WHITE PAPER

The SolarWinds Cyberthreat Guide

Seven types of internet threats and how to help prevent them

solarwinds

INTRODUCTION

Staying safe from cybercriminals is no easy task. Despite advances in cybersecurity technology, cybercriminals successfully pull off headline-worthy attacks all too often. In fact, it might even seem like cybercriminals are gaining the upper hand over many organizations. But why?

First off, the number and types of cyberthreats have changed. For example, ransomware has become a major threat in many ways over the past few years. These attacks can be devastating and can even affect crucial services, like the damage to the United Kingdom's National Health Service due to the WannaCry attack[1].

Second, the people perpetrating these attacks have grown more coordinated and organized. While organizations must still worry about individual hackers or malicious insiders, they must now also contend with organized crime and even nation state actors. According to the 2018 Verizon Data Breach Investigation report, 50% of data breaches were carried out by organized criminal groups[2].

In short, the cybersecurity game has grown more complex—and the stakes have never been **higher**.

DEFENSE-IN-DEPTH

If you've spent time reading about cybersecurity, then you are likely familiar with the concept of the "defense-in-depth" strategy, sometimes also called layered security. It refers to the idea that cybersecurity requires multiple lines or layers of defenses to protect against threats.

It's important to realize that defense-in-depth is *a strategy*, not a goal. As with any strategy, you need to keep your tactics up-to-date. The fundamental defense methods still heavily apply—patch early and often, use strong antivirus, and watch for email-based threats. However, it's important to update your strategy from time to time with strategies designed to address the modern threat landscape.

This guide discusses some major threats organizations face today and was written to help you prepare. While examining each threat, we'll discuss countermeasures designed to help protect you.

If you're in charge of the security, confidentiality, integrity, and availability of IT systems for an organization, make sure you're current on the latest threats—it could potentially mean the difference between safety and a breach.

*If you've spent time reading about cybersecurity, then you are likely familiar with the concept of the **"defense-in-depth"** strategy, sometimes also called layered security.*

This guide discusses some major threats organizations face today and was written to help you prepare.

1 RANSOMWARE

WHAT IS IT?

Ransomware is a type of malware that blocks access to or threatens to disclose a victim's data, unless a ransom is paid. The truth is any organization is at risk of getting hit with a ransomware virus. In fact, ransomware can be so lucrative that several cybercriminals have implemented SaaS platforms to make ransomware attacks easier to execute against organizations—both large and small.

Ransomware will hit a business once ***every 14 seconds*** *by the end of 2019[3].*

The biggest danger ransomware poses is the disruption, distraction, and downtime it can cause businesses. Seventy-five percent of organizations infected by ransomware went at least two days without access to their data and systems; nearly a third went more than five days without access[4].

VARIATIONS:
Some of the most common and far-reaching variants include CryptoLocker, CryptoWall, Locky, WannaCry, NotPetya, and Teslacrypt.

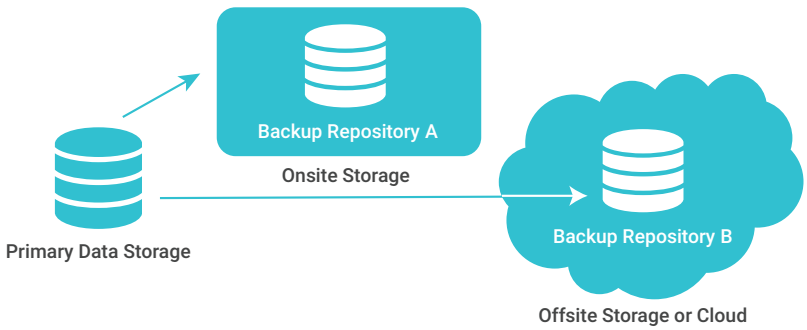
WHAT STEPS CAN I TAKE?

- Establish periodic system backup procedures
- Store backups securely
- Test system recovery procedures to ensure they work

As long as your data is securely backed up and easily recoverable, you will reduce the likelihood of vulnerability to this type of digital extortion and blackmail.

It's also worth noting that, when you back up your systems, you should likely follow the 3-2-1 backup rule. This states that you should have three backup copies across at least two different media with at least one backup kept offsite. This can further reduce your risk if local backups are corrupted or if the ransomware code attempts to delete local backups, as some ransomware strains have attempted in the past. And don't forget to periodically test your backups before you need them. The last thing you want is to end up with a useless backup file in the middle of a data breach.

It's also worth noting that, when you back up your systems, you should likely follow the ***3-2-1*** *backup rule.*



Additionally, make sure to monitor all your critical systems, databases, and applications so, you'll be able to detect suspicious access attempts and activities—before they get out of hand. Prioritize patching procedures, especially for your security software, and perform regular vulnerability scanning against your public-facing assets.

WHAT TECHNOLOGY WILL HELP ME DETECT, PROTECT, AND RESPOND?

SolarWinds® Threat Monitor™, Backup, and Log & Event Manager were each built to help assist you in mitigating ransomware attacks.

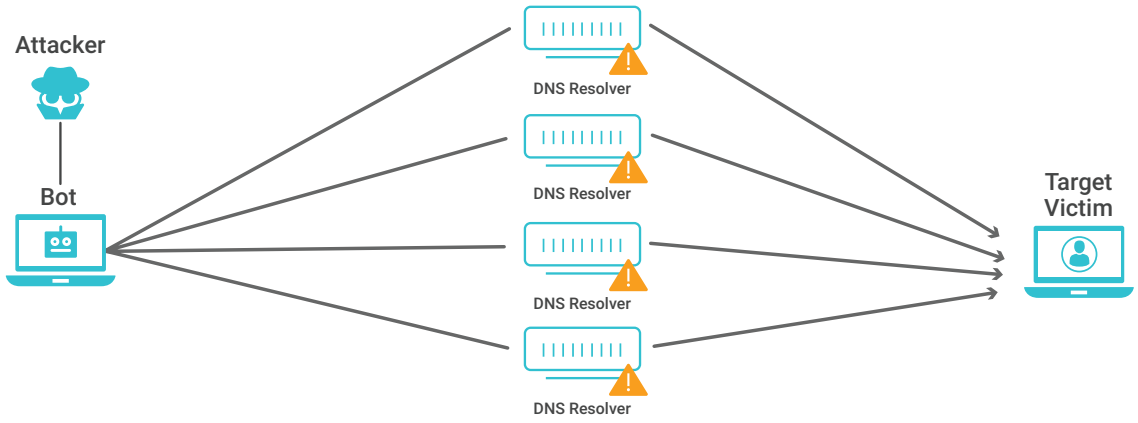
- **Make informed decisions by incorporating the latest threat intelligence at your disposal:** Receive updated threat intelligence from multiple sources, including IP and domain reputation databases, to monitor for security threats
- **Detect suspicious activity:** Help eliminate threats faster with nearly instantaneous detection of suspicious activity and automated responses
- **Cloud-first backup:** Leverage deduplication, compression, and fast, optimized movement to and from our global private cloud, built to help you back up data faster and more often—and recover more quickly in the event of an attack
- **Active response:** Mitigate threats with automated actions that block IPs, stop services, disable users, and more

2 DISTRIBUTED DENIAL OF SERVICE (DDOS)

WHAT IS IT?

DDoS (Distributed Denial of Service) attacks work by overwhelming and disrupting an online service with traffic from multiple sources. DDoS attacks are nothing new. What is new is the way attackers are using the latest technology to amplify these types of attacks. By bouncing their DDoS attacks off a Memcached server (software used to accelerate web page load times), attackers can amplify the effect of an attack by up to 51,000 times[5].

DDoS (Distributed Denial of Service) attacks work by overwhelming and disrupting an online service with traffic from multiple sources.



2018 saw the largest DDoS attack on record, perpetrated against GitHub®. In fact, reports show that the GitHub attack was twice as powerful as the DDoS attack that held the previous record from 2016[6]. While DDoS may not be the latest trick in the books, criminals still continue to use it—and innovate to make it more powerful.

VARIATIONS:
DDoS has been around for a long time. The latest innovations involve botnets and botnet armies that infiltrate systems around the world. A botnet of a few hosts is relatively harmless, but a botnet of thousands of machines can potentially be strong enough to bring down a victim's operational environment. To produce faster resource exhaustion in the victim's system, the attacker can slow the rate of response or hold open the TCP/IP connection by sending confusing, or non-RFC compliant, packets. This essentially tricks the server into thinking it will receive more data shortly. This is the equivalent of mimicking a bad cell phone connection.

WHAT STEPS CAN I TAKE?

A key to mitigating DDoS attacks is **monitoring externally facing router** and **server performance**.

SNMP metrics are intended to help you determine the load, connections, and error rates for any network interface—especially critical pieces of the infrastructure, such as firewalls. Tracking NetFlow from your network devices can also potentially help you understand how much of your bandwidth is being used by legitimate "conversations," such as data moving between an internal system and an external provider, and which is entirely inbound (a sign of potential DDoS activity). This can potentially help you locate threats or increases in conversation, protocols, or application traffic. Finally, inspecting inbound traffic by putting a tap on, or mirroring, an externally facing interface allows you to analyze the inbound network traffic, and can likely give you a good indication of whether you're under attack.

Specifically, you'll need to rely on continuously updated threat intelligence that was designed to help you recognize attacks in process to help you stop them before they disrupt operations. Threat intelligence in the form of event correlation rules, updated signatures, known CnC server IP addresses, and more can be collected in an attempt to help you detect and respond before a DDoS attack gains momentum.

In terms of stopping DDoS attacks, your service providers (cloud providers, ISPs, DNS providers, etc.) will likely be the "first responders" on the front lines of these threats. By actively monitoring for this sort of attack and actively filtering, service providers can hopefully respond and mitigate, relying on each other to take steps toward

2018
saw the largest DDoS attack on record, perpetrated against GitHub®.

In terms of stopping DDoS attacks, your service providers (cloud providers, ISPs, DNS providers, etc.) will likely be the "first responders" on the front lines of these threats.

orchestrating effective plans against these distributed and complex attack patterns. This is where deploying a layered approach, as described earlier, is essential. For example, leveraging gateway firewalls with DDoS mitigation services alongside a cloud-based DDoS mitigation solution can be helpful for businesses with mission-critical and online-based operations.

Consider testing your DDoS resilience **by simulating an attack** to see how systems respond.

A clean and "best practice" security approach to servers, especially DNS servers (no open resolvers), is designed to help ensure your organization isn't used in a proxy- or amplification-style attack. You can provide additional value by making sure firewalls, routers, edge switches, and servers are all patched and up-to-date. Unfortunately, DDoS attackers can take advantage of a single vulnerability left unpatched to turn your assets into unwilling participants in a DDoS campaign against someone else.

You can provide additional value by making sure firewalls, routers, edge switches, and servers are ***all patched and up-to-date.***

WHAT TECHNOLOGY WILL HELP ME DETECT, PROTECT, AND RESPOND?

SIEM tools, such as SolarWinds Threat Monitor and Log & Event Manager, were built to continuously monitor network access and activity by correlating disparate log events from systems across the infrastructure to discover emerging threats and indicators of compromise. Since both Threat Monitor and Log & Event Manager are updated with current threat intelligence, the systems were built to help you detect DDoS attacks in near real-time.

Additionally, with Threat Monitor Active Response, you can set the system to automatically respond to and take steps toward remediating active threats (for example, by automatically shutting down a network connection from a known CnC server).

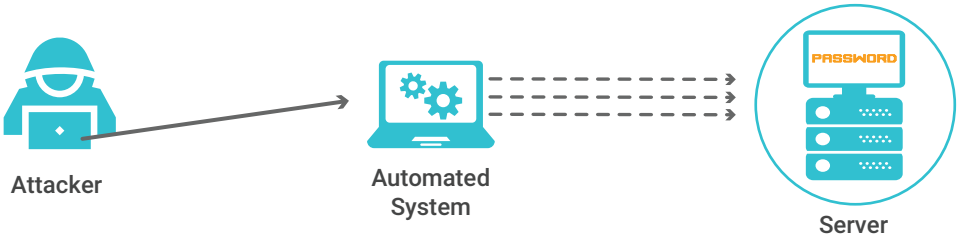
3 BRUTE FORCE ATTACKS

WHAT ARE THEY?

Successful attacks grant access to the infrastructure—whether network or server devices, in many cases with administrator-level privileges. At this stage, it's unfortunately game over for the defenders. Brute force attacks—either from malware looking for its next host to infect or a malicious actor running a script—generally target a single service exposed to the internet, such as Remote Desktop, VNC, FTP, and SMTP services.

Brute force attacks involve systematically looking for a correct network password.

Depending on the robustness of your security logging, these attacks may not be easy to detect. A high-volume brute force attack can exhibit similar patterns as a DDoS attack, only typically from just one or two IP addresses. Brute force attacks and their cousins, SQL injections, are threats to all services exposed to the internet. For example, if an attacker can guess a password for a content management system, they can possibly gain unrestricted access to that account. If this site is hosted inside the company's network, then complete network exploitation is possible.



VARIATIONS:

SQL injection attack: This occurs when someone attempts to "inject" SQL code directly into an application's database without permission. This is a more sophisticated version of the brute force attack, as many different combinations of SQL injection need to be tried to gain access to the user ID and password table, which can frequently be unencrypted or poorly encrypted.

Depending on the robustness of your security logging, these attacks may not be easy to detect.

WHAT STEPS CAN I TAKE?

One good method designed to mitigate brute-force password cracking attacks is to **limit the number of invalid logins** (e.g., auto-lockout).

In terms of protecting against SQL injection, remember there are two authentication modes used in SQL Server®: Windows® Authentication mode and mixed-mode, which enables both Windows Authentication and SQL Server authentication. The Windows Authentication mode is less vulnerable to brute force attacks, as the attacker is likely to run into a login lockout (the account-lockout-policy feature) after a finite number of attack attempts. In a production environment, consider making sure Windows Authentication mode is implemented and that you use the lockout policy feature, as this is intended to make brute force attacks time- consuming and costly for the attacker.

Additionally, it's important to remember you **shouldn't use a domain administrator** account as an SQL database connection account.

Also, review and consider strengthening your password policies, especially for your databases, domain servers, and other critical systems and applications. Multifactor authentication is designed to reduce the risk of these attacks.

Additionally, make sure you **actively monitor** suspicious login activity, particularly for sensitive databases and production servers.

WHAT TECHNOLOGY WILL HELP ME DETECT, PROTECT, AND RESPOND?

Multifactor authentication relies on more than just what you know (username and password) to combine it with another factor, such as what you have (e.g., your phone) or what you are (e.g., face ID). This approach is designed to make your credentials more dynamic and less vulnerable to theft.

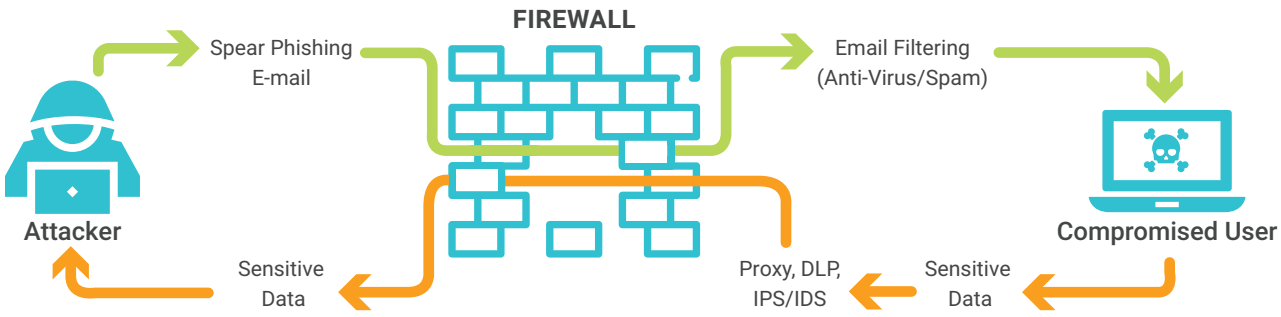
Threat Monitor and Log & Event Manager were built to augment strong authentication with nearly continuous and active monitoring and correlation of login activity—designed to help you quickly respond when suspicious login activity signals an active threat.

4 PHISHING AND SPEAR PHISHING ATTACKS

WHAT IS IT?

Phishing and spear phishing are forms of fraud where an attacker disguises themselves as a trusted entity to entice their victim to take an action (e.g., download a malicious attachment, go to a website, submit their credentials, etc.). This action is often the first step in a broader attack, where the attackers leverage stolen credentials from a "phish" to steal data, like medical records or intellectual property. The main difference between phishing and spear phishing is the scope of the intended audience. Phishing attacks are generally broad-based and widely distributed, whereas spear phishing is usually targeted at specific individuals or a group of individuals inside an organization.

The main difference between phishing and spear phishing is the scope of the intended audience.



VARIATIONS:

Cybercriminals often take their time in pulling up some of their biggest spear phishing traps to ensure they have a big payout. In fact, they will often create and store detailed profiles on their victims in databases on the dark web, collecting bread crumbs from social media platforms in their pursuit. While each of these campaigns may differ slightly in their initial approaches and tactics, these attackers typically aim for credential theft.

WHAT STEPS CAN I TAKE?

As with other forms of social engineering, educating users on how to engage online is a **critical first step**.

When designing your security awareness training programs, consider teaching your employees (especially executives) to practice good judgment and healthy skepticism when they engage on social media at work—on the road and at home. Additionally, encourage users to think critically before opening email attachments or clicking links.

It may be worth testing your security awareness program on a regular basis by sending mock phishing emails to employees. You can then adjust your security awareness training components based on these assessments. There are tools you can use to test your preparedness for social engineering attacks like these.

WHAT TECHNOLOGY WILL HELP ME DETECT, PROTECT, AND RESPOND?

Technical professionals can take steps to combat this sort of attack by using multiple layers of defense that include prevention, detection, and response capabilities SolarWinds provides several solutions designed to help combat phishing and spear phishing attacks.

In terms of prevention, SolarWinds Serv-U® FTP Server was built to offer organizations an alternative to email when sharing large documents with trusted partners, suppliers, and customers. Moving to a secure FTP standard can potentially help organizations avoid being tricked into opening large attachments in email or clicking on links to malicious websites.

By detecting and alerting you to suspicious activity related to credential use and abuse, SolarWinds Log & Event Manager was built to help your team to respond quickly to these social engineering attacks, contain outbreaks, and limit the impact on operations.

SolarWinds provides several solutions designed to help combat ***phishing and spear phishing attacks.***

Finally, SolarWinds Threat Monitor was designed to stay current with the latest threat intelligence on phishing tools, tactics, and procedures to help you keep pace with emerging risks.

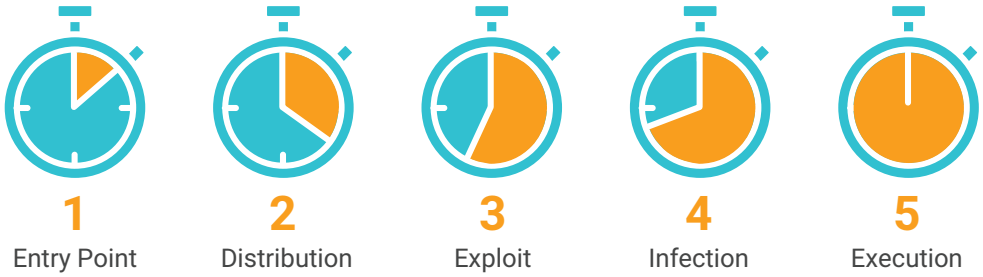
5 DRIVE-BY DOWNLOAD

WHAT IS IT?

A drive-by download refers to a **website that automatically downloads malicious code** onto a visitor's machine.

This can lead to devastating consequences depending on what is actually downloaded to the victim's machine.

FROM WEBSITE TO INFECTION IN 0.5 SECONDS



In October 2017, the city of Issaquah, Washington, was hit by a ransomware attack that took city services offline for four days[7]. While the end result was a ransomware attack, the entry point was a drive-by download when an employee opened a PDF file on a website. In other words, a drive-by download took down a city for four days!

Cybercriminals commonly use exploit kits to distribute malware to users surfing the web. Such kits can include exploits for multiple vulnerabilities within a single malicious webpage. Subroutines in the code check out a website visitor's target systems, web browsers, and browser plugins, such as Flash® Player, Adobe® Reader®, Java®, or Microsoft® Silverlight® for anything that isn't fully patched. An attack is then launched to exploit that specific out-of-date software.

Cybercriminals commonly use exploit kits to distribute malware to users surfing the web.

In October 2017, the city of Issaquah, Washington, was hit by a ransomware attack that took city services **offline for four days**[7].

WHAT STEPS CAN I TAKE?

As mentioned previously, you need to think about deploying a broad security strategy. In the case of web-based threats, web protection and filtering should likely form the basis of your thinking around security for this type of threat.

As mentioned previously, you need to think about deploying a broad security strategy.

Web protection and filtering can potentially be a broader defense than antivirus in this case as it is designed to prevent people from visiting known trouble hotspots. This can help reduce the chance of a malicious infection. This also means it can be used as a security awareness and education tool. At the other end of the scale, the reports that can be produced from a web protection and filtering tool can potentially be used to help explain poor internet performance, as well as provide a forensic solution to identify suspicious web traffic.

The importance of layered security

Just like with the phishing email described earlier, technology professionals can take additional steps to mitigate this sort of attack by **implementing multiple layers of defense**.

Robust defenses can potentially protect users from visiting the harmful web pages where these threats reside. Focusing on web-based attacks is a "quick win" for security, and would use many of the same technologies deployed against phishing attacks, as drive-by downloads could start with a simple email link.

When considering the threat the web poses, it's important to understand the delivery mechanism of an attack. This is commonly a criminal exploit kit lurking on a compromised website. Removing email with malicious attachments from the equation is the first step. However, web links can appear in many different ways—malicious advertising, social networking, or even instant messaging clients. This means you will likely need more defenses than email protection.

Besides aggressively keeping browsers and plugins up-to-date, one of the most commonly used tactics to protect end users from the dangers of internet surfing is to install multiple web browsers on workstations. In the rare situation of a zero-day threat targeting a particular web browser, users can be instructed to use a different browser until the vendor issues a patch.

As a technology professional, you're probably aware of the key role DNS plays in directing users' web surfing, email, and any other internet connection requiring name resolutions.

As a technology professional, you're probably aware of the key role DNS plays in directing users' web surfing, email, and any other internet connection requiring name resolutions. It's important to understand that DNS is not inherently secure; in fact, poorly secured ISP DNS servers can be a major security problem. Compromised DNS servers can redirect requests for a legitimate site to a fake site.

DNS is an important foundation of web-based communication, so settling on one provider—like the Google® public DNS or Webroot® Secure DNS services—will provide an additional layer of security. Also, you have the added bonus of being able to detect (through using a firewall rule (or logging onto your DNS server) when there is a DNS anomaly, like a workstation trying to reach a DNS server located in, say, Russia.

Not a good thing when you **don't have Russian clients or offices** for your company located in Russia.

WHAT TECHNOLOGY WILL HELP ME DETECT, PROTECT, AND RESPOND?

Technology professionals sometimes stretch their team thin to accomplish tasks. This could be feasible on a small scale, but it may not be sustainable with today's cyberthreats.

Technology professionals sometimes stretch their team thin to accomplish tasks.

Patching—for everything from the operating system to antivirus definitions—is designed to be your main line of defense in this case. You should consider investing in an intuitive patch management solution designed to quickly identify out-of-sync systems and address those software vulnerabilities in a way that gets the job done without impeding the end user's work.

Your stakeholders or clients will likely want you to demonstrate patch compliance by staying on top of vulnerabilities and producing summary reports to show patching status. Additionally, make sure to schedule and maintain your desktops, laptops, servers, and VM patch cycles—and make sure to keep up with the latest patches for 3rd-party applications.

Your stakeholders or clients will likely want you to demonstrate patch compliance by staying on top of vulnerabilities and producing summary reports to show patching status.

Remember, "compliance" does not mean, "everything is patched to the latest version of everything, always." Instead, you should be able to determine which systems are and aren't patched and *why they're out of date*. Not all systems can be brought up to the latest and greatest if, for example, a new driver or DLL interferes with a business-critical function. Robust patching solutions use rules to determine whether a patch can be safely applied or not. Then, when the conflict is no longer present, the patch can be applied without relying on IT staff to remember which systems they skipped the last time around.

Meanwhile, **SolarWinds Threat Monitor** was built to help allow you to continuously update your threat intelligence from multiple sources.

You can automate responses to threats and even view reports to give you greater visibility into your efforts. Having programs that continuously monitor for vulnerabilities potentially helps your company avoid becoming the low hanging fruit that drive-by downloaders count on.

6 ADVANCED PERSISTENT THREAT (APT) ATTACKS: CYBERCRIMINALS, NATION STATES, AND HACKTIVISTS

WHAT IS IT?

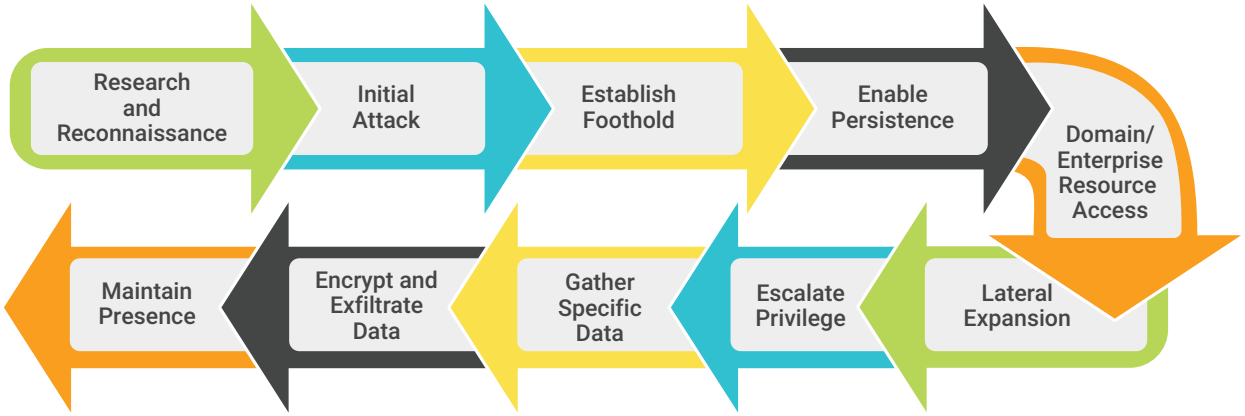
An **advanced persistent threat** refers to a sustained cyberattack against an organization, often for the purposes of espionage and gathering data.

They can be, but aren't always, state-sponsored.

APT actors are usually more sophisticated, with larger resources at their command than many other groups or cybercriminals. Often, these groups will stick with their attack against a target group until they achieve their goals. These attacks can be challenging to fight against, especially if the perpetrators are connected to a nation state.

APT actors are usually more sophisticated, with larger resources at their command than many other groups or cybercriminals.

Some of these threats can be downright frightening. To give one example, the United States Computer Emergency Readiness Team (US-CERT) issued a release claiming that people working on behalf of the Russian government had consistently been working to compromise US infrastructure since at least March 2016. The sophisticated attack took a two-phase approach: First, they would target third parties likely to have insecure networks, then they would use that to gain access to their intended victim. Over the course of the campaign, US-CERT identified the use of, "spear-phishing emails, watering hole domains, credential gathering, open-source



and network reconnaissance, host-based exploitation, and [the targeting of] industrial control system (ICS) infrastructure[8]." In other words, this attack was sophisticated, ongoing, and used a myriad amount of cybercriminal techniques to compromise systems.

VARIATIONS:

There are quite a few well-known APT groups documented by security researchers. One of the most well-known is Anonymous, which claims scores of hacktivists under its banner. Importantly, it's hard to differentiate between APT, hacktivist, fledgling nation-state sponsored actors, and sophisticated criminals. Thus, under the catch-all banner of APT, you will have varying degrees of sophistication, but they will generally have several things in common:

- They target you to steal all your internet data
- Their motivation tends to be ideological or cultural or they seek to perpetrate technological espionage either for the advancement of an ideological/ political/ cultural/agenda or the theft of intellectual property
- They persistently sustain the attack by probing for weakness, brute forcing, running spear-phishing campaigns, researching, and even conducting DDoS to ruin your day

As a technology professional, you must be realistic about the chances of defeating a persistent threat from a group that could be relatively large and contain some truly skilled hackers.

WHAT STEPS CAN I TAKE?

As a technology professional, you must be realistic about the chances of defeating a persistent threat from a group that could be relatively large and contain some truly skilled hackers.

The most important questions to ask are:

- **Do you have the skills and capabilities to take on this sort of challenge?**
- **And is it worth my time and money to build cyberdefenses to ward off these actors?**

The sort of company that draws the ire of these groups is usually a close-to-enterprise-level organization that may have significant cyber-risks due to political, cultural, religious, or ideological products or services.

Chances are a company like this will already know the appropriate configuration of systems that must never be on the internet.

Your job as a security-focused technology professional is to ensure those systems are—and continue to be—**protected from internet access**.

To reduce the chances of an attack, a non-exhaustive list of infrastructures that probably should not be connected to the internet includes:

- military/governmental classified computer networks/systems
- financial computer systems, like stock exchanges
- industrial control systems, such as SCADA in oil and gas fields
- life-critical systems, such as controls of nuclear power plants, computers used in aviation, and computerized medical equipment.

Sadly, many of these critical systems are being connected to the internet without even basic security solutions in place.

Sadly, many of these critical systems are being connected to the internet without even basic security solutions in place. You may need to help a business implement security solutions to ensure the benefits of connection to the internet do not introduce vulnerabilities with significant consequences if exploited.

WHAT TECHNOLOGY WILL HELP ME DETECT, PROTECT, AND RESPOND?

In most cases, you will likely need to employ experts with specific security skill sets, not to mention 24/7 monitoring and incident response.

Even the biggest security organizations can struggle against APTs, as most of the tools of the security trade usually need to be deployed to ward off these cybercriminals. In this sort of environment, you will need to deploy both basic and sophisticated technologies to even the playing field. The level of control over the software and hardware environment will have to be extreme, and multiple technologies will be required. In most cases, you will likely need to employ experts with specific security skill sets, not to mention 24/7 monitoring and incident response. Network segregation, intrusion detection systems, like those found in SolarWinds Threat Monitor, and application whitelisting, as well as the wide usage of encryption of data at rest and in transit, can all be used in an attempt to fend off these actors.

You should also **give serious consideration** to your architecture and internet connectivity.

Consider employing "air gap" networks and robust physical security in addition to the technical solutions mentioned previously.

A network that is not exposed to the internet could be considered, in theory, secure. However, some sophisticated attacks by nation-state actors can even compromise computers in an "air gap" configuration. It's virtually impossible for a large enterprise to take on and win against a nation-state sponsored APT attack. Putting all the security tools imaginable to work may prove to be prohibitively expensive. Ultimately, if this is the primary risk to a business or organization, you may want to consider investing heavily in physical security and ubiquitous encryption, in addition to a non-persistent and heavily encrypted connection to the internet.

In some cases, the technology professionals will be the clean-up crew, responsible for "metaphorically" burning the network to the ground and rebuilding it to remove the foothold the APT group gained on the business. One option in this scenario involves methodically designing and implementing a secure network using a robust framework, like the SANS 20 controls. At each step of the design process, security has to be considered, controls implemented, and monitoring established. This includes all layers of the OSI model 1-7, HVAC, and physical security. There are very few people in the world with the experience, skill set, and credentials to tackle all of the projects and sub-projects that come from a network build like this, which is why many large security-focused organizations—such as banks, airlines, government, and military organizations—have still been successfully hacked by APT actors.

These threats are extremely serious and challenging to tackle. We highly recommend you speak with a company that's well-versed in these kinds of attacks.

These threats are extremely serious and challenging to tackle. We highly recommend you speak with a company that's well-versed in these kinds of attacks.

7 DATA THEFT, DESTRUCTION, AND DISCLOSURE

WHAT IS IT?

The December 2014 attack on Sony Pictures Entertainment[9] set a new benchmark in the damage cybercriminals can inflict on an enterprise. In response to the damage this attack caused, including the release of highly compromising emails and data destruction, the FBI released a flash alert to warn other organizations of the danger. Elements of the Sony® attack included massive intellectual property damage (through movie releases), data destruction, unauthorized disclosure of confidential information, denial of service (through credential theft), and reputational damage (leading to the termination of senior executives).

VARIATIONS:

The Sony hack may be unique in the annals of cybercrime in terms of such a large collection of different security incidents happening rapidly over a short period of time. The motives seemed purely malicious.

At no point did the attackers try to extort money from Sony—they only had digital mayhem in their plans. Given the state of cybersecurity and what feels like a continuous and unrelenting victory streak for the bad guys, a tremendous number of businesses would likely suffer the same damage from a similar cyberattack. Even if the malware used in this attack was not detectable by antivirus programs, Sony had a "passwords.xls" document that was neither encrypted nor password-protected that listed all passwords, including ones with administrative access.

WHAT STEPS CAN I TAKE?

As a technology professional, you need to **focus your security solutions** on the risks the business is facing.

Implementing a whole bunch of technology is rarely the best solution by itself. Designing a simple, manageable network and establishing a continuous monitoring solution can potentially be easy wins. Often, data breaches occur when basic security measures simply weren't in place.

Selling fear only works to a certain extent and is generally not sustainable. Security is about a great deal more, and combines the use of technology along with people and process elements. Consider starting with a security assessment, a plan to remediate critical items identified by the business, and then offer a solution to monitor the system for compliance. Simple measures often can be surprisingly helpful in reducing data breach risk.

WHAT TECHNOLOGY WILL HELP ME DETECT, PROTECT, AND RESPOND?

Technology professionals should keep one thing in mind—all the hard work, diligence, and security technology will be ineffective if the management at the company does not support and endorse a security program. If this is the case, you're going to need to get really good at restoring data from backup.

The Sony attack is used in this paper to illustrate the worst possible scenario. The Sony attack demonstrates what can occur when the cybercriminals are simply bent on data destruction. A new type of threat, perhaps the nastiest evolution so far, is the malicious hacking of business, government, or organization systems to destroy data or to extort a ransom from the target. The consequences of a massive data breach have evolved from the looting of personal private information and intellectual property theft to attempts to destroy or get paid for threatening to destroy a target. In any case, restoring data to its original state will likely need to be an end goal. A strong cloud-based backup could potentially help in these situations.

The Sony attack is used in this paper to illustrate the worst possible scenario.

The **consequences of a massive data breach** have evolved from the looting of personal private information and intellectual property theft to attempts to destroy or get paid for threatening to destroy a target.

THE EVOLVING CYBERTHREAT LANDSCAPE

Cybercriminals have multiple tools in their toolbox to attack businesses. And the truth is they will likely never stop innovating new ways to compromise systems or destroy data.

One thing that doesn't change, however, is the importance of adopting a layered approach to security. The tools you use will depend on the types of threats you face. Most businesses will, at the minimum, need to keep up-to- date with basic cyberhygiene, like patching, antivirus, web protection, and email security. However, many businesses should consider investing in more sophisticated security tools, like SIEM solutions, which are designed to help against more complex cyberattacks.

Regardless, **technology professionals should study the threat landscape extensively** to discover the steps they can take to help keep their users safe from potential harm.

REFERENCES

[1] "NHS 'Could Have Prevented' WannaCry Ransomware Attack," BBC News. https://www.bbc.com/news/technology-41753022 (accessed September 2018).

[2] "2018 Data Breach Investigations Report," Verizon. https://www.verizonenterprise.com/verizon-insights-lab/dbir/ (accessed September 2018).

[3] "Global Ransomware Damage Costs Predicted to Exceed $8 Billion in 2018," Cybersecurity Ventures. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-exceed-8-billion-in-2018/ (accessed September 2018).

[4] "Ransomware: The New Threat to Business Uptime," Intermedia. https://www.intermedia.net/report/ransomware (accessed September 2018).

[5] "Memcached Servers Abused for Massive Amplification DDoS Attacks," The Hacker News. https://thehackernews.com/2018/02/memcached-amplification-ddos.html (accessed September 2018).

[6] "In Wake of 'Biggest-Ever' DDoS Attack, Experts Say Brace for More," Threatpost. https://threatpost.com/in-wake-of-biggest-ever-ddos-attack-experts-say-brace-for-more/130205/ (accessed September 2018).

[7] "How a Drive-by Download Attack Locked Down Entire City for 4 Days," The Hacker News. https://thehackernews.com/2017/10/drive-by-download-ransomware.html (accessed September 2018).

[8] "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," US-CERT. https://www.us-cert.gov/ncas/alerts/TA18-074A (accessed September 2018).

[9] "The Sony Pictures Hack, Explained," The Washington Post. https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained/?noredirect=on&utm_term=.0ba5848fca64 (accessed September 2018).

SolarWinds is a leading provider of powerful and affordable IT infrastructure management software. Our products give organizations worldwide, regardless of type, size or IT infrastructure complexity, the power to monitor and manage the performance of their IT environments, whether on-premise, in the cloud, or in hybrid models. We continuously engage with all types of technology professionals – IT operations professionals, DevOps professionals and managed service providers (MSPs) – to understand the challenges they face maintaining high-performing and highly available IT infrastructures. The insights we gain from engaging with them, in places like our THWACK online community, allow us to build products that solve well-understood IT management challenges in ways that technology professionals want them solved. This focus on the user and commitment to excellence in end-to-end hybrid IT performance management has established SolarWinds as a worldwide leader in network management software and MSP solutions. Learn more today at www.solarwinds.com.