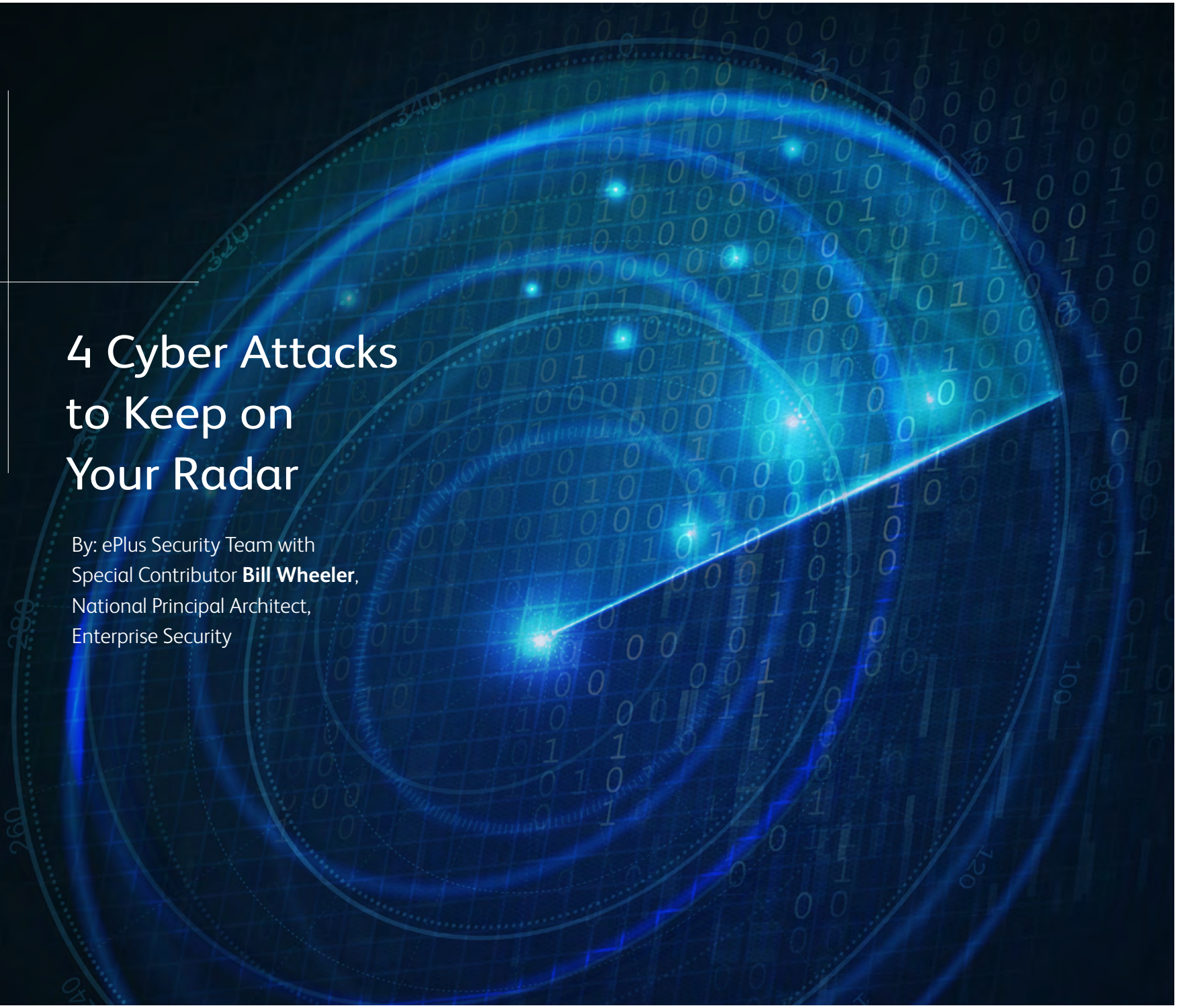
Where Technology
Means More®

4 Cyber Attacks to Keep on Your Radar

By: ePlus Security Team with
Special Contributor **Bill Wheeler**,
National Principal Architect,
Enterprise Security



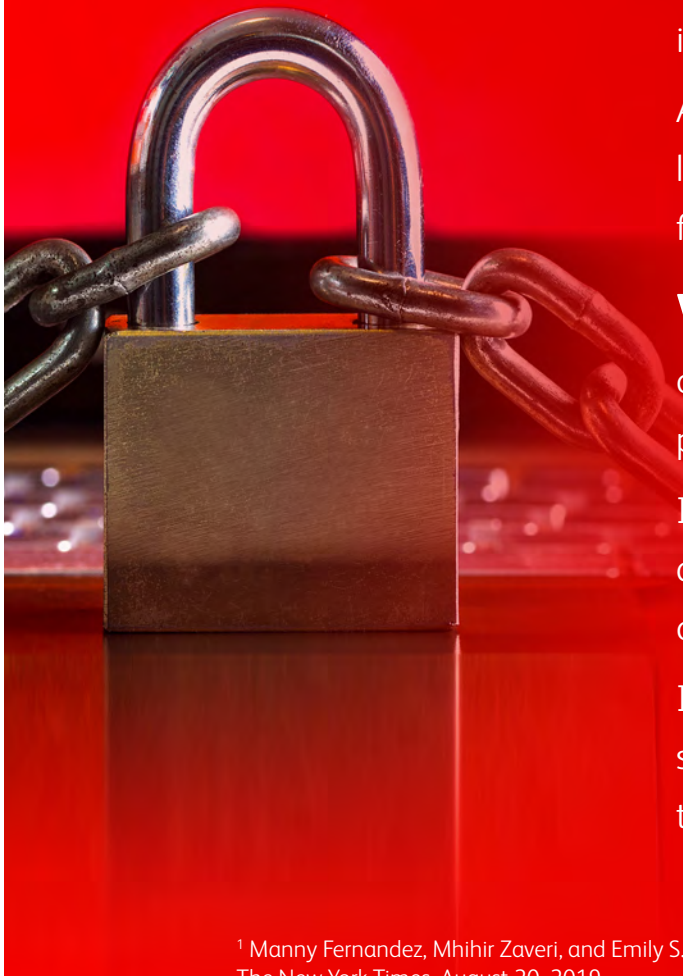
Information technology security is a race with no finish line. It's white hats against black hats from now until forever. As a consequence, security experts will tell you that absolute security is unattainable. The black hats will always be looking for ways to infiltrate, exploit, and attack your infrastructure.

In this world, the best defense is to be a less attractive target. This means adopting sufficient security measures, policies, and especially workforce practices to detect imminent threats, deter attacks, and encourage hackers to go after easier targets.

Building sufficient defenses starts with understanding the ever-evolving threat landscape. For late 2019, here is my list of the 4 critical threats that will keep you awake at night. Familiarizing yourself with these threats and potential defenses can help you assemble a security strategy that is both effective and sustainable.

e+
Where Technology Means More®

1. Common attack: | Ransomware



What is it? While ransomware attacks take several forms (lockers, scareware, doxware, and so on), they all use malware code to lock and encrypt data. Ransomware is often distributed as booby-trapped attachments or links in emails.

A new form of ransomware, called malvertising, places malicious advertising on legitimate websites and uses browsing visits to queue up an attack. With one click on a file or hyperlink (or even just browsing near an infected iframe), an attack is underway.

Why is it a problem? Ransomware attacks are very common. They can affect anyone with an email account. Increasingly, cybercriminals are targeting private companies, governments, and healthcare and educational institutions.

In August 2019, for example, systems owned by 22 Texas municipalities were attacked and needed weeks to bring public services back online.[1] At about the same time, two cities in Florida paid almost $1 million to recover their data.

Insurance sometimes offsets these costs, but paying the ransom does not guarantee a successful outcome. One industry survey suggests data is only unlocked about half the time—even when victims fully comply with ransomware terms.[2]

[1] Manny Fernandez, Mhihir Zaveri, and Emily S. Rueb. "Ransomware Attack Hits 22 Texas Towns, Authorities Say." The New York Times. August 20, 2019.

[2] Warwick Ashford. "Only Half of Ransomware Payments Honoured." ComputerWeekly.com. March 7, 2018.

e+ Where Technology Means More®

1. Common attack: | Ransomware

What can you do? Patch applications and other software. Create multiple backups of critical data, and locate backups in secure, offsite storage. Lock down drives and servers, and set policies that restrict system access. Scan email for threats, and authenticate all email traffic to prevent spoofing. And configure firewalls to block malicious IP addresses.

All these system-side controls are helpful, but your most important defense is an educated workforce. Cultivating a “trust no one” attitude when online or communicating over connected infrastructure is essential in today’s threat-rich environment. Training employees to see their work-related mobile devices as an extension of your infrastructure is also vital.

2. Common attack: Phishing and Smishing

What is it? Ever received an email from a service provider apologizing for suspending your account and offering to help you sort out the problem? Ever open up a new tab and checked your supposedly locked account and found no problem? Then you – security superstar – avoided a phishing attack.

With phishing, a criminal adopts a known identity and uses that position of trust against you. Often, the email contains a link to a realistic-looking but fake web page. Smishing, also known as SMS phishing, follows a similar attack strategy but uses a text message instead of an email to gain your trust.

Cybercriminals can use both types of attacks to gain user privileges and then load keyloggers, a type of malware, on your system. As the name suggests, keyloggers capture login credentials and send them back to the hackers so they can continue the attack.

2. Common attack: Phishing and Smishing

Why is it a problem? Cybercriminals are increasingly using phishing and smishing to go after large organizations. While the payment services industry has been a prime target for years, a recent APWG survey suggests hackers are shifting their attention to Software-as-a-Service (SaaS) and webmail services.[3] Both techniques use social engineering and technical subterfuge to steal personal identities and sensitive credentials.

SaaS and webmail services are fundamental business tools. Organizations rely on email to communicate, and they are increasingly using SaaS for sales management, customer relationship management, human resources, and similar business purposes. When these services are compromised, cybercriminals are able to access sensitive information, cause financial and reputational damage, and infiltrate deeper into vital infrastructure.

[3] "Phishing Activity Trends Report, 1st Quarter 2019." Anti-Phishing Working Group. May 15, 2019.

2. Common attack: Phishing and Smishing

What can you do? Software can monitor systems and devices and help to prevent phishing and smishing. But, as with ransomware attacks, the most effective control is changing end-user behavior. Security awareness training helps employees understand the threat landscape and develop a healthy suspicion of attachments and links.

3. Common attack: | Credential Stuffing

What is it? In 2019, 20 million people woke up to discover their personal and financial information had been stolen from the American Medical Collection Agency (AMCA), an online payment service used by Quest Diagnostics and Labcorp, two of the healthcare industry's largest medical testing companies.[4]

The attack was the result of credential stuffing. Unlike a brute force attack that attempts to "guess" its way past security, credential stuffing uses stolen usernames and passwords to speed up the attack process. People tend to use the same userID/password combination for many if not all of their internet-based and other services, which gives the attackers a front row seat to all the user's accounts.

In the case of AMCA, the hackers used their computers to try to automatically log into targeted website services. When a match was found, the hackers were able to take over and begin infiltrating the compromised account.

[4] Kayla Matthews. "Incident of the Week: Millions Hit by Quest, LabCorp Data Breach." Cybersecurity Hub. June 7, 2019.

3. Common attack: | Credential Stuffing

Why is it a problem? Cybercriminals want to be as efficient as possible. Credential stuffing dramatically increases their effectiveness by allowing them to automate attacks while using fewer resources. Too often, end-users facilitate this process.

After a Sony Pictures attack in 2011, the company ordered a forensic analysis. The study revealed that two-thirds of its users were sharing their Sony credentials on another site, which had been breached earlier the same year.[5] This sort of security malpractice is probably behind the AMCA attack as well. In that case, credential stuffing provided access to a poorly protected webpage. From this foothold, the hacker was able to access the company's systems and, over the next 8 months, skim off millions of customer records.

[5] "Credential Stuffing." Open Web Application Security Project. November 9, 2018.

3. Common attack: | Credential Stuffing

What can you do? Analysis by Microsoft suggests organizations can stop 99.9 % of attacks by requiring multi-factor authentication (MFA), which enforces multiple steps in the log-in process. Many financial institutions have implemented two-factor authentication (for example, a temporary code delivered by phone or email) to better protect their customers.

Is it possible for cybercriminals to outsmart multi-factor authentication? Of course. They can intercept text messages or clone mobile phone numbers and gain access to the additional authentication credentials. But these steps take more time and resources than going after a less protected site or account.

Organizations can also reduce their vulnerability by implementing additional defenses to detect suspicious log-in activity. These techniques include looking for new browsers, devices, and IP addresses and alarming on unusual country codes or script-driven activity.

In addition to technology upgrades and policy changes, organizations need to educate end-users on the value of password managers. Password managers make it easier to give every web account and service its own uniquely complex set of log-in credentials.

e+ Where Technology Means More®

4. Emerging threat: Service Account Attacks

What is it? Service accounts are privileged accounts that provide access to system resources, including information that can be monetized if stolen. They are often used to provide "hooks" to look up other computers, applications, and data. Some organizations use these hooks to initiate a service call using resources hosted by a third-party company, for example.

Because these accounts are business-critical, they are usually protected by long passwords. Unfortunately, it is also true that resetting these passwords can "break" applications. To avoid outages, these passwords are rarely changed.

e+

Where Technology Means More®

4. Emerging threat: Service Account Attacks

Why is it a problem? Cybercriminals are focusing on service accounts because they hold elevated privileges. Privileges allow access to more valuable parts of the infrastructure and the ability to change how systems work without raising alarms.

If cybercriminals are able to use malware to gain access as authenticated users, they can then learn enough about your system to begin cracking into your service accounts within minutes. With those account privileges, they can compromise services or break systems while avoiding detection.

It is even possible they can use your own tools to begin living off the land (LOTL). These LOTL attacks actually accounted for 40 % of the total number of cyberattacks in 2018.[6] Hackers are employing this strategy because it allows them to lurk in an environment indefinitely and slowly find, exfiltrate, and destroy data or operations.

[6] Mark Goudie. "Going Beyond Malware: The Rise of 'Living Off the Land' Attacks." Crowdstrike. May 7, 2019.

4. Emerging threat: Service Account Attacks

What can you do? Using long and complex passwords on service accounts is a good security practice. But resources will be more secure if those passwords are routinely rotated. And a compromise assessment can provide a baseline for improving security by looking for old attacks, suspicious files, silent failures, and active threats.

Monitoring for unusual account usage or spikes in service ticket requests is critical, as is learning what to do if prevention fails. Managed threat hunting, endpoint detection and response, and inventorying applications and assets can further harden your systems and shift the focus to less well-defended organizations.

Where Technology
Means More®

eplus-security@eplus.com

www.eplus.com/security

ePlus Technology | 13595 Dulles Technology Drive | Herndon, VA 20171