Threat Landscape for Critical National Infrastructure

Threat Landscape 2022

October 31 2022

Microsoft case study of TTPs in a ransomware attack. The Microsoft Detection and Response Team (DART) has published a detailed technical case study of the TTPs used in an attack where the actor eventually deployed the Cuba ransomware. This study describes how the actor was able to use commodity tools to launch malicious code and gain persistence. Importantly, it also includes technical measures that organisations can use to monitor networks to detect TTPs and anomalous behaviour.

Ransomware continues to be a threat to organisations globally, as actors' techniques continue to evolve. The findings here again make the case why it's so important for organisations to take proactive action to monitor networks.

The NCSC has guidance for organisations advising how to mitigate ransomware and other malware.

Google support for Chrome browser on Windows 7 and 8/8.1 to end in early 2023

Google has announced that from February 2023 it will no longer support Chrome running on Windows 7, Windows 8/8.1 and so no updates will be released.

This is also a timely reminder that Microsoft support for Windows 7 and 8.1 ends in January 2023. Running out-of-support operating systems presents a real security threat. The NCSC has advice for organisations on keeping software up to date and managing obsolete products.

More Generally

Over the past year, the cyber security threat to the UK has evolved significantly. The threat from ransomware was ever present – and remains a major challenge to businesses and public services in the UK. This year 18 ransomware incidents required a nationally coordinated response, including attacks on a supplier to NHS 111, and a water utility company, South Staffordshire Water. The most significant threat facing citizens and small businesses continued to be from cyber-crime, such as phishing, while hacking of social media accounts remained an issue. Official figures revealed there were 2.7m cyber-related frauds in the 12 months to March 2022 in the UK

Internationally, Russia's invasion of Ukraine brought the cyber security threat into sharper focus in the UK. During the invasion, Russia sought to use offensive cyber operations to support their military campaign. However, like on the battlefield, Ukrainian authorities – assisted by the NCSC – created strong cyber defences, limiting the impact of Russian operations. Ukraine's successful defensive operations were an exemplar to network defenders across the world.

While not as prominent as Russian operations in cyberspace, the Chinese Government's cyber capabilities continued to develop. Beijing's activity has become ever more sophisticated, with the state increasingly targeting third-party technology and service supply chains, as well as exploiting software vulnerabilities. This approach shows no sign of abating, with China's technical evolution likely to be the single biggest factor affecting the UK's cyber security in the future. Evolving state threats were not the only cyber security challenges this year: the proliferation and commercial

availability of cyber capabilities continued and is likely to expand the threat to the UK. It is expected that further malicious and disruptive cyber tools will be available to a wider range of state and non-state actors and will be deployed with greater frequency and less predictability.

Threats to the global supply chain continued to be apparent this year where attackers accessed target victim organisations' networks or systems via third-party vendors or suppliers. Meanwhile, the disclosure of the Log4j vulnerability highlighted the challenges where weaknesses in IT systems are exploited to deliver successful attacks.

In our archives

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, or are setting the stage for another APT[1]. 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.

1.1.1 Disruption of Service

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. Engage with internal and external stakeholders to agree alternative methods of communication (e.g. telex, satellite, microwave).

[1] APT = Advanced Persistent Threat

1.1.2 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 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.

1.1.3 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.

1.1.4 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 attac
k method has earned its creators a whopping US$6.5 million in three years.

1.1.5 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.

1.1.6 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.

1.1.7 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.

1.1.8 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

1.1.9 Distortion of the Truth

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

1.1.10 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.

1.1.11 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.