An Introduction to the Top Cyber Security Threats Today

ARTICLE 10.27.21 DEAN DORTON

Organizations today are at a cyber security crossroads. As the world rapidly changes, we've all had time to adjust to "new normals" in how we work and conduct business. Including cyber criminals.

Increased connectivity to more users — coupled with the accelerated growth of the Internet of Things (IoT) — has made it possible for businesses to operate efficiently from virtually anywhere. But it also created unsecured gaps in remote networks that **lowered the entry bar** for malicious actors to step over. Which they did, and continue to do, at a rapid pace.

In fact, the FBI has seen a fourfold increase in cyber security complaints since the beginning of the pandemic with global losses from cyber crime exceeding $1 trillion in 2020 alone.

Now, as organizations consider returning to in-person while managing the risks versus rewards of working from home, new cyber threats are emerging. In order to boost your cyber security posture, it's important to understand what those threats are, and where they could be coming from.

Common Sources of Cyber Security Threats

A cyber attack is most often a malicious attempt to gain unauthorized access to data, disrupt operations, or damage sensitive information. While data remains a primary target and deliberate attacks are typically done for some form of financial gain, theft is not always the goal: attacking data integrity to breed distrust is on the rise.

In short, the reasons for attacks can be as varied as the perpetrators themselves. Some of the most common sources of cyber threats stem from:

- **Cyber criminals & crime organizations:** These can be individuals or groups out to generate a profit. Cyber criminals can select specific computers and other devices as their targets to spread malware, use computers as a weapon to spread spam and create fraud, or use the computer as an accessory to steal sensitive data.
- **Hacktivists:** Rather than seeking financial gain, these individuals or groups carry out malicious activities to promote a political agenda, religious belief, or social ideology.
- **Nation-states & terrorist attackers:** Responsible for some of the most serious attacks to interrupt critical infrastructure or military operations, create social disruption, and generate misinformation.
- **Industrial espionage:** Designed to create a competitive advantage that can result in intellectual property theft, IT damage, and significant financial losses — as well as damage a company's reputation with shareholders and

customers.
- **Insider threats:** Usually occur from within by employees or former employees, but may also arise from third-party contractors or customers. Insider threats can be segmented as malicious, accidental, and negligent.

Emerging Cyber Security Threats

Cyber threats are never static. In fact, millions are being created every year, growing in frequency, diversity, and sophistication. As the technology that businesses rely on day in and day out evolves, so too does the challenge that every IT security team faces. Cyber criminals are becoming more agile and deceptive — even cooperating with other bad actors in ways never seen before — to tailor their attacks using new methods, devices, and entry points.

IoT Devices

It's estimated that the global IoT market could surpass $2.5 trillion annually by 2027, with upwards of 41 billion devices online by then.

No doubt IoT offers many benefits to businesses. From decreased operating costs, to new consumer insights, to more opportunities to optimize business operations, the value is evident. But with the proliferation of remote work that relies on an individual's devices, cyber criminals are finding a much broader attack surface.

Anything from cell phones, tablets, and laptops, to smart watches, smart TVs and voice assistants are fair game. By infiltrating these everyday devices, criminals can gain access to critical data, including Wi-Fi passwords, work emails, and login information.

Cloud & Remote Service Attacks

Cloud computing has made remote work easier for businesses and employees alike. With each day that passes, the reliance on application suites like Zoom, Meets, Microsoft 365, and Google Drive grows. And while cyber security has been a top priority for organizations since the start of the pandemic, surprisingly IoT devices working in cloud applications haven't always been included in the plan.

But with every cloud service in a remote environment, along with every device connected, the number of endpoints increases. So do the chances for misconfiguration and vulnerability that compromise not just the targeted company, but the slew of other organizations down the stream. Because these resources are in the cloud, most (if not all) endpoints are Internet-facing, opening the door to access by attackers on a global scale.

Fileless Attacks

This type of malicious activity uses native tools built into a system to conduct a cyber attack known as **"living off the land,"** or LotL.

Unlike traditional malware, fileless malware doesn't require an attacker to install any code on a targeted system. It's a stealthy attack difficult to detect because the compromised files are recognized as legitimate, designed using approved platforms or software tools that already exist within a company's network.

While fileless attacks have technically been around for decades, they're rapidly trending upwards thanks to their considerable success rate. Attackers in 2021 are likely to continue using fileless malware to compromise service providers rather than individual businesses, exploiting their existing infrastructure to attack the clients who rely on them.

Artificial Intelligence

According to MIT Technology Review, artificial intelligence in the hands of cyber criminals poses an "existential threat" to organizations.

While IT security teams are using AI to detect suspicious behavior, criminals are using it to make bots that pass for human users. And to dynamically change the characteristics and behaviors of malware.

Part of the reason for this advance in nefarious activity is the growing accessibility to AI. In the past, developing machine learning models was only possible if you had access to significant resources. However, these days AI models can be developed on personal laptops.

Supply Chain Attacks

This new type of threat occurs when a criminal deliberately targets multiple organizations through a third-party service they rely on. Most often, the entry point for attack comes via smaller businesses and vendors — and these attacks are increasing at an alarming rate.

In fact, the European Union Cybersecurity Agency (ENISA) reports that supply chain attacks may increase by 4x in the remainder of 2021.

This method of attack is becoming more popular and prevalent because it allows cyber criminals to target many victims through a single breach. They're especially severe because the applications being compromised are signed and certified by trusted vendors, allowing bad actors to slip in through the backdoor of a network — often with elevated privileges.

Traditional Cyber Security Threats

Even as attackers develop new types of threats, tried-and-true methods remain a significant go-to for cyber criminals. The weaknesses exposed by the shift to remote and work-from-home alternatives have allowed for the refinement of tactics, and improvement of threats that have worked for years.

Social Engineering

Aimed at the weakest link in the cyber security chain — people — social engineering exploits human error and vulnerabilities to expose data, spread malware infections, or provide access to restricted platforms. A few of the multiple forms social engineering can take include:

- **Phishing:** Particularly effective because the message appears to come from a credible source via emails or social media. Attackers are most commonly seeking to install malware or access sensitive information like credit card details and login credentials.
- **Spear phishing:** A more sophisticated and extremely targeted form of phishing where the attacker learns about the victim and impersonates someone he or she knows and trusts.
- **Smishing:** Or SMS phishing, here the attacker uses text messages as the means of deceiving the victim.
- **Password attacks:** These rely heavily on human interaction and often involve tricking people into breaking standard security practices, or accessing a password database.

Malware

One of the most common types of attacks, "malicious software" gets installed into a system when a user clicks a dangerous link or email. Once inside, it can block access, damage systems or devices, and gather critical data. Types of malware include:

- **Ransomware:** Where an attacker locks or encrypts the victim's data until paid.
- **Virus:** A piece of code that injects itself into an application designed to replicate itself and spread from host to host.
- **Trojans:** These enter a system looking like one thing such as a standard piece of software, but then lets out the malicious code once inside the host system.
- **Spyware:** Monitors internet activity, tracks login credentials, and spies on sensitive information once installed.

- **Adware:** Generates revenue for its developers by automatically placing ads on your screen, usually within a web browser.
- **Botnets:** A network of devices that has been infected with malicious software, often used to overwhelm systems in a distributed-denial-of-service attack (DDoS) attack.

Man-in-the-Middle (MitM)

Also known as eavesdropping attacks, MitM attacks occur when cyber criminals insert themselves into a two-party transaction over devices. Once in control, the attacker can redirect users to a fake site that looks like the intended site where they can steal or modify information. Two common points of entry for MitM attacks include unsecure public Wi-Fi and malware.

Denial of Service

A DoS is a sophisticated attack that floods servers or networks with massive amounts of traffic to deny fulfilling legitimate requests. When attacks compromise multiple devices on the target it's known as **Distributed Denial of Service (DDoS)**.

Domain Name System Attack

An exploit in which an attacker takes advantage of vulnerabilities in the domain name system — a protocol that translates a user-friendly domain name into a computer-friendly IP address. There are numerous and complex types of DNS attacks in use today designed to leverage communication between clients and servers to perform commands the user didn't request.

SQL Injection

Cyber criminals inject malicious code into vulnerable servers and applications using Structured Query Language to gain access to sensitive data and perform commands or similar actions that the user didn't request.

Advanced Persistent Threats

ATPs use continuous, sophisticated techniques to gain access to a system, allowing the attacker to remain there for a prolonged period of time. While a more common threat to larger organizations, cyber criminals are targeting smaller businesses that are part of a **supply chain** as a stepping stone to reach their ultimate goal.

Zero Day Exploits

Attackers use zero-day exploits after a network vulnerability is announced, but before a patch or solution is implemented. Attackers target the disclosed vulnerability during this window of time, giving developers "zero days" to fix the problem.

Navigating the Cyber Security Threat Landscape

As we cover in our recent Cyber Security FAQ, a comprehensive, independent analysis of your current cyber security posture can identify vulnerabilities, mitigate the risk of attacks, and continue to foster confidence and trust with your key stakeholders and customers alike.

While there's no way to prevent every cyber attack — old or new — cyber security assessments are the most proactive way to minimize cyber threats, and the consequences of a breach. Once issues are identified, strategic measures can be put in place to **increase real-time visibility** across your network and devices, and **improve your team's ability to react** in the event a breach occurs.

And as the business world continues to grapple with persistent cyber threats, businesses themselves are being held to account. Failure to comply with evolving regulatory requirements such as GDPR, HIPAA, PCI DSS, and SOX, can result in significant fines. As well as a damaged reputation.

Understanding and Mitigation Are Key

In the beginning, the abrupt shift to remote work understandably caught companies of all sizes off guard. Lack of policy, procedure, resources — even imagination — exposed cyber security vulnerabilities.

Today, persistent threats have our full attention. As more are invented and old ones improved, vigilance and consistent action can help keep you and your company ready to react.

Take the first step to mitigating risks, safeguarding your valuable data, and protecting your reputation. Connect with Dean Dorton for a cyber security assessment today.

And for more insights and analysis on trends and cyber security solutions, be sure to subscribe to our blog.