THREAT LANDSCAPE 2019

The Threat Landscape, as IL7 Security sees it

IL7

SECURITY CONSULTANTS

The threat landscape in 2019, as IL7 sees it.

This short paper looks at the threat landscape today. It looks at the new attacks as well as looking at new targets. Distributed Denial of Service (DDOS) are increasing again presenting a major threat to operations, customer access, financial and reputational risk, so it is worth looking at this phenomenon first. But we should also look at Critical National Infrastructure and how attacks are targeting our facilities, fuel and transport. The legally binding NIS regulations (May 2018) have caught many of our essential service providers by surprise at the range of security controls required by the NCSC Cyber Assurance Framework.

The case for Installing Denial of Service protection

In 2016, we saw several huge attacks — many that exceeded 1Tbps. In 2017, by contrast, we saw fewer large distributed denial-of-service (DDoS) attacks, possibly because hackers were finding little advantage in taking a company completely offline. Another explanation is that hackers were simply enjoying the success of the previous year's myriad of extortion and ransomware-oriented attacks, as well as the many DDoS associated data breaches.

So far in 2018, however, the big attacks are back with a vengeance. DDOS attacks could bring businesses down and international trade will suffer through lack of communications in an environment of fractured international relations. On a national level, core internet infrastructure will become a target as nation states and terrorist groups aim to inflict widespread economic damage on their adversaries. Existing business continuity plans can no longer be relied upon. Businesses and Government need to engage with internal and external stakeholders to agree alternative methods of communication (e.g. telex, satellite, microwave), supplying and trading .

Earlier this year we saw the largest DDoS attack ever recorded — 1.35Tbps — using a new type of attack called Memcached, which will be discussed later. Then, a 1.7Tbps DDoS attack was recorded. Previous amplification attacks, such as DNSSEC, returned a multiplication factor of 217 times, but Memcached attacks returned amplification records exceeding 51,000 times!

In fact, the potential return from Memcached attacks is so large that they do not require the use of botnets, making them a new and dangerous risk vector. We are hoping that these attacks will go the way of the Simple Service Discovery Protocol (SSDP) amplification attacks, which used the protocol designed to advertise and find plug-and-play devices as a vector. SSDP amplification attacks are easily mitigated with a few simple steps, including blocking inbound UDP port 1900 on the firewall. There are similar steps that Organisations can take to mitigate Memcached attacks, including not exposing servers and closing off ports.

This year we are also seeing different uses for DDoS beyond simple volumetric attacks, including what we call quantum attacks. Quantum attacks are relatively small and designed to bypass endpoint security and avoid triggering cloud failover mitigation. These attacks are being used for scouting and reconnaissance. In a recent incident, Once such quantum attack that never peaked over 300 Mbps, but it featured 15 different attack vectors, went on for 90 minutes, and involved all of the available globally distributed 'scrubbing' centres. This attack came from all over the world and was designed to bypass perimeter hardware, using protocols to circumvent their defences. The attackers behind such campaigns may start small, but they can quickly add botnets, attack vectors, and ports to get what they want.

One DDOS protection vendor reports that it recently thwarted what is believed to be the first IPv6 attack. This attack presented a new direction that attackers are likely to pursue as more and more companies adopt IPv6 and run dual IPv4/IPv6 stacks. We believe that IPv6 vectors will continue to emerge as Organisations around the world move to adopt the new standard.

You can also expect to see more Layer 7 (application layer) attacks, including those targeting DNS services with HTTP and HTTPS requests. These attacks are often designed to target applications in a way that mimics actual requests, which can make them particularly difficult to detect. It is important to note, however, that Layer 7 attacks are typically only part of a multi-vector DDoS attack. The other parts are aimed at the network and overall bandwidth.

DDoS attacks can be found in a multitude of sizes and for any reason imaginable. They can now be used to find vulnerabilities, to locate backdoors for exfiltration, and as a smokescreen-like distraction for other activities. Today's organized criminals can focus on the results that they want and simply buy or rent the malware or botnets they need to get there. Some have gone so far as to comment that criminals are getting more and more like corporations, each with their own specialization. The simple fact is that if you're online, you're susceptible to an attack. Whether you are vulnerable or not is entirely up to you.

Customers surveyed in the early part of 2018 showed a growing concern over ransomware. And for good reason. According to the Verizon Data Breach Incident Report 2018, this threat has become "… the most prevalent variety of malicious code for this year's dataset."1 The Verizon report goes on to observe that ransomware is an interesting phenomenon that, when viewed through the mind of an attacker, makes perfect sense.

Emerging threats to CPNI

Before 2018, successful attacks against critical infrastructure were relatively rare – they were always feared, but highly uncommon. Not anymore. Last year, we saw the hacking group GreyEnergy, which took down Ukranian power grids in 2015, systematically target other critical infrastructure across the Eastern European nation and its neighbours. Industrial control systems running SCADA software in Ukraine and Poland were GreyEnergy's primary targets this year. Rather than shut down the grids after compromise, the attackers preferred to remain undetected and cover their tracks after collecting the intelligence they were seeking. According to researchers, this new degree of stealth is because the attackers were either preparing to sabotage the networks at the most damaging time possible. Alternatively they may be setting the stage for another APT1. Interestingly, fileless attacks, see below, were part of GreyEnergy's arsenal.

Last year also saw the emergence of perhaps the most damaging critical infrastructure-specific malware since Stuxnet: Triton. Widely believed to have been developed by Russia, Triton was used in an attack against a Saudi Arabian petro-chemical plant, shutting it down (although the shut-down seemed to be inadvertent). Triton targets Industrial Control Systems, with the aim of handing over full control to the attackers. This year, given the ongoing geopolitical uncertainty, we expect to see more critical infrastructure-specific payloads targeting SCADA and ICS systems across the globe.

Organisations need to avail themselves with unprecedented levels of collaboration. To get the best results from this more collaborative culture, business leaders will need to ensure conversations are underpinned by proficiency. There has never been a greater organisational need to attract talent and retain knowledge. 2019 will see more malicious attacks through disruption, malware and misinformation whilst increasing regulation will prevent fighting back. Organisations need to talk to each other and collaborate in defence. This will harden the debate between cloud and on-prem.

Threats to Everyone

Ransomware

Ransomware will be used to hijack the Internet of Things. Already one of the most prevalent ways to exploit the value that organisations place on digital information, ransomware will evolve to target connected smart physical devices, potentially putting lives in danger. Cybercriminals have built up a repertoire of other attacks making ransomware less needed. Ransomware is noisy, threatening and most people are trained not to pay—making it a last resort. But this doesn't mean ransomware is going away. Over the last year, many of the worst manual ransomware attacks started when the attacker discovered that an administrator had opened a hole in the firewall for a Windows computer's remote desktop. Closing these easy loopholes goes a long way to preventing ransomware attacks. Malicious spam is a primary vector of malware with email messages most commonly the source of bad links and attachments. At the very least, organisations need to be aware that malware may leverage files that aren't typically considered dangerous, like Office documents, to start the infection process. Educate employees about the risk of email, how to spot a bad link and the importance of validating files before opening them. Practice the security fundamentals such as using a password manager and never reusing passwords. Change the default administrator passwords on things like home routers, modems and network-attached storage servers and add a passcode or password pattern to phones. For administrators, it's vital to keep up to date with operating system patches and app or

[1] APT = Advanced Persistent Threat

software updates, which so frequently provide the means of attack to criminals. Engage with industry bodies to lobby for (and influence) regulation ensuring minimum security standards for Internet of Things (IoT) devices. Ransomware can be:

- Used in completely opportunistic attacks, affecting individuals' home computers, as well as targeted strikes against Organisations.
- Attempted with little risk or cost to the adversary involved.
- Successful, with no reliance on having to monetize stolen data.
- Deployed across numerous devices in Organisations to inflict bigger impacts and command bigger ransoms.

Ransomware attacks have grown in such significance that they have been cited by the World Economic Forum2 as a global security issue. According to the WEF 2018 Global Risk Report, "The financial impact of cybersecurity breaches is rising, and some of the largest costs in 2017 related to ransomware attacks, which accounted for 64% of all malicious emails. Notable examples included the WannaCry attack — which affected 300,000 computers across 150 countries — and NotPetya, which caused quarterly losses of US$300 million for a number of affected businesses." In fact, according to the Cisco 2017 Annual Cybersecurity Report3, ransomware is growing at a yearly rate of 350%.

WannaCry

WannaCry is a ransomware crypto worm targeting machines running certain older versions of the Microsoft Windows operating system. One characteristic that made this exploit dangerous was the variety of different elements that it contained, including a transport mechanism used to spread through a network. The mechanism would scan for vulnerable systems, then use the Eternal Blue exploit to gain access to the system via a vulnerability in the Windows Server Messaging Block. It is thought that this exploit is how the WannaCry infection began. The malware then used the Double Pulsar backdoor tool to create a copy and install itself. Both Eternal Blue and Double Pulsar were released by the hacker group the Shadow Brokers. In a single day, the code was reported to have infected more than 230,000 computers in over 150 countries.

Once executed, the WannaCry malware would check for the presence of a kill switch domain. If the kill switch domain could not be reached, the malware would encrypt the device data, then attempt to spread to other devices on the Internet. The kill switch domain was eventually found in the malware itself, registered, and pointed to a DNS sinkhole, which rendered the malware useless. Attackers released several variants of WannaCry with different kill switch domains, and even attempted a DDoS attack on the domain using a Mirai botnet variant.

Petya and NotPetya

Petya, a reference to an atomic-powered satellite in the James Bond film Goldeneye, is encrypting ransomware that predated WannaCry. Propagated via infected emails, Petya works by infecting the master boot record on Microsoft Windows machines. Once executed, the payload encrypts a hard drive's file system table, prevents Windows from booting, and presents a screen demanding payment.

In 2017, after the WannaCry attack, a second variant of the ransomware emerged. This version, named NotPetya by Kaspersky Labs to differentiate it from the previous malware, used Eternal Blue to propagate itself.

BOTNETS

It is important to note that bots themselves are not necessarily malicious. Bots and botnets can be used in many legitimate ways, including aggregation tools, site indexing, online trading, and more. In fact, as of 2016, bot traffic on the Internet surpassed that of human-initiated traffic.

Even when used destructively, however, it is useful to remember that botnets are themselves merely a tool, and a tool with many uses. Botnets are probably best known for being used in DDoS attacks, but they have also been used to send spam and propagate phishing attacks, sniff traffic for private information displayed in clear text, record keystrokes, and manipulate polls and games.

The primary function of botnets is to recruit more bots. The examples that follow include several of the most recent botnets, and the multiple factors that make them dangerous. Botnet examples include:

- The malware has been designed to target Internet of Things (IoT) devices, which means that targets are always on and available 24/7/365.
- Many of the target hosts are in use with low or no security precautions; in fact, many working IoT devices still use factory default credentials. These devices are often not monitored at all.
- The malware includes a means to use infected devices to scan for other vulnerable targets.
- End users typically notice little or no changes to their network, except for occasionally slower speeds.

The Changing Face of Cyber Attacks

As botnets have evolved and spread, they have actually become money makers in their own right. It is possible to “rent” a botnet for any purpose the buyer desires. This not only gives criminals a dangerous weapon, but it makes creating and spreading a botnet a lucrative proposition.

Among the most notorious known botnets, Mirai was one of the first to make use of IoT devices several years ago. Mirai takes advantage of the publicly released source code that powers everything from routers to closed-circuit television (CCTV) cameras and DVRs to scan the Internet looking for devices that use factory default or hard-coded credentials. Once found, these devices are infected with malware and can be used for DDoS attacks. Mirai inflicted a large-scale, Internet-wide disruption in 2016, when the botnet shut down security expert Brian Krebs’ site and targeted DNS provider Dyn. Mirai is said to have generated traffic volumes of over 1Tbps and featured 10 pre-defined attack vectors.

The Mirai source code has since been placed on GitHub, ensuring that the threat it posed continues. At least two new variants have been seen, including Sartori, which implements exploits on the web interface of particular routers. Another variant, called Okiru, which some sources describe as another version of Sartori, targets embedded processors. Other variants — Masuta and PureMasuta — exploit a vulnerability in another router's use of the Home Network Administration Protocol (HNAP). Sartori, Okiru, Masuta, and PureMasuta

WireX is a botnet designed to attack content delivery networks (CDNs) and other content providers with DDoS traffic. This botnet is primarily made up of Android devices running malicious apps that were actually offered on the Google Play store for a time. WireX ran a volumetric DDoS attack at the application layer, with traffic that was primarily made up of HTTP GET requests aimed at a number of different CDNs and content providers. Devices from more than 100 countries participated in the attack, which was finally halted by the cooperative efforts of researchers from a number of different Organisations.

Reflection and amplification attacks

Reflection and amplification attacks often come as a pair, though they serve two different but often compatible purposes. By spoofing source addresses, attackers can hide their identity by "reflecting" requests off a third party. Amplification attacks add to this by taking advantage of processes in which a small query will have a large — sometimes very large — response. Amplification attacks are, by nature, always reflection attacks as well.

Amplification attacks begin with the attacker spoofing the target's IP address. This is one reason that the majority of amplification attacks target services that use UDP, as it is a connectionless protocol that does not validate the source IP address. In the next step, the attacker sends a small query to a server or resource that generates a very large response forwarding that response to the target. The answering resource is behaving exactly as it should; in fact, the only real issue is that it is reachable by the attacker. The United States Computer Emergency Readiness Team (US-CERT) publishes a list of services vulnerable to these attacks.

Memcached attack

The recent Memcached attack deserves a closer look, if only for the size of the amplification factor that it generated.

Memcached is a distributed memory caching system that uses free, open source software originally written in 2003. Memcached stores data and objects in RAM to speed up the response of dynamic database-driven websites. Memcached services are typically found in a cloud environment and should be reachable on the local network only, behind a firewall. It should not be open to the Internet. Unfortunately, some networks and some Linux servers have left TCP or UDP port 11211 open to the Internet. In a recent example, such a large amount of response traffic was generated that the attack significantly impacted the owner of the amplification server, as well as the actual target of the attack.

Memcached uses UDP, a connectionless protocol that does not require authentication. This makes it easy for attackers to spoof a target's IP address to launch an attack.

Attackers can take advantage of a simple “stats” command from a spoofed target IP address—a payload of approximately 15 bytes. The reply, on the other hand, can range from 1500 bytes to hundreds of kilobytes. Memcached servers typically have high bandwidth access links because of the nature of their function and are often located on networks with high-speed transit links, making it possible to launch volumetric attacks quickly without the need for a botnet. Because of how Memcached is configured, it is possible for hackers to search for servers listening on TCP or UDP port 11211 to find vulnerable servers. According to Krebs on Security, the potential devastation of Memcached DDoS attacks is now being used to threaten sites, demanding ransoms to stop assaults.

This information also makes it relatively easy to block Memcached attacks, according to Johannes B. Ullrich, Dean of Research at SANS Technology Institute. “You should see traffic *from* port 11211 if you are hit by this attack. Blocking all traffic from port 11211 should be possible as all modern operating systems tend to use a source port higher than that for client connections. But given the traffic volumes people are seeing, you will likely need help ‘upstream’ or from an anti-DDoS company.

Layer 7 Attacks

Large-scale DDoS attacks have captured the media’s attention, but from the perspective of cybercriminals, the focus is increasingly toward web application, or Layer 7, attack. In fact, according to the Cisco 2018 Annual Cybersecurity report, application DDoS has overtaken network DDoS this year.14 Such attacks provide virtually no warning, are much more difficult to spot than DDoS attacks, and because they often target consumers, they can do irreparable damage in a very short amount of time. Techniques include:

- Cross-site scripting (XSS) is a form of injection in which an attacker injects malicious script into a web application. The end user will have no idea that a hacked site should not be trusted.
- Cross-site request forgeries (CSRF) trick end users into executing state-change actions on a web app with which they are authenticated. Such attacks can instigate actions such as transferring funds or changing email addresses.
- SQL injections are a well-known exploit in which SQL data is inserted into a query response from a client.

Web applications are increasingly indicated in breaches, growing even more strongly in 2017 to surpass privilege misuse, cyber-espionage, and point-of-sale and payment card skimmers, among others. When considering industries that have been breached, Verizon reports that the retail industry has been most affected, with healthcare coming in second. Payment Card Industry Data Security Standard (PCI-DSS) requirement 6.6 suggests “installing an automated technical solution that detects and prevents attacks” as a method of mitigating dangerous web application attacks. Most companies utilize a Web Application Firewall (WAF) to meet this requirement, but it is not a “one-size-fitsall” solution. To be effective, a WAF must protect your applications regardless of platform, and must take into account that many applications are housed in more than one environment. An effective WAF must be a cloud, hardware, or CDN-agnostic solution. In many cases, the best approach is to combine WAFs with DDoS mitigation vendors. This combination ensures that an attack will not sneak in via a gap in coverage, which can occur when protections are provided by disparate vendors.

Rasputin

The name Rasputin has frequently come up in discussions about web application exploits over the past year. Rasputin is not the name of an exploit, but rather the alias of the author, said to be a Russian-speaking, financially motivated hacker. Rasputin is believed to have breached over 60 prominent targets, state and local governments, and colleges and universities in the U.S. and the UK. Rasputin apparently developed his own SQL injection scanner, which he used to find and take over vulnerable targets. This approach is noteworthy, not because SQL injection scans are unusual, but because they have become so common that most hackers take advantage of freely available scanners to conduct reconnaissance, rather than go to the trouble to write their own. Once vulnerable targets have been identified, Rasputin conducts an SQL injection attack, making off with personal data that is then offered for sale.

IPv6 Exploits

IPv4 addresses are exhausted. This forecast, first examined in the 1980s, has been in the process of being fulfilled since 2011 in some regions. As of September 2015, North America exhausted its pool of addresses. While ISPs in each region may have unassigned pools of IP addresses, and can recycle those that are no longer needed by subscribers, the fact is that IPv6 is finally beginning to make its way into the mainstream. Because of the fundamental differences between them, it has been vitally important that existing IPv4 networks can still operate as IPv6 gets implemented. Some companies have begun the process by running “dual stacks,” running IPv4 and IPv6 in parallel, often with two different teams. This approach speeds IPv6 network implementation but works against consistent security. Complicating matters even further, many security tools still do not support IPv6, or may not be configured properly. This allows attackers to bypass firewalls and intrusion preventions systems, generating malicious IPv6 traffic that these controls do not recognize. Another attack features both IPv4 and IPv6 traffic. Such an attack can proceed while target security teams implement IPv4 defences, and cause confusion when the usual tools do not completely mitigate the offensive. IPv6 could then be used to compromise the networking infrastructure used to run the dual protocols side by side, attacking the IPv4 stack through a backdoor.

IPv6 addresses can also be used for amplification attacks, including a recent DNS attack. The Internet community has recently been dedicated to plugging these holes in IPv4 DNS open resolvers, aided by the fact that the address space is scannable. The IPv6 space, however, is new and much larger. In the most recent attack, computers behind 1,900 IPv6 addresses attacked a DNS server as part of a larger army of commandeered systems, most of which used IPv4 addresses. Of the 1,900 IPv6 addresses, 400 were used by poorly configured DNS systems, producing roughly one-third of the overall attack traffic. Because DNS configuration for IPv6 is very different than that used for IPv4, DNS-based amplification attacks could become an enormous problem in the future.

On the plus side, IPv6 networks are still not ubiquitous enough for attackers to focus on and develop new attack methods specifically for the new protocol—IoT products and the botnets that target them are focused almost entirely on IPv4. But on the downside, pretty much every modern mobile device and PC has IPv6 support included and turned on as a default, so when those IPv6 attacks come, they are going to hit hard.

Automated Attacks to Targeted Attacks

The attack vectors used by cybercriminals are evolving. Over the past five years, we've witnessed a barrage of 'spray and pray' automated attacks. Attackers have built up a repertoire of automation, increasingly using artificial intelligence and machine learning, in an attempt to rapidly attack their targets. Automation has taken various forms—from the weaponisation of word documents, to phishing emails (as we've seen in Australia with fake AGL and Medicare emails making the rounds). With automated attacks, once a business realises an email contains something malicious, it can take steps to block it. This usually will include increasing security (i.e. spam filters) and improving internal security practices. As a result of increased awareness and the predictable nature of automated attacks, cybercriminals are moving towards highly targeted, manual attack methods, which will be a key trend shaping the security industry into 2019. An example of this is the SamSam ransomware, for which two men were recently indicted. Instead of using mass spamming techniques, the SamSam orchestrators (SamSammers) identified networks where there was a security hole, such as a remote access portal with a guessable password. Attackers make their way onto a network and once in, they escalate their own privileges and spread a payload laterally across the network; a sleeper cell that lays in wait until ready to begin encrypting. This manual attack method has earned its creators US$6.5 million in three years.

Malware

Most malware continues to be designed to run exclusively on Windows computers (this is not news). But what is interesting is how cybercriminals are abusing legitimate admin tools on the Windows operating system's (OS)—such as PowerShell, WMI and Windows Scripting Host—to evade detection and bring a new wave of attacks to victims. Living off the land is a simple strategy, and it's hard to detect. In recent years, protections such as disabling macros inside documents or using preview mode have blunted this technique. However, criminals are fighting back and have developed methods to encourage users to enable their attacks. As a result, the scope of what one might consider a dangerous file has expanded over the past two years to encompass a wide range of Windows file types, not all of which are executables. When used in conjunction with malicious email messages, these file types are often encased in compressed file formats, such as .zip files, and may also be password protected to further thwart automatic detection.

Malware & Breaches

IT Users surveyed in the early part of 2018 showed a growing concern over ransomware. And for good reason. According to the Verizon Data Breach Incident Report 2018, this threat has become "… the most prevalent variety of malicious code for this year's dataset."1 The Verizon report goes on to observe that ransomware is an interesting phenomenon that, when viewed through the mind of an attacker, makes perfect sense.

Fileless Attacks

Last year we saw attackers become much smarter and harder to detect. They've thrown away a lot of the tools they used to rely on, in favour of tactics that slip by traditional defences completely undetected. While this used to be the calling card of more advanced attackers, methods like PowerShell attacks are becoming more popular every day. By looking at the trends that took shape this year, there are a number of tools and tactics we expect to see attackers embrace in 2019. As a Windows scripting language, PowerShell provides unprecedented access to a machine's inner core, including unfettered access to APIs. It is inherently trusted by Windows, so any commands it executes are typically overlooked by security software. Once an attacker hijacks PowerShell (or another trusted Windows tool), complete compromise of the victim's environment is almost inevitable. Because no actual malware is used in these 'fileless' attacks, there isn't anything for antivirus programs to scan which means they bypass these controls without even trying. This makes PowerShell attacks a favoured tactic of APTs. So far, this type of attack has been favoured by Chinese and Russian nation-state actors. So, while 2017 was the year of Ransomware, 2018 was the year that sophisticated fileless and PowerShell attacks reigned supreme. Given the ease with which these attacks bypass defences, coupled with the complete pwnage once successful, this is a trend we expect to see continue well into 2019.

Mobile Malware

As internet user's transition from desktop computers and laptops to mobile and the Internet of Things (IoT), so too are cybercriminals. We're seeing that users of mobile devices are increasingly subject to malicious activity that's pushing malware apps to their phones, tablets and other devices running Android and iOS. The favoured tactic of cybercriminals is to sneak malicious apps past Google's Play Store and Apple's App Store. Other popular tactics include:

- Cryptominers can be hidden as a function inside another innocent-looking app, making it difficult for users to notice their device's processor straining under the load.
- Advertising click fraud – Like cryptomining, this is embedded inside apps that simulate users clicking ads to generate revenue. The negative for users is the same —battery and process drain—while advertisers are charged for useless clicks and the cost of online advertising is driven up.
- Supply chain compromise – Earlier this year, SophosLabs researchers discovered a legitimate app supplied as part of the stock firmware of a small

phone maker that had been ‘Trojanised’ in the supply chain, before anyone purchased the device.

Similarly, as IoT becomes more embedded in our daily lives, cybercriminals are unleashing new ways to hijack and compromise these devices. A popular method among attackers is to hijack IoT devices to use as nodes in massive botnets. These botnets are then leveraged in distributed denial-of-service (DDoS) attacks, as well as for cryptomining and network infiltration activities. Attacks such as these are difficult to detect as it’s rarely apparent that the device is affected—until something has gone wrong on the network.

Other Factors to Consider

Privileged insiders

Administrators and Maintainers will be coerced into giving up the crown jewels Soft human targets, with access to mission-critical information, will be subjected to various old-fashioned criminal techniques of coercion. Identify the organisation’s mission-critical information assets, and the individuals who own and access them. Enter into contractual confidentiality agreements, pay your key staff, watch out for signs of malcontent. Make staff aware of dangers, encourage whistle blowing – even enforce two-man rules where precious assets are at risk.

CCTV

Over the last two years there has been significant growth in the volume of attacks targeting IoT devices. It’s highly likely that the IoT target list will continue to expand to include database servers, commercial-grade routers and internet-connected CCTV systems

Distortion of the Truth

Automated Information

Automated misinformation gains instant credibility. The practice of deliberately spreading misinformation will evolve to target commercial organisations, driven by advances in artificially intelligent personas. Build scenarios covering the spread of misinformation into the organisation’s overall incident management process.

Falsified information compromises performance Attacks that compromise the integrity of an organisation’s internal information will increase in number, scale and complexity. Monitor access and changes made to sensitive information, using tools such as a Federated Identity and Access Management (FIAM) systems and Content Management Systems (CMS).

Subverted blockchains shatter trust; Blockchains will be subverted to commit fraud or launder money, shattering the trust on which they rely. This could result in abandoning the affected blockchain, along with the loss of process efficiencies. Appoint a sponsor or steering committee to consult widely and take decisions concerning the adoption and use of blockchain throughout the organisation.

Artificial Information

A headlong rush to deploy AI leads to unexpected outcomes. Use of artificial intelligence will produce outcomes that go beyond the understanding of business leaders, developers and system managers, creating new vulnerabilities. Recruit, develop and retain talent with the skills to understand and manage AI systems

Government Regulation

Surveillance

Surveillance laws expose corporate secrets. Organisations will not be able to define the security arrangements around reservoirs of data collected in bulk by communications providers. Attackers will exploit this. Collaborate across the organisation and conduct a risk assessment to understand the impact of metadata being lost by a communications provider.

GDPR and DPA

Privacy regulations will increasingly impede the monitoring of insider threats. Restrictions on individual profiling will result in a conundrum for the organisation: either lose the ability to monitor the insider threat; or defy regulations. Both will have negative consequences. Take legal advice on restrictions regarding user profiling in every jurisdiction in which the organisation operates.

Conclusion

Today's threats are not standing still. New malware types are evolving every day. The astronomical growth of often-vulnerable IoT devices has created a fertile ground for botnets of all types. Amplification attacks are as close as the next unsecured service or unapplied patch. The question has become not if you will be attacked, but when. Perhaps the best advice comes from the Verizon Data Breach Incident Report, 2018, which suggests, "Don't roll the dice. While we are not seeing the biggest and most damaging attacks on a daily basis, organisations must ensure they have retained DDoS mitigation services commensurate to your tolerance to availability loss. Verify that you have covered all of your bases from a scoping standpoint."15 Organisations often focus on defending against a single type of threat, but attacks are increasingly blending. Such blended attacks raise the importance of a holistic and comprehensive defence. For example, the combination of a WAF and DDoS mitigation system from the same vendor often provides a more seamless and comprehensive defence.

Summary

A look at the different types of threats propagating today, combined with the sheer volume of attacks, can paint a discouraging picture. Even more alarming, however, is the fact that today's threats seldom occur in isolation. A DDoS threat in one segment can divert attention from malware in another. Ransomware can be used to hasten data exfiltration. IPv6 attacks can be used to access parallel IPv4 constructs. Another consideration is that, with individual components available for sale, attackers no longer need overall computer or network expertise. Botnets can be rented from vendors and application exploits simply purchased. This allows perpetrators to concentrate on results that they desire without having to create the means to commit the crime. This is obvious from the results of Verizon’s 2018 Data Breach Incident Report, which shows that 50% of breaches were carried out by organized criminal groups, and 12% involved nation-state or state-affiliated actors. The bottom line is that for today’s enterprise, the question is not whether you will be attacked. It’s when, by what, and how badly your company’s reputation or finances will be damaged. And one thing is sure in the uncertain world of cybersecurity — the wrong time to consider defence is after the attack has occurred.

Joe Ferguson

CCP M. Inst ISP SIRA

Cyber Risk specialist

IL7 Security

www.il7security.com

For a review of DDOS protection solutions look at the excellent Forester Report embedded below.

forrester-wave-ddos-mitigation-solutio