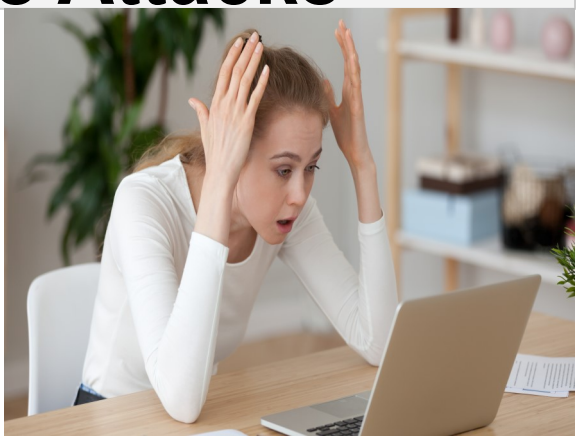
Bank of Botetourt

SEPTEMBER 2020 Issue 9

Fileless Attacks

There is no doubt that security measures continue to get better and better, producing improved methods to block or and identify malware. However, cybercriminals understand that all too well and are adapting to the changes as they come. One of the ways hackers are able to circumvent security points is by using fileless attacks. Fileless attacks do not require malicious software to infiltrate networks, instead they use tools readily available within the system.



Fileless attacks are considered one of the biggest threats to companies and continue to be on the rise. In 2019 Trend Micro stopped over 1.4 million threats. For years, cybercriminals often looked for ways to install malicious files on your computer via different methods of phishing. But a fileless attack doesn't require that. Instead, it can use software and applications that are already built into your operating system. This presents a significant problem because fileless malware is memory-based, not file-based, making them sometimes undetectable by antivirus software. Typically when you make the unfortunate mistake of opening a phishing email or opening a malicious link, there is a file that antivirus software can scan as it's saved to or opened from a drive, therefore there is a trail or a footprint of file activity that allows you to look back and review if any damage has been done. However, fileless malware bypasses that making it difficult to identify.

To protect your organization against fileless malware here are some things to consider.

- *Always be careful when downloading and installing applications.*
- *Keep up-to-date with security patches and software applications.*
- *Make sure you always have the latest version of applications installed.*
- *Update your browsers.*
- *Consider security solutions that include memory analysis and protection.*
- *Consider Endpoint security tools that include detection and response.*
- *And always be on the lookout for phishing emails.*

This type of malware is not a new threat but makes it challenging because it is hard to detect. Organizations should use a multilayered defense. However, new techniques and tools continue to be developed to help stop fileless malware attacks in hopes of preventing network security breaches.

Sources:
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/security-101-how-fileless-attacks-work-and-persist-in-systems

EQUAL HOUSING LENDER Member FDIC

Bonsack

Buchanan

Care Center

Cave Spring

Daleville

Eagle Rock

Fairfield

LakeWatch

Lexington

Natural Bridge

Peters Creek

Salem

Troutville

www.bankofbotetourt.com
www.facebook.com/botetourt
(540) 591-5000

Five Reasons a VPN Is Important

Especially During COVID-19

Nowadays, working remotely is the "new normal." Six months into the COVID-19 pandemic, many organizations are extending their work from home schedules; for some, indefinitely. Companies are rethinking their security measures to avoid any loopholes that can possibly lead to security breaches. More than ever VPN's are a critical tool for ensuring data is transmitted safely while avoiding the prying eyes of cybercriminals.

A Virtual Private Network (VPN) provides online privacy and anonymity by creating a private network from a public internet connection. It allows your IP address to remain hidden, so your online activity is unable to be traced. More importantly, VPN services establish secure and encrypted connections to provide greater confidentiality. While many are working remotely due to the pandemic, it is critical to have a secure connection. Some employees work with and access sensitive data from their company's network, making them a prime target for a cybercriminal. Phishing campaigns depend on human vulnerabilities and manipulation; however, having a VPN connection provides a way for employees working from home to do so securely.

Business transactions on an unsecured Wi-Fi network could mean possible exposure of sensitive data. Here are five reasons why a VPN is extremely important, especially during the COVID-19 pandemic.

1. It Hides Your Browsing History

It is no secret that all your internet searches can be tracked by your internet service provider. Most websites keep a history of your browsing activities and it can be traced back to the IP address used. We have all seen the barrage of related ads we get after doing online searches for something as mundane as a pair of shoes. Surfing the web using a VPN will help eliminate that annoyance.

2. Your IP address and location Remain Secret

Your IP address can provide a lot of background information. Capturing your IP address means capturing your internet habits, location and device used when doing the search. It can be extremely invasive. Having a VPN uses an IP address that is not yours, hence allowing you to use the internet incognito. It also protects against having your search history gathered, viewed, or sold.

3. Your Devices Will Be Protected

A VPN can help protect your devices, including desktop computer, laptop, tablet, and smart phones from cybercriminals. A VPN also helps protect the data you send and receive on your devices so hackers won't be able to watch your every move.

4. Protection Against Spam

Because a VPN allows your usage on the internet to be hidden, hackers will not have the ability to track your email address and send you spam emails that are most likely phishing expeditions.

5.Some VPN Services Offer Malicious Website Detectors and Firewall Protection.

There are variety of VPN services that offer advanced protection. Malicious website detector is a database that contains phishing website links that have been deemed dangerous. If such a site is visited, the user will be warned immediately not to share any data with that site. Also, the firewall protection will prevent any hackers or malicious software from accessing your device without your permission, thus preventing any type of phishing threat to occur.

As of today, there are no clear predictors of when the pandemic will end, but VPN's are an extremely valuable tool during COVID-19. To remain safe, it is critical that organizations take all necessary measures to scale up and reinforce their corporate VPNs to protect against possible attacks.

Sources:
https://us.norton.com/internetsecurity-privacy-what-is-a-vpn.html
https://www.vpncrew.com/5-ways-vpn-can-protect-you-from-advanced-phishing-threats-that-use-https-protocol/