The LOGICnow Cyber Threat Guide

Nine types of internet threats and how to stop them

LOGICnow

CHOOSE INTELLIGENCE


www.logicnow.com

Contents

4 Introduction

6 Network Probe / Hostile Scan

10 Distributed Denial of Service

14 Brute Force Attack

18 Phishing Attack

22 Drive-by Download

26 Spear Phishing Attack

30 Case Study: The Great Bank Robbery

32 Advanced Persistent Threat Attack – Cyber Criminal / Hacktivist

36 Advanced Persistent Threat Attack – Foreign Intelligence Service

40 Data Destruction

Introduction

Defending networks from attacks is no easy task for IT professionals. Attacks range in capability and threat; and over reacting or implementing the wrong technology can be costly and make it easier for the bad guys.

This ebook sets out the types of attacks a typical network faces and offers some of the successful mitigation strategies IT professionals have implemented against them.

Ultimately, treat this guide as a first step in designing your defense-in-depth strategy. IT professionals must truly understand the risk to the business and that IT security does not have ”magic” solutions. There is not a single technology that can prevent all the bad things from happening, despite what vendors say.

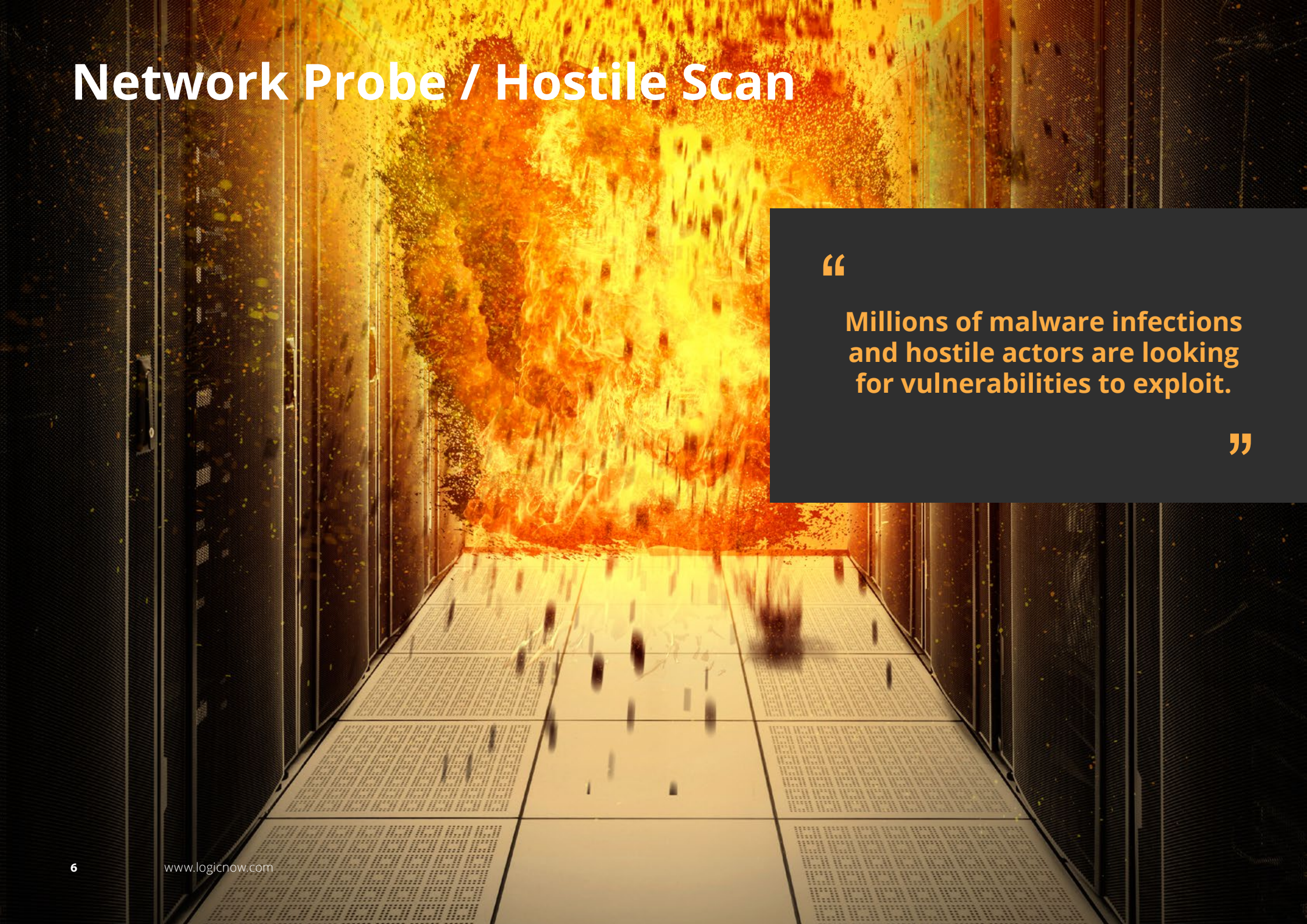
Cyber attacks, malware, and system vulnerabilities have all been mystified and media-hyped beyond any sort of reasonable analysis. In fact, the most effective IT strategies against all unknown and known threats are generally the same. Patch and update the operating system, patch and update third-party applications, restrict administrative access, and use malware defenses. All of these recommendations come from years of analysis by government and security organizations around the world.

Lastly, offense informs defense. This means IT service providers need to learn how to view their customers' networks as targets. I'm certainly not advocating unleashing your own destructive cyberattacks on unwitting customers, but setting up a virtual cyberdefense lab and downloading some free tools to explore vulnerabilities will help you get better at defending and detecting attacks on your own networks.

Remember, as an IT professional you are partially or completely responsible for the confidentiality, integrity, and availability of the IT systems in your care. Don't make it easy for the bad guys; make it frustrating and difficult by putting in detective, preventive, and forensic defensive layers.

Ian Trump, Security Lead at LOGICnow

Network Probe / Hostile Scan



> Millions of malware infections and hostile actors are looking for vulnerabilities to exploit.

What is it?

Millions of malware infections and hostile actors are looking for vulnerabilities to exploit. A great example of this sort of attack is the Moon Worm. This was a self-replicating program that infected Linksys routers by exploiting an authentication bypass vulnerability in various models from the vendor's E-Series product line. It moved from router to router by scanning for its next victim. If it didn't find a vulnerable router it moved on to the next IP address. By using commercial software, such as Metasploit, Nessus or the free tool NMAP, these programs can locate vulnerable services on the Internet.

Variations:

Worms and other self-propagating malware come in a wide variety. Some target specific vulnerabilities in software with specific exploit packages, such as the first generation of NIMDA and Code Red worms. Others simply use a brute force approach to passwords in an attempt to gain access to protected systems.

Network Probe / Hostile Scan

What do I need to do?

If you're serious about improving Internet security, move as many services as you can to hosted services and try to close as many Internet-facing ports as you can. With no open ports the chances of a Network Probe or Hostile Scan finding something to exploit is greatly reduced.

The external vulnerability scan and continuous monitoring of the security environment (via logging) are becoming compliance requirements, especially for PCI DSS. If the business is hosting Internet accessible services or a web application there is an opportunity to upgrade the firewall to a more sophisticated application-aware version, frequently called a "Next Gen" firewall.

Finally, password audits, secure de-fault configurations and architecture plans to move to external hosting providers all open the door to project opportunities and continuous monitoring solutions.

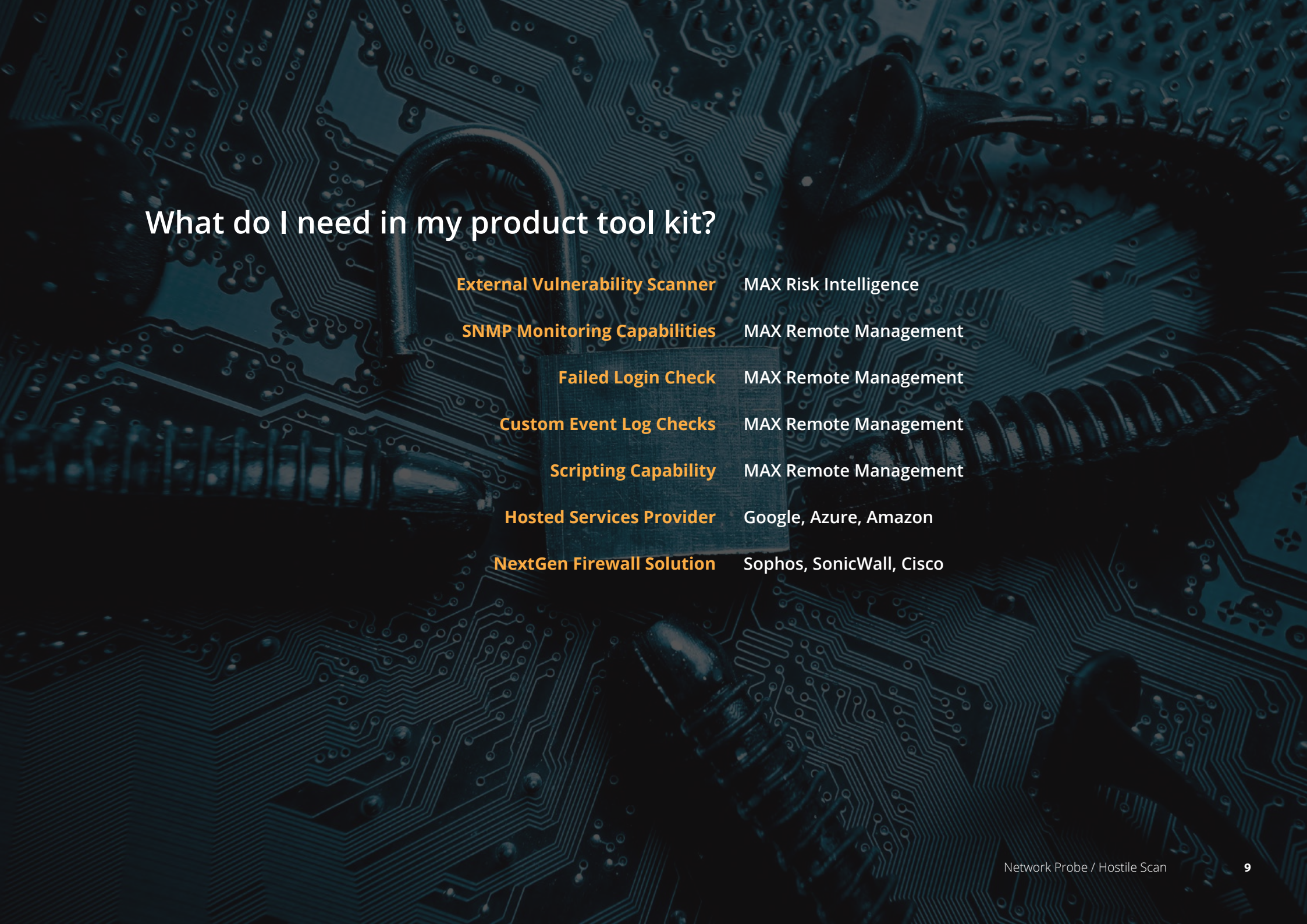
"Some attacks target vulnerabilities in software with specific exploit packages. Others simply use a brute force approach to passwords in an attempt to gain access to protected systems."

What technology will help defend my networks?

Inexpensive firewalls designed for the home market or devices with built-in firewall capabilities (as in those frequently provided by an ISP) are not sufficient for protecting a business. A more robust solution is recommended from an upmarket manufacturer; Watchguard, Cisco & Cisco Small Business, Sonicwall and Checkpoint are all popular options. Try to standardize on one or two firewalls and learn how to program effective rules.

Some attacks target specific vulnerabilities in software with specific exploit packages such as the first generation of NIMDA and Code Red worms.

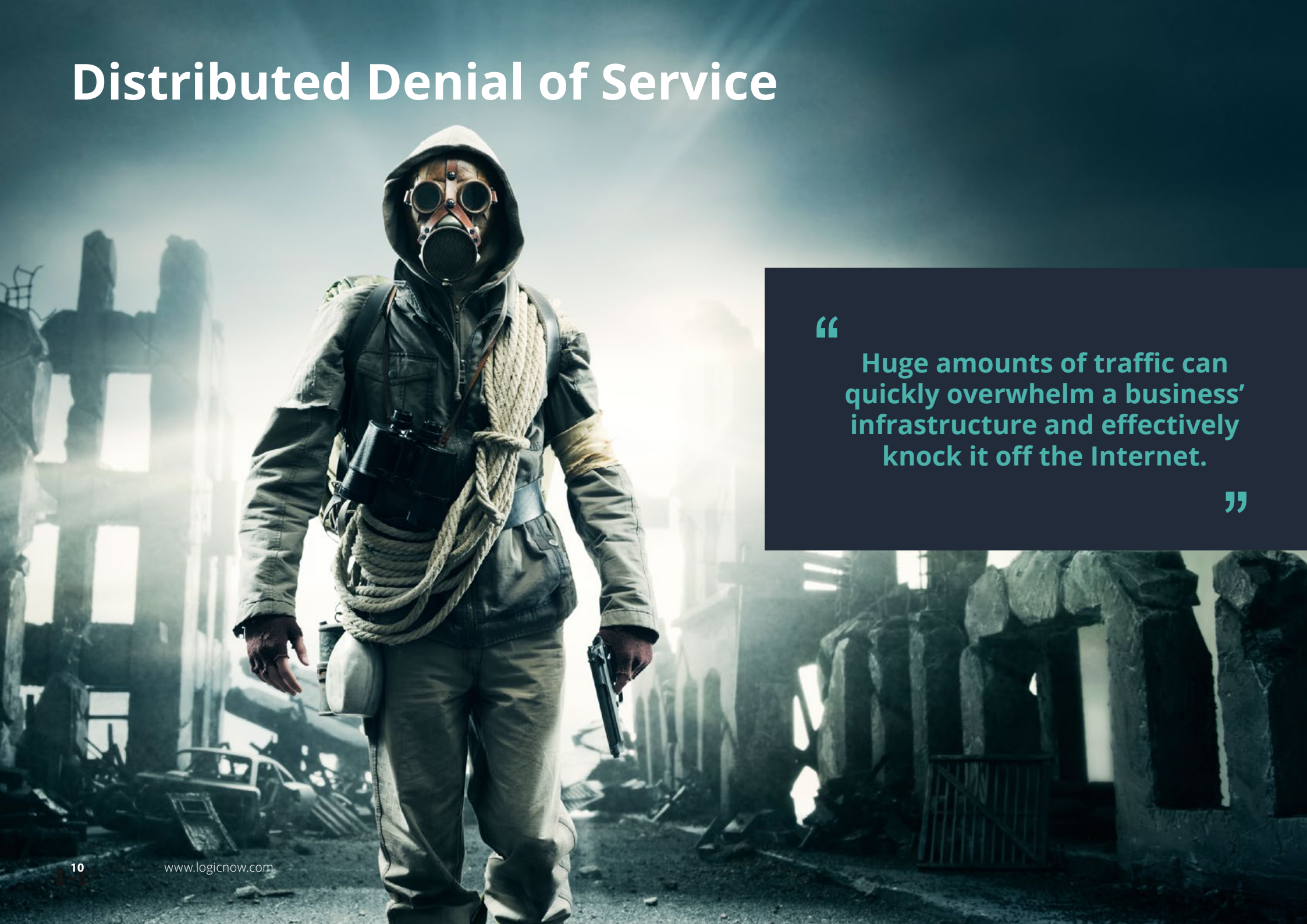
Others simply use a brute force approach to passwords in an attempt to gain access to protected systems.



What do I need in my product tool kit?

External Vulnerability Scanner	MAX Risk Intelligence
SNMP Monitoring Capabilities	MAX Remote Management
Failed Login Check	MAX Remote Management
Custom Event Log Checks	MAX Remote Management
Scripting Capability	MAX Remote Management
Hosted Services Provider	Google, Azure, Amazon
NextGen Firewall Solution	Sophos, SonicWall, Cisco

Distributed Denial of Service



> “Huge amounts of traffic can quickly overwhelm a business’ infrastructure and effectively knock it off the Internet.”

What is it?

In late 2014/early 2015, both the PlayStation Network and Xbox Live went down after a group called LizardSquad began using a tool called LizardStresser to attack the network connections. LizardStresser leveraged poorly secured routers that had default passwords. As a result thousands of routers were turned into internet-facing cannons that blasted garbage Internet traffic at the IP addresses critical to the gaming networks.

By leveraging tools such as NTP amplification, DNS reflection and SYN flood, huge amounts of traffic can quickly overwhelm a business' infrastructure and effectively knock it off the Internet. In a sinister twist, cybercriminals may try to extort money from a potential victim – threatening them with a DDOS attack if they don't pay.

Variations:
DDOS has been around for a very long time. In general, the attacks are categorized as connection-based or resource based in addition to the newer type of amplification attacks. Connection-based attacks simply attempt to open as many simultaneous connections as possible with the targeted server in order to degrade its performance. A Resource Exhaustion attack occurs when the server is overwhelmed with requests. In order to produce faster Resource Exhaustion, 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: "Hello, Hello, Hello, can you hear me?"

What technology will help defend my networks?

There are a range of options for companies that may be at risk of either DDOS extortion or DDOS attacks. Most importantly, if there are Internet-dependent critical systems they should not be located on premise, they should be in a data center with multiple Internet providers and infrastructure redundancy. Rackspace, Amazon, Google, and Microsoft Azure all have excellent Internet connections, DDOS mitigation capability and redundant infrastructure. A business that is dependent on its Internet connection should consider load balancing across two or more ISPs and consider DDOS mitigation services such as CloudFlare.

Distributed Denial of Service

What do I need to do?

Clearly the key to mitigating any style of attack is monitoring the performance of the network router. Using SNMP capabilities makes it relatively easy to determine how hard the firewall is working. On top of this, reports from an ISP can determine if the volume of traffic is excessive. Finally, being able to put in a network tap, or mirror a switch port on the outside of the firewall, and using a tool like Wireshark to see the inbound network traffic, can give you a good indication of whether you're under attack.

The less technological approach is simply to ask the users. Questions like "Is the Internet really slow?" and "Is saving files on the network drive nice and quick?", will give you a good barometer of network performance.

A quick and simple check to implement is a "ping" of the outside gateway, or a TCP service check on any exposed port like the VPN. If you see drops, then you know something is going wrong with the external network connection. If you see corresponding high CPU or packet rates on your Firewall then you're under attack. Most ISPs have filtering capability and are actively monitoring for this sort of attack; a call to the network provider can give you more details. Mitigation of this style of attack can be complex and requires an active plan. Increasingly, the attack may be accompanied by a ransom demand from cybercriminals. Access to the technical support of the ISP, and a discussion of the impact and mitigation of a DDOS attack, should take place before suffering the effects of an actual incident. Again, a more sophisticated Firewall with DDOS mitigation services, alongside a cloud-based DDOS mitigation solution may be required for businesses with mission critical, or ecommerce-based connections.

> **"Mitigation of this style of attack can be complex and requires an active plan."**

This should be underpinned by extensive consultation and network architecture reviews, possibly with a simulated attack to see how systems respond. A clean and "best practice" security approach to servers, especially DNS servers (no open resolvers), will ensure your organization is not used in a proxy or amplification-style attack. Additional value can be provided in ensuring firewalls, routers, edge switches, and servers are all patched and up-to-date; just one vulnerability left unpatched can leave you open to a DDOS attack, or to becoming an unwilling participant in a DDOS campaign against someone else.

What do I need in my product tool kit?

Patch Management for Servers hosting services	MAX Remote Management
SNMP Monitoring of Router, Firewall and switching infrastructure	MAX Remote Management
Redundant Internet Connections, Hosted DDOS services	CloudFlare
Packet Analysis/Inspection Solution	WireShark, NetFlow, Observium
NextGen Firewall with DDOS mitigation capabilities	Sophos, SonicWall, Cisco
Mail Protection	MAX Remote Management / MAX Mail integration

Brute Force Attack

> **Attacks consist of a predictable and systematic checking of all possible passwords until the correct one is found.**

What is it?

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, Outlook Web Access, and SMTP services. Attacks consist of a predictable and systematic checking of all possible passwords until the correct one is found. This then grants access to the network, in many cases with domain administrator privileges. At this stage it's unfortunately game over for the defenders.

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 consequences as a DDOS attack, only typically from just one or two IP addresses. Brute Force attacks and their cousins, SQL Injection, are a threat to all services exposed to the Internet. One of the most commonly attacked platforms is WordPress, as all installations have an easily located admin login page. Once the attackers have guessed correctly they gain unrestricted access to that account. If this site is hosted inside the company's network then complete network exploitation is likely.

Variations:

SQL injection attacks: Here an unauthorized user "injects" SQL code into fields where the SQL Server expects data values, and uses an available database connection to access your data. This type of attack can be extremely damaging because it lets the intruders execute commands directly against your database. This is a more sophisticated version of the Brute Force attack, as many different combinations of SQL injection need to be tried in order to gain access to the user ID and password table, which is frequently unencrypted or poorly encrypted.

What technology will help defend my networks?

Your first point of call is to look at implementing robust passwords for all Internet-facing services and managing those passwords accordingly. For commercial websites, it's a good idea to segment them off in a Firewall DMZ (demilitarized zone); this is an area between the company's private network and the outside public network. It works as a buffer zone that prevents outside users from getting direct access to a server that stores company data. Alternatively, you could move them to a hosted cloud provider that has multiple ISPs and DDOS mitigation. Certainly application-aware Firewalls have a role to play in securing SQL Injection attacks.

There are, of course, technological solutions available in ever-increasing complexity and expense. However, the most important advice is this: Don't get caught unaware of the risk of exposed services, especially for vendor-supplied or web-based applications that connect to SQL databases. Certainly prevention of breach is the goal, but so is awareness of the threat.

Brute Force Attack

What do I need to do?

The mitigation of Brute Force and SQL Injection attacks has a great deal to do with network architecture and the hosted application. The first piece to understand is how the SQL server is configured to communicate with the web application. 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, Windows Authentication mode should be implemented and the Lockout Policy feature utilized, as it makes Brute Force attacks time consuming.

It's important to remember that you should never use a domain administrator account as an SQL database connection account.

There are two key reasons for this:

- If you are compromised at this level that would be a disaster
- Locking out the administrative account, especially the domain administrative account, could result in a denial of service condition

When it comes to SQL Server authentication Brute Force attack vulnerability, the situation is grim. Older versions of SQL running on SQL Server Authentication have no features that allow you to detect when the system is under a Brute Force attack. This means that the SQL Server Authentication is a perfect target for this type of attack.

Looking at the encryption of database information, how it connects and authenticates to the application, and what security precautions can be implemented before an application and database system is implemented is strongly advised. It becomes a nearly impossible task to secure an application, which requires Domain Level Administrative privileges and has no logging or alerting capability running on an old version of SQL. In the best-case scenario VPN and/or Access Control Lists secure any Internet-facing services.

What do I need in my product tool kit?

Vulnerability Management for Applications	MAX Remote Management
SNMP Monitoring of Router, Firewall and Switching infrastructure	MAX Remote Management
NextGen Web Application Firewall with SQL injection mitigation capabilities	Sophos, Check, Cisco
Mail Protection	MAX Remote Management / MAX Mail integration
Failed Login Check	MAX Remote Management
Custom Event Log Checks especially with a newer version of SQL	MAX Remote Management
Web Application Vulnerability Scanner	ZED by OWASP, Nessus
Robust Password Management especially for exposed Internet Services and database connections	

Phishing Attack

> **“Every month thousands of businesses fall victim to email attachments that lead to serious network compromise.”**

What is it?

In November 2013, the UK's National Cyber Crime Unit warned of a mass email-spamming event targeting tens of millions of UK customers – predominantly small and medium-sized businesses. The emails carried an attachment that appeared to be linked to the correspondence in the message, for example a voicemail, fax, or details of a suspicious transaction or invoice.

The attached file was actually a piece of malware called CryptoLocker, which caused massive disruption to its victims by encrypting files and then demanding a ransom to unlock them. While CryptoLocker is one of the most infamous pieces of malware delivered via this type of attack, every month thousands of businesses fall victim to email attachments that lead to serious network and system compromise.

Variations:

Phishing emails remain the primary Vector for Malware attacks and are almost evenly distributed between two variants with a malicious Email Attachment (39.9%) or Email with Malicious link (37.4%). On a positive note, all Phishing emails have one thing in common: they arrive via email. This situation allows for multiple opportunities to mitigate the threat.

Phishing Attack

What do I need to do?

You have to understand that users are at some point going to click on or open something nasty. This understanding should inform your response and with an understanding of the threat, allow you to roll out a defense-in-depth strategy.

A study of Microsoft's Patch bulletins from 2013 demonstrates that removing administrator rights is an extremely effective first step against the threat of Phishing email exploits.

The report states that of the 147 vulnerabilities published by Microsoft in that year with a "Critical" rating, removing administrator rights mitigated 92% of the vulnerabilities. Verizon's team notes that 99.9% of exploited vulnerabilities in 2014 were disclosed and given a Common Vulnerabilities and Exposures (CVE) number more than a year prior to the patch being announced. Just 10 CVEs were responsible for nearly 97% of all exploits observed.

Understanding this data is key. Keeping up to date on patching the operating system and applications is the next "quick win". With these two items in place you are well on your way to making a business hard to hack.

> **"IT professionals have a huge opportunity to combat this sort of attack with multiple layers of defense."**

What technology will help defend my networks?

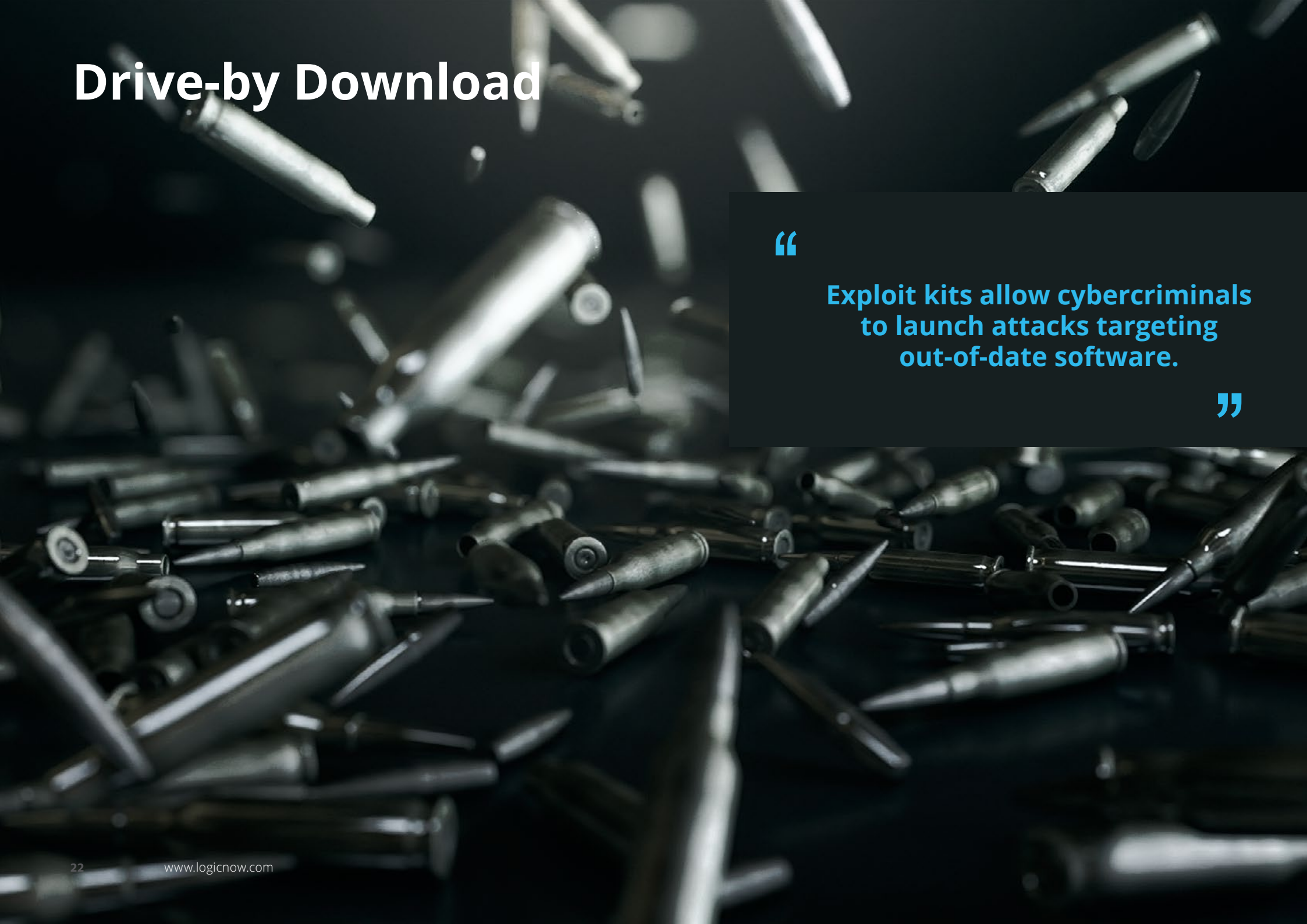
Focusing on protection from email-based attacks is a "quick win" for security-conscious IT professionals and would address over 77% of security incidents resulting from user interaction with email. However, it's folly to think of providing a security solution just built around the threat from email. It's more important to create a defense-in-depth philosophy that provides multiple detective and preventive solutions as part of a security bundle that attempts to mitigate all cybersecurity hazards.

IT professionals have a huge opportunity to combat this sort of attack with multiple layers of defense. Unlike the first three attacks listed, robust in-depth defenses can be implemented to protect users from opening harmful attachments or clicking on malicious web links.

What do I need in my product tool kit?

Patch Management of OS and third-party applications	MAX Remote Management
Managed Antivirus	MAX Remote Management
Web Protection	MAX Remote Management
Email Protection	MAX Remote Management / MAX Mail integration
Managed Online Backup	MAX Remote Management / MAX Backup
Mobile Device Management	MAX Remote Management

Drive-by Download



> **Exploit kits allow cybercriminals to launch attacks targeting out-of-date software.**

What is it?

In May of 2015, MadAdsMedia, a US-based advertising network was compromised by cybercriminals. They planted links that took visitors to multiple Adobe Flash exploits delivered by a cybercrime exploit kit. It's estimated that up to 12,500 users per day may have been affected by this threat.

In this particular case, the Nuclear Exploit kit was used to good effect. Exploit kits are efficient at distributing malware to users surfing the web. Such kits include exploits for multiple vulnerabilities within a single malicious webpage. Built-in checks target systems, web browsers and browser plugins, such as Flash Player, Adobe Reader, Java, or Microsoft Silverlight for anything that is not fully patched. An attack is then launched to exploit that specific out-of-date software.

What technology will help defend my networks?

As mentioned previously, you need to think about providing a broad security solution. Focusing on just one type of threat is not a terrific idea. Having said that, in the case of web-based threats, Web Protection offers far more than just a security solution and should form the basis of your thinking around security for this type of threat.

Firstly, Web Protection delivers a broader solution than Antivirus, and because of the fact that it works to prevent people from visiting certain known trouble hotspots, it actively reduces the chance of a malicious infection. This also means it can be used as a security awareness and educational tool. At the other end of the scale, the reports that can be produced from Web Protection can be used to help explain poor Internet performance, as well as provide a forensic tool to identify suspicious web traffic.

Drive-by Download

What do I need to do?

Just like with the Phishing email described earlier, there is a lot IT professionals can do to mitigate this sort of attack by implementing multiple layers of defense. Analysis shows that email with malicious links (37.4%) and web-based Drive by Download (16.6%) account for 54% of security incidents. Robust in-depth defenses can protect users from visiting harmful webpages where these threats reside. Focusing on web-based attacks is another "quick win" for security and would use many of the same technologies deployed against Phishing attacks.

When considering the threat the web poses, it's important to understand the delivery mechanism of the attack. This is most 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 that the bigger challenge is to block malicious web links delivered by means other than email.

> **"Analysis shows that email with malicious links and web-based Drive-by Download account for 54% of security incidents."**

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 an IT 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 secure; in fact history suggests that poorly secured ISP DNS servers are a major security problem. Compromised DNS servers can re-direct requests for a legitimate site to a fake site.

DNS is an important foundation of web-based communication so settling on one provider for all your customers – like Google's public DNS or Webroot's 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 have no Russian clients.

What do I need in my product tool kit?

Patch Management of OS and third-party applications	MAX Remote Management
Managed Antivirus	MAX Remote Management
Web Protection	MAX Remote Management
Secure or well-known public DNS service	Webroot Secure DNS, Google, Microsoft
Vulnerability Scanning Solution	MAX Risk Intelligence

Spear Phishing Attack

> **“Spear Phishing is like an old-fashion confidence trick. This makes it difficult to defend against as on the surface it’s not a technology-based threat.”**

What is it?

Fraudsters targeted an Omaha company, Scoular, in summer 2014 by using extremely legitimate looking emails to convince its financial controller to send a series of wires – totaling $17.2 million – to a bank in China. The emails also instructed the controller to get the wire instructions from a genuine employee of the company's actual accounting firm, KPMG.

While the KPMG employee did exist, and the email looked like it came from a valid KPMG email address, it was actually based on a server in Russia and the telephone number listed was a Skype account registered using an IP address in Israel. This attack was successful, and many subsequent Automated Clearing House (ACH) attacks have made big news in past years.

In many ways Spear Phishing is an old-fashion confidence trick, and on the surface is therefore difficult to defend against, because it does not appear to be a technology-based threat, but instead an attack on trust. As cybercriminals have evolved from crudely fashioned Nigerian 419 scams to "cute Russian girls", the line between common Phishing and Spam has blurred – not so with these types of targeted attacks.

Variations:
Spear Phishing will be targeted towards an organization and its advanced cousin, Whale Phishing, is reserved for senior executives.

What do I need to do?

When dealing with this type of targeted threat, the requirement for technology is certainly important, however user security awareness training becomes the best defense. In our case study example, the breached banks truly believed they were secure behind robust perimeter defenses, yet the manager end-points were not. Had the criminal gang deployed a zero-day attack, but users were not allowed to install programs – due to the removal of administrative privileges – the attack could have also been defeated. It's important to understand that security technology and people can both fail. So you need to give both the technology and the people as many chances as possible to detect and hopefully prevent the criminals' payday.

IT professionals have an opportunity to help businesses combat this type of sophisticated social engineering attack. Certainly there is an opportunity to provide Security Awareness training for new employees and annual refresher training. The more sophisticated could also provide Penetration Testing and Social Engineering Red Team services to help businesses continuously improve process and procedures when it comes to financial transactions and safeguarding confidential data.

Spear Phishing Attack

What technology will help defend my networks?

When dealing with this type of targeted threat, the requirement for technology is certainly important, however user security awareness training becomes the best defense. In our case study example, see page 30, the breached banks truly believed they were secure behind robust perimeter defenses, however the manager end-points were not. Had the criminal gang deployed a zero-day attack, but users were not allowed to install programs – due to the removal of Administrative privileges – the attack could have also been defeated. Again it's key to understand that security technology and people can both fail. So you need to give both as many chances as possible to be effective against criminals.

> **"Sometimes it's worth introducing an *"it's so easy to breach"* benchmark."**

Security audits and vulnerability scans are an important part of a company's security portfolio, and are essential to the compliance requirements for many. Sometimes it's worth introducing an "it's so easy to breach" benchmark. You don't have to be an expert and many good guys (as well as many bad guys) can use off-the-shelf tools to identify infrastructure vulnerabilities.

If you're moving towards a "full security" package of services to defeat this kind of attack, have a look at something called the Social Engineer Toolkit (SET)*. This is an open source tool designed to help you do penetration testing. You can now start sending some Spear Phishing emails to test your systems – with written permission from the appropriate chain of command, of course.

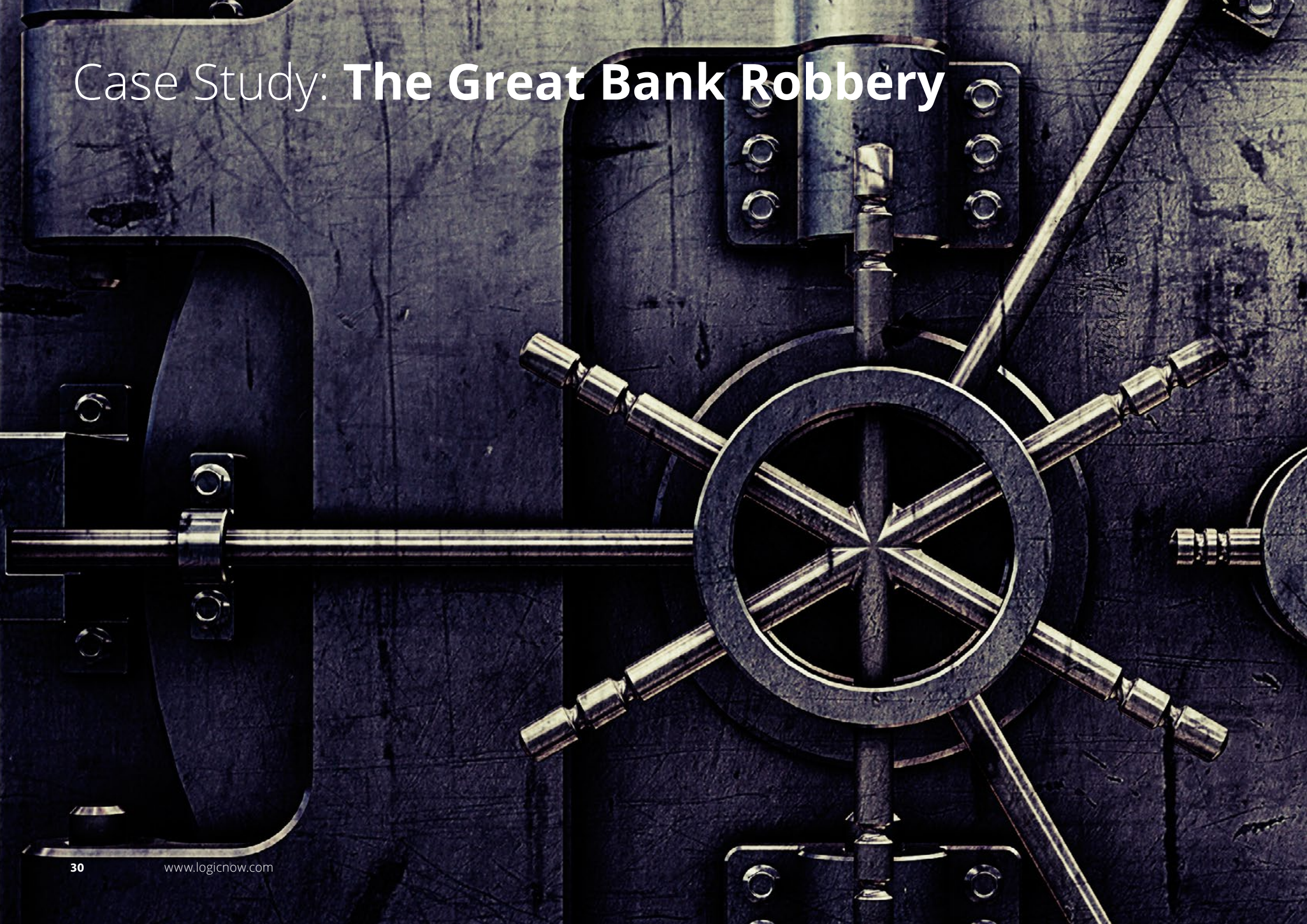
The SET incorporates many useful social engineering attacks all in one interface. The main purpose of SET is to automate and improve on many of the social-engineering attacks in use by cybercriminals, so you can stay one step ahead of the bad guys. SET can automatically generate exploit-hiding web pages or email messages, and can use Metasploit payloads to, for example, connect back with a command shell once the page is opened.

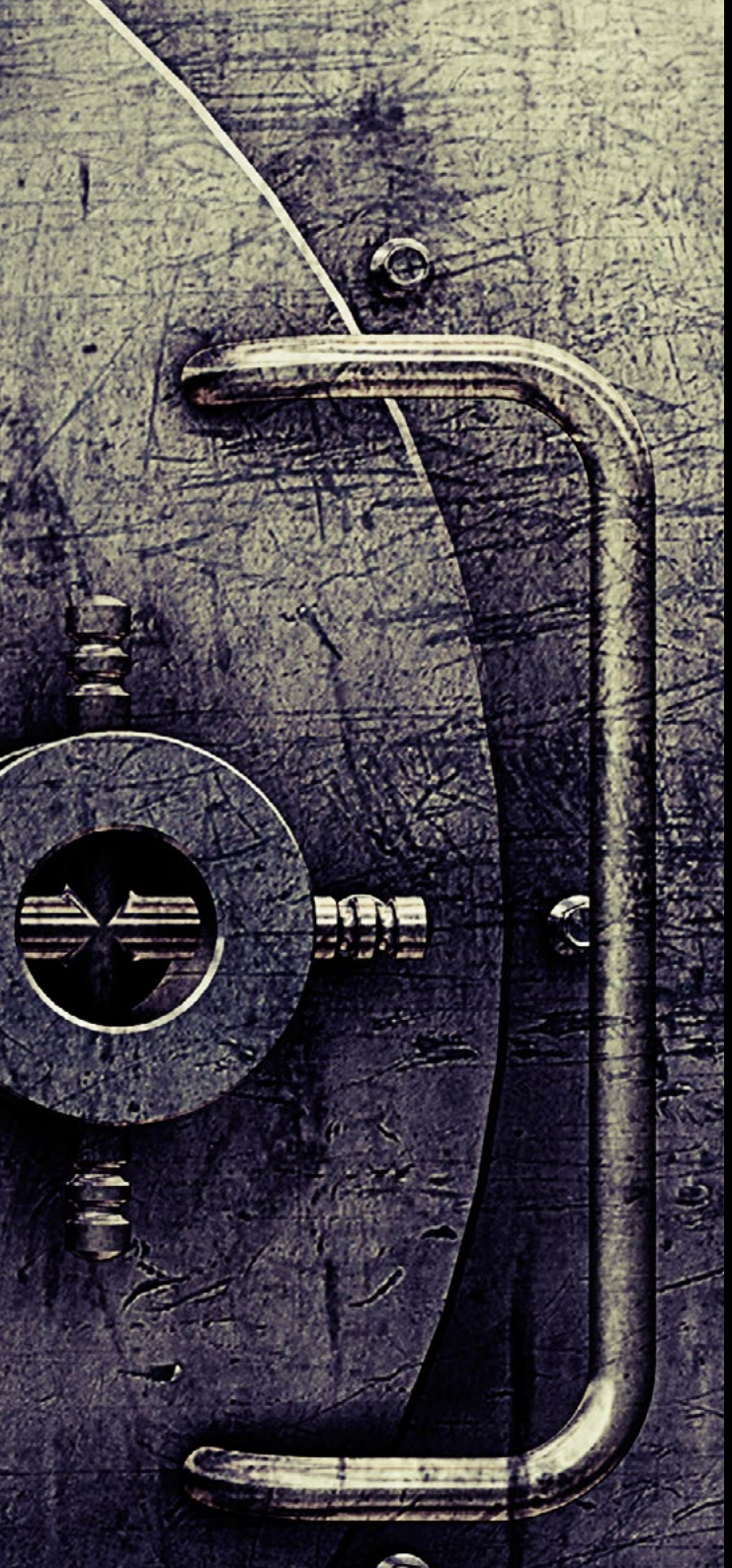
* https://www.trustedsec.com/social-engineer-toolkit/

What do I need in my product tool kit?

End-user security awareness training program	
Risk and Vulnerability Assessment	MAX Risk Intelligence
Patch Management of OS and third-party applications	MAX Remote Management
Managed Antivirus	MAX Remote Management
Web Protection	MAX Remote Management
Managed Online Backup	MAX Remote Management / MAX Backup

Case Study: **The Great Bank Robbery**





Stories early in 2015 revealed a massive attack on the banking system across the globe through the use of Carbanak malware delivered via a Spear Phishing campaign. Reports estimate that between USD $300 million and $1 billion were stolen by the gang over the course of two years. However, further investigation reveals that a basic bundle of security products could have prevented this string of cyber attacks.

Patched and updated machines would have not been affected by this Spear Phishing attack. “All observed cases used spear phishing emails with Microsoft Word 97 - 2003 (.doc) files attached or CPL files. The doc files exploit both Microsoft Office (CVE-2012-0158 and CVE-2013-3906) and Microsoft Word (CVE-2014-1761),” said one source.

The age of the Trojan malware that was used indicates that it is very likely that Antivirus would have intercepted it. Reports also indicated that there was evidence that in most cases the network was compromised for between two to four months. This means that the worst-case scenario is that the banks in question had up to four months to deploy the appropriate patches, but failed to do so.

As this attack started off with a Spear Phishing email attack on the bank managers, the cyber criminals understood both the infrastructure vulnerabilities and had enough information about bank managers (compiled from Social Networking sites) to launch an enticing malicious email with an attachment.

Advanced Persistent Threat Attack — Cybercriminal / Hacktivist

> **APT actors will target a specific organization or entity and perpetrate a sustained campaign until they achieve their goals.**

What is it?

In February of 2015, The APT group Desert Falcons claimed some 3,000 hacking victims in more than 50 countries. Most of them were located within Palestine, Egypt, Israel, and Jordan, but there have also been discoveries in Saudi Arabia, the UAE, the US, South Korea, Morocco, and Qatar among other places. The victims include military and government organizations, employees responsible for health organizations and combating money laundering, economic and financial institutions, leading media entities, research and educational institutions, energy and utilities providers, activists and political leaders, physical security companies, and other targets that have access to important geopolitical information.

What separates APT actors from other malicious actors is their level of sophistication, organization and resources. APT actors will target a specific organization or entity and perpetrate a sustained campaign until they achieve their goals. Their persistence, adaptability, and ability to vary attack forms also differentiate APT actors. They may act independently or more likely, as part of a larger team or effort. In the case of teams, activities may be fully compartmentalized, much like how a business separates roles, functions and organizations internally.

Variations:
There are well over 100 known APT groups documented by security researchers. One of the most well known is Anonymous, which claims thousands 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 three things in common:

- They target you to steal all your Internet things
- They tend to specialize either along a line of ideologically / culturally / politically / religious motivation or focus on technological espionage either seeking knowledge and information for advancement of an ideological/ political/ cultural/agenda or the theft of intellectual property
- Persistence – this type of actor continues the attack, probing weakness, Brute Forcing, Spear Phishing, researching, and even conducting DDOS in order to ruin your day

What do I need to do?

As an IT professional you have to 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 I 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 actors such as these? The sort of company that draws the ire of groups like these is usually a near enterprise-level organization that may have significant cyber risks due to political, cultural, religious, or ideological products or services.

> **“Do you have the skills to take on this sort of challenge, and is it worth your time and money to build cyberdefenses to ward off actors such as these?”**

* https://www.sans.org/critical-security-controls/

What technology will help defend my networks?

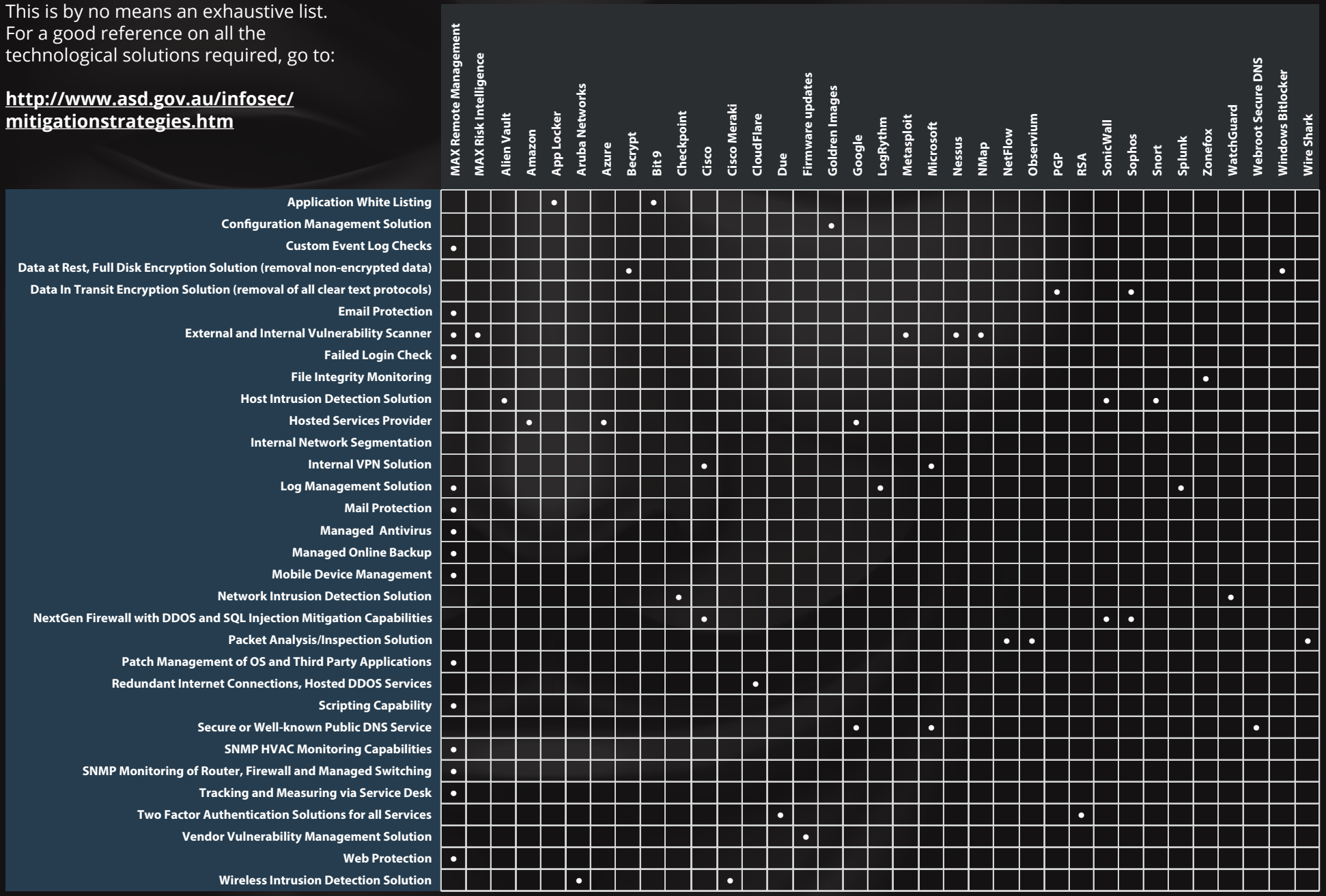
Even the biggest security organizations are struggling against APT, and all the tools of the security trade are deployed in attempts to ward off these cyber bad guys.

In this sort of environment, you will need to deploy sophisticated and not so 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 specific security skill sets will be needed not to mention 24/7 monitoring and incident response. Adding network segregation, Intrusion Detection Systems, and application whitelisting capability, as well as ubiquitous use of encryption of data at rest and in transit are some of the more sophisticated tools you will need when trying to fend off these actors.

In some cases the IT professionals will be the clean-up crew, responsible for “metaphorically” burning the network to the ground and rebuilding it to remove the foothold that the APT group(s) gained on the business. This is a long and difficult road ahead and certainly a massive project to consider. The best advice here is to methodically design and implement a secure network using a 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.

This is by no means an exhaustive list. For a good reference on all the technological solutions required, go to:

http://www.asd.gov.au/infosec/mitigationstrategies.htm



All in addition to End User Security Awareness Training Program (ongoing), Service Provider Security Awareness Training Program (ongoing) and Internal Network Segmentation.

Advanced Persistent Threat Attack — Foreign Intelligence Service

> “In the best cases, they are spying on your activities. In the worst case, it’s possible every system and device is hopelessly compromised or possibly destroyed.”

What is it?

In February 2015, Moscow-based cybersecurity firm Kaspersky Lab revealed a number of sophisticated cyberattacks by state-sponsored hackers, labeled the Equation Group. Reuters reported that two former National Security Agency (NSA) employees confirmed the validity of the analysis and said that operatives within the NSA "valued these spying programs as highly as Stuxnet."

The report also stated that, "the Equation group and the Stuxnet developers are either the same or working closely together." Various security experts have traced back the Stuxnet attacks to the US and Israeli governments. According to the report, the Equation Group hackers were able to rewrite the hard-drive software of infected computers, which makes the normal attack recovery procedures (replacing the hard drive, reformatting the drive, wiping a computer's operating system and reinstalling software) ineffective, since spyware-manipulating firmware is impossible to detect or remove.

Generally, APT hackers – criminal or otherwise – employ familiar methods, using Phishing emails or other tricks to fool users into downloading malware. But Foreign Intelligence services bring this to the next level. In the best cases they are spying on your activities. In the worst case it's possible every system and device is hopelessly compromised or possibly destroyed.

Variations:

An exact count of which nations are developing cyber warfare capability is not readily available, however most developed nations (and a few developing ones) are actively building this capability. For now it's accurate to say 50 to 100 countries have varying degrees of capability. A nation-state engaging in offensive cyber warfare embodies the worst aspects of any APT group. The sophistication and expertise of the advanced hackers let loose on a private, or government organization are terrifying to behold. Millions of dollars in physical damage is possible, not to mention massive disruption and ensuing panic. These APT cyber units of national military and intelligence agencies are given classified budgets with access to almost unprecedented resources. A significant philosophical difference exists between APT criminal groups and hacktivist APT actors. A nation-state's offensive APT cyber units have access to top training resources, and no fear of criminal prosecution for their acts. They operate with obscurity and have no fear of facing retribution. The government they serve typically directs the legality and ethics of their acts.

What do I need to do?

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 IT professional is to ensure those systems are, and continued to be, protected from Internet access.

A list of infrastructures that should not be connected to the Internet, includes: Military/governmental classified computer networks/systems; Financial computer systems, such as stock exchanges; industrial control systems, such as SCADA in Oil & Gas fields; Life-critical systems, such as controls of nuclear power plants, computers used in aviation and computerized medical equipment.

> **“Too many 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 will need to help a business implement security solutions to ensure the benefits of connection to the Internet do not introduce vulnerabilities with enormous consequences if exploited.

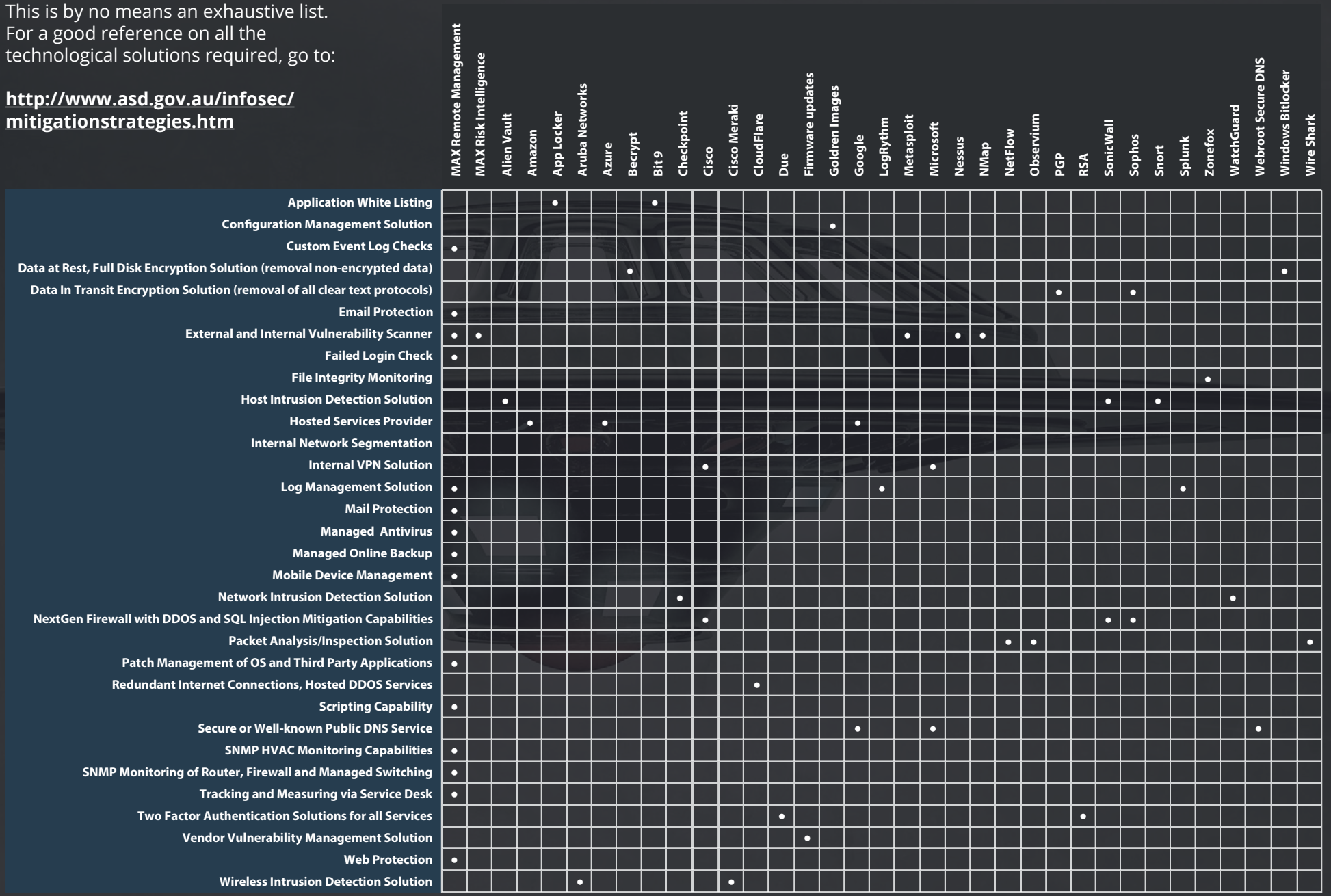
What technology will help defend my networks?

Serious consideration should be made about architecture and Internet connectivity. “Air Gap” networks and robust physical security, as well as all the technological solutions mentioned previously, need to be considered, even on the “Air Gap” network. A network that is not exposed to the Internet is, in theory, secure. However, some sophisticated attacks, by nation-state level resources, can even compromise computers in an “Air Gap” configuration.

However, 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, the best advice is to invest heavily in physical security, ubiquitous encryption, and have a non-persistent and heavily encrypted connection to the Internet, via the Tor network.

This is by no means an exhaustive list. For a good reference on all the technological solutions required, go to:

http://www.asd.gov.au/infosec/mitigationstrategies.htm



All in addition to End User Security Awareness Training Program (ongoing), Service Provider Security Awareness Training Program (ongoing) and Internal Network Segmentation.

Data Destruction

> **“The hack’s purpose was to both destroy property and release confidential info.”**

What is it?

The December 2014 attack on Sony Pictures Entertainment has set a new benchmark in the damage cybercriminals can inflict on an enterprise that has a cavalier attitude towards information security. Security firm Mandiant reported the hack's purpose was to "both destroy property and release confidential info." 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 firing of senior executives).

Variations:

In the annals of cybercrime there has not been such a collection of different security incidents all happening rapidly over a short period of time. There are only a few incidents to identify where the motive of the attackers has been so malicious. At no point did the attackers try and extort money out of 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. The claim that the malware used in this attack was not detectable by antivirus programs is suspect and distracts us from the fact that Sony had a "passwords.xls" document that was neither encrypted nor password protected, which listed all passwords including ones with administrative access. As discussed earlier in this document: if a single vendor's antivirus solution is the only security control in place at a global company then the results of this hack were entirely predictable and avoidable.

Data Destruction

What do I need to do?

As an IT Professional you need to design a security solution that addresses the risks the business is facing. Implementing a whole bunch of technology is rarely the best solution. Designing a simple, manageable network and establishing a continuous monitoring solution will be easy "security" wins. In virtually all the recent data breaches basic security was not in place, and organizations relied too heavily on perimeter defenses.

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 alongside elements of people and process. As an IT professional, the best place to start is with a security assessment, a plan to remediate the critical items the business identifies, and then a solution to monitor the system for compliance. It is often the simple things that are most effective when it comes to security. According to James Lewis's seminal paper on Cybersecurity in 2013*, little if anything has changed since then:

> **"All your hard work will be ineffective if your management does not support and endorse a security program."**

- More than 90% of successful breaches required only the most basic techniques
- Only 3% of breaches were unavoidable without difficult or expensive actions
- 96% of successful breaches could have been avoided if the victim had put in place simple or intermediate controls
- 75% of attacks use publicly known vulnerabilities in commercial software that could be prevented by regular patching

What technology will help defend my networks?

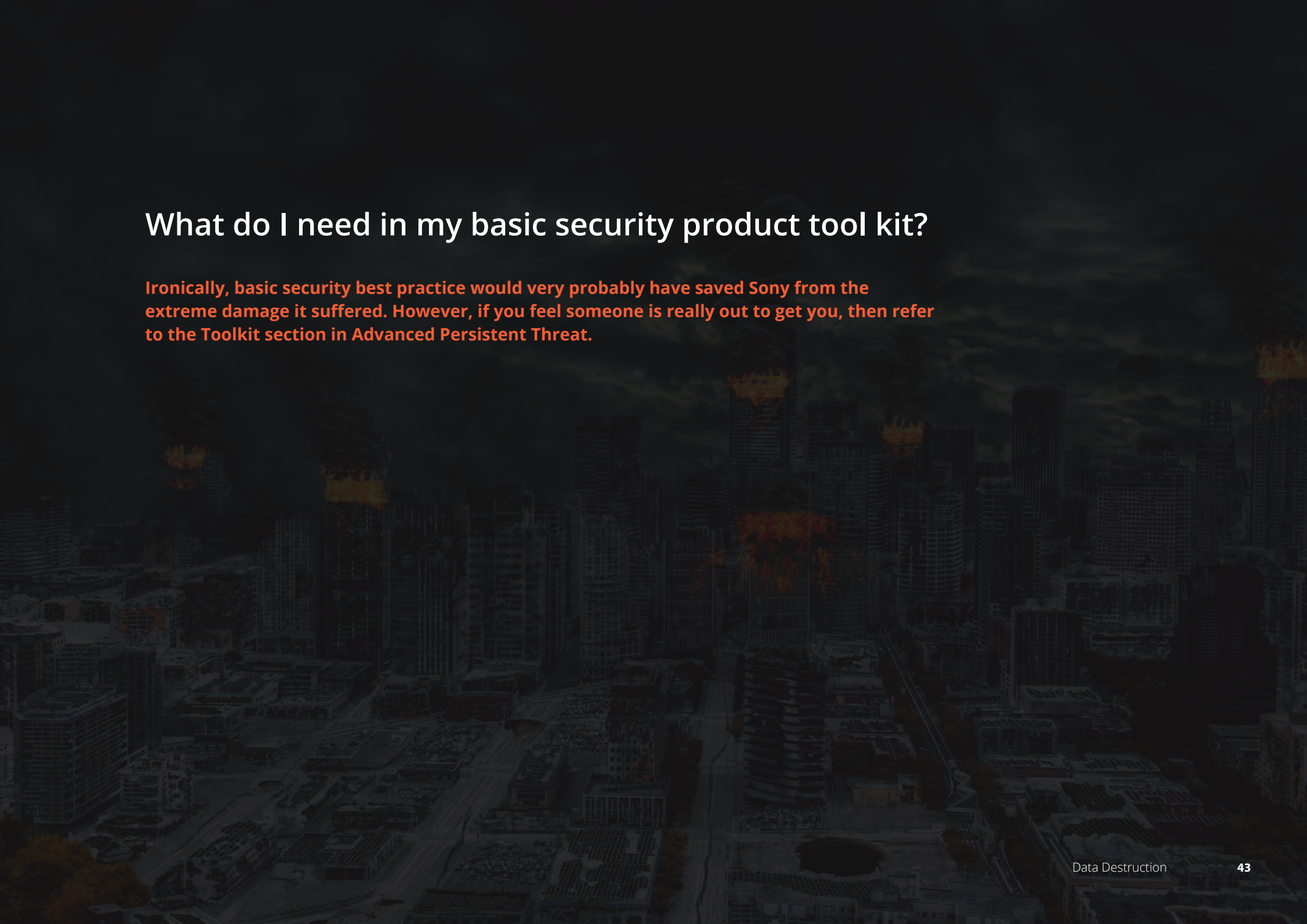
IT Professionals have a lesson to learn here. All the hard work, diligence, and security technology will be ineffective if the management at the company does not support and endorse a security program. If this is the case you're going to need to get really good at restoring data from backup.

The Sony attack is used in this paper to illustrate the worst possible scenario, and what happens if the organization is unprepared for attack. The Sony attack, following in the footsteps of the Saudi Amoco attack and Stuxnet have given rise to the data destruction attack. Recent successful attacks on Critical Infrastructure in the Ukraine and Israel show the motivation of APT actors to inflict physical harm through hacking. 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. The layered security defense including excellent business resiliency capability – in the form of robust backup - is the key to surviving the worst attack malicious actors can devise.

* https://csis.org/files/publication/130212_Lewis_RaisingBarCybersecurity.pdf

What do I need in my basic security product tool kit?

Ironically, basic security best practice would very probably have saved Sony from the extreme damage it suffered. However, if you feel someone is really out to get you, then refer to the Toolkit section in Advanced Persistent Threat.



Connect with us!

Please get in touch if you have any questions about any of our services.

UK: +44 (0) 1382 309040
US: +1 855 217 7199
APAC: +61 (0) 8 7123 4060

info@logicnow.com

https://www.linkedin.com/company/logicnow

@LOGICnow

LOGICnow
CHOOSE INTELLIGENCE

www.logicnow.com

recycle