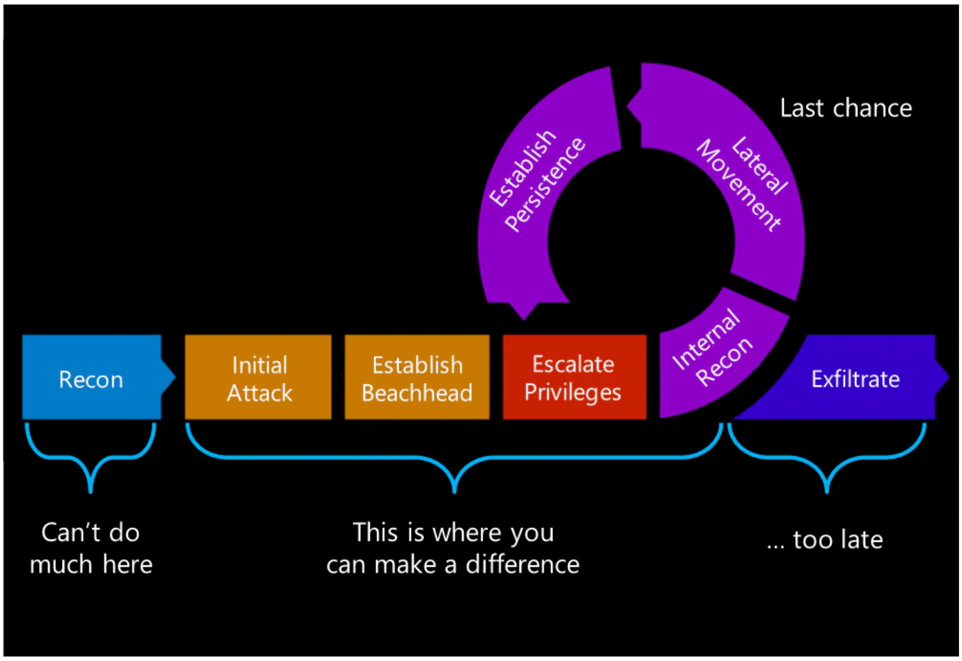

Figure 2: Cyber Kill Chain

In order to compromise a VPN, the attacker must figure out which kind it is, what encryption protocol it is running, and credentials. Mitigating any one of these infiltration avenues will effectively thwart a simple attempt to attack one's VPN.

Current VPN encryption protocols can be robust and offer significant protection. However, nothing is 100% immune to hacking. Traditionally, Internet Key Exchange (IKE) VPNs are those that have been targeted because the IKE (currently on v2) negotiates a security association between clients to establish the tunnel. This process can be difficult to do with many current VPN setups, but the process usually looks something like the following: identify the VPN being used, confirm that aggressive mode is enabled, identify group ID, identify XAUTH credentials, extract hash, crack hash, and join VPN.

Most VPN service providers offer to store authentication data such as usernames and passwords for their customers, which can create significant security risks, such as the following: storing unencrypted usernames in a file or the registry, storing the password in a scrambled form, storing plain-text passwords in memory, and weak registry or file permissions for stored credentials. In addition, error messages and packet headers can divulge information about the type and version of VPN one is running.

To combat such risks, the following mitigation techniques have been recommended:

- VPN Tunnel Fingerprinting – VPNs may hide the user's IP address, but other information about the system, such as the operating system (OS), could be retrieved.

Fingerprinting is a method that allows an attacker to narrow down the search space for exploitable weaknesses on the target system by analyzing traffic and inferring information about a device from its behavior.

- Use Multi-Factor Authentication (MFA) with VPN – MFA requires a user to demonstrate at least two forms of authentication, such as a combination of something you know (password, PIN), something you are (facial recognition, fingerprint, retinal scan), and/or something you have (token, access card, badge).
- Avoid using vendor-supplied default configurations
  - Password history and rotation should be enforced; every 90 days and a history of the past 30 passwords should not be repeated.
  - Enable account lockout after three attempts. Inactive accounts and sessions should automatically timeout after a recommendation of no more than 15 minutes. VPN connections often persist after the endpoint has been locked, but it can still be accessed remotely.
  - Leverage identity access management (IAM) permissions. Grant access to resources based on the security concept of least privilege. Do not make everyone an admin-level user, segregate which users can go which places on the network. That way, if an end user account becomes compromised, the amount of data that is accessible is limited.
- Routinely patch – In an alert published in August of 2019, the United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Agency (CISA) noted that over 14,500 VPN servers were identified to be vulnerable due to missing patches.

3.2.2 User Exploits

The strongest and weakest link in any cybersecurity program are people. One can have the most advanced threat intelligence program with active network scanning, but it only takes one employee to click on a link that could effectively bring down an organization's network. No matter how secure the organization is, no matter how many sophisticated solutions are implemented and policies are enforced, if personnel are not operating under the established governance processes, the security layers of defense-in-depth become less effective at protecting the organization. Historically, IT departments were responsible for implementing solutions to aid and support various business functions and processes, including security-based solutions. More often than not, these solutions are developed and deployed without a complete understanding of the business need. As a result, a disconnect forms between end users and IT resulting in workarounds that might impact or affect an organization's security posture.

Process automation is an approach to reducing user interactions; however, that alone is not sufficient in reducing user error. Security awareness and constant education are two useful tools to inform users about threats and vulnerabilities affecting them and the organizations they support.

Finding the right balance between security, sophistication, and user design can oftentimes be difficult, but it starts with understanding the organization's risks, implementing education, and continuous monitoring. When developing security policies, solutions, and practices, keeping the end user in mind is essential when implementing security controls.

For example, when implementing multi-factor authentication, will the token be installed on the user's end device, or will a physical token be given to them? When they access the website, what will the user see when they are asked to provide their username/password and token key? The emphasis here is to drive ease and efficiency with these complex solutions without making efforts so difficult that adoption is abandoned and/or a bypass method, typically less secure, is used by personnel.

The better-informed end users understand why security policies and practices are critical, the higher probability they will adopt and follow them. This is a crucial part of all security efforts. For example, information security professionals agree that one of the biggest risks to an organization is insider threat. Additionally, providing security awareness contributes to the mitigation and prevention of successful phishing campaigns. Teaching users what to be aware of during their day-to-day activities and conducting regular phishing assessments and periodic Security Awareness Training is a way to drive enforcement and testing. Coincidentally, conducting these kinds of tests on employees is a requirement for many certifications such as ISO 27001, PCI, and more.

In today's world, a personal computer is not only your desktop or laptop. More and more people work on their tablets and smartphones. In the case of using iOS, iPadOS, or Android-powered devices, they all have built-in VPN. Most VPN solutions offer multi-platform usage, which means that with one subscription, one can use it across all his/her devices. Some of these services offer family plans as well as business or corporate plans. With one subscription, one can easily put a VPN on all the family devices. The advantage here is that most of these VPN apps run in the background and are fully automated. Once set up, it will run all the time unless your device is connected to a trusted network specifically indicated by the user. For families, it is always good to consider using parental control settings that are available on many devices or/and applications. By using such control, children can be restricted from accessing websites and services with inappropriate content, and restrictions can be placed on their device usage time for playing games, watching YouTube, etc.

The items below are general security recommendations for users:

- Use a personal firewall – a personal firewall is a software that monitors and controls the network traffic by permitting or denying the traffic based on predetermined security policy such as OPNsense, pfSense, SmallWall, etc.
- Install Antivirus (AV)/Anti-Malware – AV is software that can prevent, detect, and remove malicious programs. Popular AV examples include Avast, AVG, Symantec, Avira, etc.
- Leverage Anti-Adware tools – Adware is software that is installed on the computer (often with other software) without the user's knowledge to provide more effective advertising methods by following the Internet activities and habits of computer users. Anti-adware can scan and remove such programs.
- Update OS – Regardless of OS version, having automatic updates on, is a good practice. Updates can set to run overnight so they do not interrupt the user's daily workflow.
- Update Applications
    - Check application stores, such as the App Store, Google Play, and the Microsoft Store, and in-app updates to ensure they are up to date with the latest security patches. If the OS offers it as a feature, turn automatic updates of applications on.
    - Control application permissions – Turn off unnecessary permissions on settings.
- Secure home wireless network
    - Using a wireless network without any security settings and/or without a password may be convenient, but this is not the best way to protect sensitive data. Wireless networks are discoverable and without any protection, they are vulnerable to malicious attacks.

- Setup a guest Wi-Fi network – Many routers support guest networking features. Creating a segregated guest network can minimize the attack surface. So even if your guest downloads any malicious program, it would not affect main devices.
- Consider purchasing advanced Wi-Fi solutions – By purchasing a commercial Wi-Fi solution such as Eero, Google Wi-Fi, Orbi, Turris Omnia, etc., onr can make wireless communication even more secure and reliable with high-speed wireless connections.

- Consider encrypted solutions when sharing sensitive data – Public cloud solutions are the easiest to use, but in most cases, are not safe enough if one needs to share sensitive data. Using solutions for an encrypted file transfer is a good practice to keep data-in-motion safe.

3.2.3 Corporate Network Exploits

Whether in a large or small organization, setting strong policies, enhancing already existing controls, and providing education to end users are the first initial best practices to help drive situational awareness. Organizations that conduct sensitive business will always be a target due to the nature of their operations. For example, online banking enhances the risk of a company being identified and targeted for financial crimes. Large conglomerate/Fortune 500 companies have a brand associated with them, which expands the threat surface. This could range from brand/website defacement, economic tampering, intercepting banking transactions, to stealing intellectual property and personnel PII data. As a result, organizations need to be able to identify and respond to a broad level of cyber incidents.

Driving governance of appropriate applications to connect to an organization via VPN, multi-factor authentication and using only corporate owned devices are some steps that can help reduce the level of risk an organization faces. Maintaining a strong level of governance around asset acquisition and implementation will also assist in ensuring unsecured systems are not being utilized by unauthorized individuals, teams, and/or business units without the appropriate approvals and reviews. Additionally, ensuring proper permissions of users and admins is critical in the mitigation of appliance and/or system misconfigurations. Oftentimes, privilege escalation could result from personnel changing settings with or without their knowledge. As a result, it is important to only allow admin rights and access to authorized personnel and to continuously audit to ensure actions performed on assets are done appropriately.

When trying to identify any malicious attacks, most enterprise appliances utilize automatic threat detection based on heuristics, prior historical data, and application whitelisting/blacklisting. Additionally, the use of certificates that are constantly refreshed when the devices are physically connected to the organization's network will help drive assurances that any potential threats are detected in a timely manner.

For smaller-sized organizations and/or those who cannot afford enterprise solutions, setting strong policies, enhancing already-existing controls, and driving education to end users are the first initial best practices to help drive situational awareness of any potential inbound threats against the organization. There are also many tools that could be used by an organization to protect its own networks, such as the following:

- Firewalls – Considered as the first line of defense of any network, firewalls protect against initial access via open/unused ports and insecure protocols and services running on those ports (such as Telnet).
- Network Intrusion Detection System (NIDS) and Network Intrusion Prevention System (NIPS) – NIDS is able to detect intruders' activities over the organization's network,

while NIPS is able to respond to suspicious activities over the network and prevent intruders from breaking into the organization's networks.

Additional recommendations include the following:

- Reviewing and closing unnecessary ports – Review the logs and determine which ports that are currently open are not being used or accessed by any services and disable them. A free, open port is a door in which a hacker can assign themselves and use without the IDS knowing or flagging the activity.
- Create firewall rules – Make sure the rules, in order of operations, are configured for the least amount of access necessary and limit the ingress and egress by IP address range, if possible.
- Utilize IDS/IDR/IPS – This can be via an automated tool with AI built-in to anti-virus software, a SIEM, or an MSSP monitoring logs and activities.

3.2.3.1 VPN Best Practices

The recommendations outlined below are basic VPN best practices. Please defer to in-house IT, security teams, and third-party vendors to ensure specific VPN setup adheres to industry standards:

- Use a different local area network (LAN) IP subnet at both ends while configuring VPNs between different sites. For example, if the site one connects to uses a 192.168.x.x addressing scheme, then use a 10.x.x.x or 172.16.x.x - 172.31.x.x subnet. Another option would be to have different subnet masks. When changing the router IP address, the devices using dynamic host configuration protocol (DHCP) would automatically pick up an IP address in that subnet.
- Use the static public IP on the wide area network (WAN) interface of the router for stable VPN connectivity.
- Select the same level of encryption and authentication for the VPN, router, and all applicable infrastructure.
- If using a pre-shared key (PSK), be sure the PSK and key lifetime entered are the same as the remote router. Key lifetime is how often the system changes the key. A PSK can be whatever the user choses; however, depending on the device, there may be some characters that cannot be used.
- For most VPNs, clients do not need a certificate. In contrast, OpenVPN requires both client and site certificates. A certificate is preferred since it is considered more secure.
- Set the security association (SA) lifetime in Phase I longer than the Phase II SA lifetime. If the Phase I is shorter than Phase II, the tunnel may have to renegotiate back and forth frequently.

The additional list below includes tips provided by Computerworld (Heller, 2006):

1. Utilize the strongest possible authentication mechanisms available for VPN Access – This will ensure that both obtaining access to the secure network as well as keeping any encryption mechanisms and keys secure are only available to authorized personnel.
2. Utilize the strongest encryption for VPN Access – This is especially crucial as well as the protection of data during transit is as difficult as possible to intercept data while moving across public networks.
3. Limiting access of VPN capabilities to those with business justification and only when necessary since VPNs allow access to an organization's internal network,

limiting who can use this access can help prevent accidental or malicious access to the organization's network and releases of organizational data.

4. Providing access to certain sites through the use of multi-factor authentication and/or network segments – limiting certain sites that don't hold data classified as sensitive can provide numerous benefits such as reducing strain on VPN servers as well as lowering the risk of potential malicious access. Using already existing technologies like multi-factor authentication can help keep information protected from unauthorized users while also reducing the risk exposure based on risk acceptance.
5. Enabling capabilities such as email without requiring a VPN connection to be enabled – similar to point 3 and 4, allowing low-risk activities to be accessed by personnel without requiring VPN access will help reduce the risk exposure of VPN attacks being exploited by end users either accidentally or maliciously.
6. Implement a strong password policy for all accounts, including VPN – similar to point 1, having a strong password will add to the defense in depth supporting protective capabilities to ensure the VPN connection itself is secured.
7. Implement anti-virus, anti-spam and local firewall capabilities to remote users and drive firm requirements requiring its use - adding to the defense in depth capabilities to support security controls around the organization's environment, endpoint devices and ensuring that anything that the user isn't in direct contact with, is still caught and remediated.
8. Isolate devices connecting to the VPN to allow for verification of the device prior to enabling VPN connection – this will ensure that if there are any vulnerabilities with the endpoint device, they are identified and remediated prior to the device being granted access to the VPN and possibly opening more risks.
9. Require that no other VPN and/or remote-desktop/remote-access capabilities be used while utilizing the corporate VPN – similar to point 8, limiting access of other applications/systems will ensure any other vulnerabilities are not exploited when a user accesses the organization's network via the VPN.
10. Ensure that encryption and other protective mechanisms are in place for wireless networks – similar to point 7, adding this control capability helps enhance defense in depth controls and reduces the possibility for a hacker to access and view data being transmitted across the network both with and without the VPN enabled.

Although CSFI is vendor agnostic, many technology industry leaders offer best practices for their solutions. For example, Cisco Business provides substantial documentation online for VPN and network configurations for their Cisco Appliances.

3.2.3.2 General Best Practices

As mentioned earlier in this report, most hackers exploit known vulnerabilities and misconfigurations. Keeping ahead of any potential backdoors or exploit opportunities can help deter a multitude of potential threats and vulnerabilities, not just for VPNs. For example, Windows 7's end-of-life affected many users and organizations. While most large organizations have a significant defense, this alone is not enough to help prevent vulnerabilities from being exploited. Oftentimes, most end-of-life management responsibilities fall under asset management, so having a strong partnership between Information Security and IT is crucial.

The following outlines specific areas of focus:

- Deploying high-availability environments enables rapid and redundant patch management

- Regular policy checks
    - Manage user and administrator permissions
    - Manage vendor relationships
    - Oversee third-party integrations – This will prevent known vulnerabilities from being exploited. Understanding which security controls vendors have implemented is critical prior to using their services.

4. SECURITY OPERATIONS CENTER (SOC) RESPONSE

Being front-line defenders, SOC analysts are responsible for analyzing and responding to security threats. The almost immediate transformation from working in corporate offices to working from home/remotely, which requires remote access and remote connectivity, has changed the typical type of traffic and threats SOC analysts would encounter in a daily routine. Given such a chaotic situation, attackers can mobilize with various techniques, tactics, and procedures in an unbelievably short period of time. This leaves SOC analysts no choice but to take a new, holistic approach to battle control of the organization's digital footprint.

While relying on traditional security controls which are part of a reactive strategy, proactive techniques should also be applied to help in the battle against threats and vulnerabilities. Threat-intelligence and threat-hunting functions have become more prominent in order to increase the level of proactivity and also improve the overall security posture of enterprises. Through this approach, SOC analysts have a higher chance not only to detect malicious attempts but also to find existing vulnerabilities, potential compromises, lateral movements, and data exfiltration. Subsequently, SOC analysts are compelled to consider all the contributing factors.

With the rise of remote work across organizations, overseeing vulnerabilities has shifted dramatically. Typically, these sorts of activities required SOC analysts to be on-site, with access to numerous toolsets scattered across the corporate network, until now. Many SOC analysts are now actively working to identify mechanisms to monitor corporate networks without having the intelligence collected leaked outside for bad actors to utilize. Furthermore, some SOC analysts and leaders, among corporate employees, are using their corporate-owned laptops, VPNs, firewalls, and many other capabilities to continue operations of ensuring the organization. As a result, its many users are not as impacted by cyber incidents during the course of their work activities due to the many layers of defense-in-depth and level of security controls on these corporate-owned assets. Meanwhile, many small or medium businesses have resorted to using personally owned devices, which may not have the same level of security controls as a corporate device would. While combatting this through a remote desktop connection or solutions like Citrix, the risk still stands as personal devices do not have the same level of cyber assurance as a corporate-owned device would. While most organizations of this size will not have dedicated teams or departments along with budgets in place to have their own SOC/NOC monitoring, they will either outsource this service to a managed service provider for action or will not have access to enterprise-level support capabilities, thus putting them at higher risk. In addition, implementing security best practices will help reduce the risk exposure small/medium businesses could face without impacting day-to-day operations as well as in times where a business continuity/disaster recovery plan would be activated.

Therefore, ensuring that all corporate activities occur on corporate-owned devices is highly recommended. This will ensure that actions performed are done so in a secure manner, drive higher confidence in actions performed, and provide visibility to SOC analysts who will be able to maintain logs to analyze suspicious activity. Moreover, unnecessary and expired third-party user accounts or formal employees' accounts should be immediately eliminated. As a case study, Walmart's breach is a reminder of what a forgotten active VPN account could lead to; threat actors prefer using these accounts in times when higher VPN activity is expected than normal to remain undetected.

Typically, what to look for can be difficult to identify as hackers employ a variety of techniques to conduct attacks. One reason is enterprises cannot make use of the typical elements of perimeter security such as firewalls, IPS, and IDS devices when VPNs are utilized due to the nature of how they work. These security measures have at least visibility on any connection attempts coming from public networks to private networks and vice-versa. However, that is not the case for VPN traffic, and a reactive response not enough in this environment.

Based on the list of attacks detailed earlier in the report, the most common items to observe are a large amount of password fail attempts, unusual IP activity, potential denial of service or distributed denial of service (DoS/DDoS) type activity from unknown devices, and/or any activity from locations that the organization does not do business in or is not historically similar. These types of scenarios are already built into some cloud solutions and SIEM products looking for such activities and other types of anomalies. Using threat intelligence, analysts can create active lists or lookups to cross check the source of inbound connections against blacklists to identify the IPs with a bad reputation. This type of analysis is not limited to only IP addresses; any other indicator of compromise (IOC) information (domain, hash, etc.) can also be harvested from web/dark web with various OSINT techniques and kept as watchlists/lookups.

For SOCs with relatively limited capabilities, analysts can create new rules, generate periodic reports, and perform some manual data analysis on the generated data. Keeping an eye on failed authentications is crucial to ensure that authentication related rules/use cases/alerts include the used VPN source type. If necessary, thresholds for VPN authentications could be modified to more sensitive levels. Lockout-policy for VPN accounts could be also considered; this way brute-force attacks, dictionary attacks, and rainbow table attempts could be prevented. As mentioned earlier, some of the known vulnerabilities in well-known vendors and their products should be low-hanging fruit and fixed or mitigated with workarounds immediately since impact, remediation, and risk processes are usually known. Network access control (NAC) solutions could be very useful to have endpoint visibility, to locate unknown or non-corporate devices in the network, and also to take preventative measures such as removing or quarantining those devices. However, enterprises need to have a full asset inventory and implementation of policies in order to make good use of network access control solutions.

5. CONCLUSION

The primary objective of this report is to educate and explain how VPNs can be compromised, particularly during the COVID-19 pandemic where much of the workforce is working remotely. To minimize VPN risks, it is vital to educate the workforce on how to maintain a secure remote working environment, to raise awareness of potential avenues of compromise during remote work, and to understand the usage of SOC response. Therefore, it must become the user's responsibility to understand how to behave when user exploitation has occurred or receive direction from the company's IT department in order to prevent a domino effect of compromise. Lastly, this report included some best practices and recommendations to mitigate cyberattacks on the VPN and ensure an effective, secure remote working environment.

6. REFERENCES (ALL SOURCES)

- Bhatnagar, Nitin. (06 April 2020). *Securing Payment Card Data During COVID-19 Pandemic.* MoneyControl.com. Retrieved from https://www.moneycontrol.com/news/technology/fintech-securing-payment-card-data-during-covid-19-pandemic-5113541.html
- Cisco. (15 January 2020). *Cisco Business VPN Overview and Best Practices.* Retrieved from https://www.cisco.com/c/en/us/support/docs/smb/routers/cisco-rv-series-small-business-routers/1399-tz-best-practices-vpn.html

- Heller, Martin. (02 October 2006). *10 Tips to Secure Client VPNs*. Retrieved from https://www.computerworld.com/article/2547058/10-tips-to-secure-client-vpns.html
- Winder, Davey. (13 January 2020). *U.S. Government Issues Powerful Security Alert: Upgrade VPN or Expect Cyber-Attacks*. Retrieved from https://www.forbes.com/sites/daveywinder/2020/01/13/us-government-critical-security-alert-upgrade-vpn-or-expect-continued-cyber-attacks/#46db46de6f70
- Zetter, Kim. (04 October 2009). *Big-Box Breach: The Inside Story of Wal-Mart's Hacker Attack*. Retrieved from https://www.wired.com/2009/10/walmart-hack/