National Cyber Security Centre
a part of GCHQ

Cyber Attacks White Paper
January 2016

Common cyber attacks: reducing the impact

Contents

Part 1: The Threat Landscape

Although computer systems can be compromised through a variety of means, the NCSC looks to understand malicious actions and the attackers that carry them out.

The risk to information and computer assets comes from a broad spectrum of threats with a broad range of capabilities. The impact (and therefore the harm) on your business will depend on the opportunities you present to an attacker (in terms of the vulnerabilities within your systems), the capabilities of the attackers to exploit them, and ultimately their motivation for attacking you.

TECHNICAL FOCUS: RISK

In cyber security terms, **risk** is the potential for a **threat** (a person or thing that is likely to cause damage) to exploit a **vulnerability** (a flaw, feature or user error) that may result in some form of negative impact.

For example, an easily guessed password to an online account takes very little technical capability to exploit. With a little more technical knowledge, attackers can also use tools that are readily available on the internet. They can also bring resources (people or money) to bear in order to discover new vulnerabilities. These attackers will go on to develop bespoke tools and techniques to exploit them; such vulnerabilities enable them to bypass the basic controls provided by schemes like Cyber Essentials. To protect against these bespoke attacks will require you to invest in a more holistic approach to security, such as that outlined in the 10 Steps to Cyber Security.

The motivation of an attacker can vary from demonstrating their technical prowess for personal kudos, financial gain, commercial advantage, political protest; through to economic or diplomatic advantage for their country.

Whilst attackers may have the capability and the motivation, they still need an opportunity to deliver a successful attack. **You have no control over their capabilities and motivations, but you can make it harder for attackers by reducing your vulnerabilities.**

WHO MIGHT BE ATTACKING YOU?

Cyber criminals interested in making money through fraud or from the sale of valuable information.

Industrial competitors and **foreign intelligence** services, interested in gaining an economic advantage for their companies or countries.

Hackers who find interfering with computer systems an enjoyable challenge.

Hacktivists who wish to attack companies for political or ideological motives.

Employees, or those who have legitimate access, either by accidental or deliberate misuse.

Commodity vs bespoke capabilities

In this paper, we are using the terms 'commodity' and 'bespoke' to characterise the capabilities attackers can employ.

Commodity capability involves tools and techniques openly available on the Internet (off-the-shelf) that are relatively simple to use. This includes tools designed for security specialists (such as system penetration testers) that can also be used by attackers as they are specifically designed to scan for publicly known vulnerabilities in operating systems and applications. Poison Ivy is a good example of a commodity tool; it is a readily available Remote Access Tool (RAT) that has been widely used for a number of years.

Bespoke capability involves tools and techniques that are developed and used for specific purposes, and thus require more specialist knowledge. This could include malicious code ('exploits') that take advantage of software vulnerabilities (or bugs) that are not yet known to vendors or anti-malware companies, often known as 'zero-day' exploits. It could also include undocumented software features, or poorly designed applications. Bespoke capabilities usually become commodity capabilities once their use has been discovered, sometimes within a few days[3]. By their very nature, the availability of bespoke tools is not advertised as once released they become a commodity.

3 'When Vulnerabilities are Exploited: the Timing of First Known Exploits for Remote Code Execution Vulnerabilities', Tim Rains, 17 June 2014, http://blogs.microsoft.com/cybertrust/2014/06/17/when-vulnerabilities-are-exploited-the-timing-of-first-known-exploits-for-remote-code-execution-vulnerabilities
'Before We Knew It: An Empirical Study of Zero-Day Attacks In The Real World', Leyla Bilge and Tudor Dumitras, CCS '12, 16-18 October 2012, http://users.ece.cmu.edu/~tdumitra/public_documents/bilge12_zero_day.pdf

Openly available commodity capabilities are effective because basic cyber security principles, such as those described in **Cyber Essentials** and **10 Steps to Cyber Security**, are not properly followed. Regardless of their technical capability and motivation, commodity tools and techniques are frequently what attackers turn to first.

In part 2 we will look in more detail at the vulnerabilities that attackers exploit using both commodity and bespoke capabilities.

Un-targeted attacks

In un-targeted attacks, attackers indiscriminately target as many devices, services or users as possible. They do not care about who the victim is as there will be a number of machines or services with vulnerabilities. To do this, they use techniques that take advantage of the openness of the Internet, which include:

- **phishing** - sending emails to large numbers of people asking for sensitive information (such as bank details) or encouraging them to visit a fake website
- **water holing** - setting up a fake website or compromising a legitimate one in order to exploit visiting users
- **ransomware** - which could include disseminating disk encrypting extortion malware
- **scanning** - attacking wide swathes of the Internet at random

Targeted attacks

In a targeted attack, your organisation is singled out because the attacker has a specific interest in **your** business, or has been paid to target **you**. The groundwork for the attack could take months so that they can find the best route to deliver their exploit directly to your systems (or users). A targeted attack is often more damaging than an un-targeted one because it has been specifically tailored to attack **your** systems, processes or personnel, in the office and sometimes at home. Targeted attacks may include:

- **spear-phishing** - sending emails to targeted individuals that could contain an attachment with malicious software, or a link that downloads malicious software
- **deploying a botnet** - to deliver a DDOS (Distributed Denial of Service) attack
- **subverting the supply chain** - to attack equipment or software being delivered to the organisation

THE INSIDER THREAT

Although this paper is focussed on threats from the Internet, insiders (anyone who has legitimate access to your systems as an employee or a contractor) should also be considered as part of a holistic security regime. They may be motivated by personal gain or redress against grievances.

An insider could simply use their normal access to compromise your information, take advantage of unlocked computers or guessable passwords. They could use social engineering techniques (fooling people in to breaking normal security procedures) to gain further accesses. They may even have the technical skills to use commodity tools and techniques to become a 'hacker within the system', with the opportunity to cause greater damage and steal information at will. In the worst case scenario, an insider could be working for an adversary who can develop bespoke tools, and introduce these deep within your organisation. Assessing which (if any) of these scenarios is likely should be a critical part of your risk assessment process.

Without appropriate training, insiders can also accidentally compromise a system or the information it holds. So make sure that particular care is taken when evaluating all aspects of the insider threat as part of your organisation's overall assessment of cyber risks, referring to external guidance where required.

In general attackers will, in the first instance, use commodity tools and techniques to probe your systems for an exploitable vulnerability.

Every organisation is a potential victim

Before investing in defences, many organisations often want concrete evidence that they are, or will be targeted, by specific threats. Unfortunately, in cyberspace it is often difficult to provide an accurate assessment of the threats that specific organisations face.

However, *every* organisation is a potential victim. All organisations have something of value that is worth something to others. If you openly demonstrate weaknesses in your approach to cyber security by failing to do the basics, you will experience some form of cyber attack.

If you openly demonstrate weaknesses in your approach to cyber security by failing to do the basics, you will experience some form of cyber attack.

As part of your risk management processes, you should be assessing whether you are likely to be the victim of a targeted or un-targeted attack; every organisation connected to the Internet should assume they will be a victim of the latter. Either way, you should implement basic security controls consistently across your organisation, and where you may be specifically targeted, ensure you have a more in-depth, holistic approach to cyber security.

Part 2: Understanding Vulnerabilities

Vulnerabilities provide the opportunities for attackers to gain access to your systems. They can occur through flaws, features or user error, and attackers will look to exploit any of them, often combining one or more, to achieve their end goal. In the context of this paper, a vulnerability is a weakness in an IT system that can be exploited by an attacker to deliver a successful attack.

Flaws

A flaw is **unintended** functionality. This may either be a result of poor design or through mistakes made during implementation. Flaws may go undetected for a significant period of time. The majority of common attacks we see today exploit these types of vulnerabilities. In the last twelve months nearly 8,000 unique and verified software vulnerabilities were disclosed in the US National Vulnerability Database (NVD)[4].

Features

A feature is **intended** functionality which can be misused by an attacker to breach a system. Features may improve the user's experience, help diagnose problems or improve management, but they can also be exploited by an attacker.

When Microsoft introduced macros into their Office suite in the late 1990s, macros soon became the vulnerability of choice with the Melissa worm in 1999 being a prime example. Macros are still exploited today; the Dridex banking Trojan that was spreading in late 2014 relies on spam to deliver Microsoft Word documents containing malicious macro code, which then downloads Dridex onto the affected system.

JavaScript, widely used in dynamic web content, continues to be used by attackers. This includes diverting the user's browser to a malicious website and silently downloading malware, and hiding malicious code to pass through basic web filtering.

User error

A computer or system that has been carefully designed and implemented can minimise the vulnerabilities of exposure to the Internet. Unfortunately, such efforts can be easily undone (for example by an inexperienced system administrator who enables vulnerable features, fails to fix a known flaw[5], or leaves default passwords unchanged).

More generally, users can be a significant source of vulnerabilities. They make mistakes, such as choosing a common or easily guessed password, or leave their laptop or mobile phone unattended. Even the most cyber aware users can be fooled into giving away their password, installing malware, or divulging information that may be useful to an attacker (such as who holds a particular role within an organisation, and their schedule). These details would allow an attacker to target and time an attack appropriately.

TECHNICAL FOCUS: VULNERABILITIES

Vulnerabilities are actively pursued and exploited by the full range of attackers. Consequently, a market has grown in software flaws, with 'zero-day' vulnerabilities (that is recently discovered vulnerabilities that are not yet publically known) fetching hundreds of thousands of pounds.

Zero-days are frequently used in bespoke attacks by the more capable and resourced attackers. Once the zero-days become publically known, reusable attacks are developed and they quickly become a commodity capability. This poses a risk to any computer or system that has not had the relevant patch applied, or updated its antivirus software.

The ability for an attacker to find and attack software flaws or subvert features depends on the nature of the software and their technical capabilities. Some target platforms are relatively simple to access, for example web applications could, by design, be capable of interacting with the Internet and may provide an opportunity for an attacker.

[4] https://nvd.nist.gov/

[5] Fixes such as applying software patches, removing detected malware and updating device configuration to address issues detected through vulnerability scanning

Part 3: Common Cyber Attacks - Stages and Patterns

Regardless of whether an attack is targeted or un-targeted, or the attacker is using commodity or bespoke tools, cyber attacks have a number of stages in common. Some of these will meet their goal whilst others may be blocked.

Stages of an attack

An attack, particularly if it is carried out by a persistent adversary, may consist of repeated stages. The attacker is effectively probing your defences for weaknesses that, if exploitable, will take them closer to their ultimate goal. Understanding these stages will help you to better defend yourself.

A number of attack models describe the stages of a cyber attack (the Cyber Kill Chain® produced by Lockheed Martin is a popular example[6]). We have adopted a simplified model in this paper that describes the four main stages present in most cyber attacks:

Stages in a cyber attack

- Survey - investigating and analysing available information about the target in order to identify potential vulnerabilities
- Delivery - getting to the point in a system where a vulnerability can be exploited
- Breach - exploiting the vulnerability/vulnerabilities to gain some form of unauthorised access
- Affect - carrying out activities within a system that achieve the attacker's goal

Survey

Attackers will use any means available to find technical, procedural or physical vulnerabilities which they can attempt to exploit.

They will use open source information such as LinkedIn and Facebook, domain name management/search services, and social media. They will employ commodity toolkits and techniques, and standard network scanning tools to collect and assess any information about your organisation's computers, security systems and personnel.

User error can also reveal information that can be used in attacks. Common errors include:

- releasing information about the organisation's network on a technical support forum
- neglecting to remove hidden properties from documents such as author, software version and file save locations

TECHNICAL FOCUS: SURVEY

The default settings of computer systems can reveal a lot of useful information about the software running on them, and how they are configured. They can broadcast a range of network protocols and communications channels that can be exploited if they aren't removed.

The attacker will point network scanning tools at your network to try and identify any of the following:

- open ports
- open services
- default settings
- vulnerable applications and operating systems
- the makes and models of your network equipment

6 The Lockheed Martin Cyber Kill Chain® can be found at www.lockheedmartin.co.uk/us/what-we-do/information-technology/cyber-security/cyber-kill-chain.html

Attackers will also use social engineering (often via social media) to exploit user naivety and goodwill to elicit further, less openly available information.

Delivery

During the delivery stage, the attacker will look to get into a position where they can exploit a vulnerability that they have identified, or they think could potentially exist. Examples include:

- attempting to access an organisation's online services
- sending an email containing a link to a malicious website or an attachment which contains malicious code
- giving an infected USB stick away at a trade fair
- creating a false website in the hope that a user will visit

The crucial decision for the attacker is to select the best delivery path for the malicious software or commands that will enable them to breach your defences. In the case of a DDOS attack, it may be sufficient for them to make multiple connections to a computer in order to prevent others from accessing it.

Breach

The harm to your business will depend on the nature of the vulnerability and the exploitation method. It may allow them to:

- make changes that affect the system's operation
- gain access to online accounts
- achieve full control of a user's computer, tablet or smartphone

Having done this, the attacker could pretend to be the victim and use their legitimate access rights to gain access to other systems and information.

Affect

Depending on their motivation, the attacker may seek to explore your systems, expand their access and establish a persistent presence (a process sometimes called 'consolidation'). Taking over a user's account usually guarantees a persistent presence. Taking over an administrator's account is an attacker's Holy Grail. With administration access to just one system, they can try to install automated scanning tools to discover more about your networks and take control of more systems. When doing this they will take great care not to trigger the system's monitoring processes and they may even disable them for a time.

TECHNICAL FOCUS: BREACH

With the great variety of potential vulnerabilities in any IT system, there is a similar diversity in the often highly technical and innovative mechanisms used to exploit them. Although attackers continue to develop novel techniques to exploit vulnerabilities, attackers are ultimately successful due to an unfixed flaw, misused feature or user error.

Some types of attack are much more obvious or easier to detect than others. DDOS attacks are often quickly noticed by system users, as they struggle to access or simply cannot use the targeted service. On the other hand, most malware is designed to be stealthy, hiding from users and detection mechanisms alike.

Determined and undetected attackers continue until they have achieved their end goals. Depending on their objectives, the activities they aim to carry out on your systems will differ, but they can include:

- retrieving information they would otherwise not be able to access, such as intellectual property or commercially sensitive information
- making changes for their own benefit, such as creating payments into a bank account they control
- disrupting normal business operation, such as overloading the organisation's internet connection so they cannot communicate externally, or deleting the whole operating system from users' computers

After achieving their objectives, the more capable attacker will exit, carefully removing any evidence of their presence. Or they could create an access route for future visits by them, or for others they have sold the access to. Equally, some attackers will want to seriously damage your system or make as much 'noise' as possible to advertise their success.

Part 4: Reducing Your Exposure to Cyber Attack

Preventing, detecting or disrupting the attack at the earliest opportunity limits the business impact and the potential for reputational damage. Once the attacker has consolidated their presence they will be more difficult to find and remove.

Breaking the attack pattern

Even though it's normally the most motivated attackers who have the persistence to carry out multiple stage attacks, they will frequently do this using commodity tools and techniques, which are cheaper and easier for them to use. So putting in place security controls and processes that can mitigate these will go some way to making your business a hard target. Equally, adopting a defence-in-depth[7] approach to mitigate risks through the full range of potential attacks will give your business more resilience to cope with attacks that use more bespoke tools and techniques.

Even though it's normally the most motivated attackers who have the persistence to carry out multiple stage attacks, they will frequently do this using commodity tools and techniques.

Reducing your exposure using essential security controls

Fortunately, there are effective and affordable ways to reduce your organisation's exposure to the more common types of cyber attack on systems that are exposed to the Internet. The following controls are contained in the **Cyber Essentials**, together with more information about how to implement them:

- boundary **firewalls and internet gateways** - establish **network perimeter defences**, particularly **web proxy**, **web filtering**, **content checking**, and **firewall policies** to detect and block executable downloads, block access to known malicious domains and prevent users' computers from communicating directly with the Internet
- **malware protection** - establish and maintain **malware** defences to detect and respond to known attack code
- **patch management** - patch known vulnerabilities with the latest version of the software, to prevent attacks which exploit software bugs
- **whitelisting and execution control** - prevent unknown software from being able to run or install itself, including AutoRun on USB and CD drives
- **secure configuration** - restrict the functionality of every device, operating system and application to the minimum needed for business to function[8]
- **password policy** - ensure that an appropriate **password policy** is in place and followed
- **user access control** - include limiting normal users' execution permissions and enforcing the principle of least privilege[9]

7 Strengthened security achieved by establishing multiple layers of security mechanisms

8 For broader guidance on secure configuration see the following publications:

Cloud Security Principles, www.gov.uk/government/collections/cloud-security-guidance
End user devices security and configuration guidance, www.gov.uk/government/collections/end-user-devices-security-guidance
Bring Your Own Device Guidance, www.gov.uk/government/collections/bring-your-own-device-guidance

9 Applying only those privileges to a user account that are essential to that user's work

If your organisation is likely to be targeted by a more technically capable attacker, give yourself greater confidence by putting in place these additional controls set out in the 10 Steps to Cyber Security:

- security monitoring - to identify any unexpected or suspicious activity
- user training education and awareness - staff should understand their role in keeping your organisation secure and report any unusual activity
- security incident management - put plans in place to deal with an attack as an effective response will reduce the impact on your business

The 10 Steps to Cyber Security sets out the features of a complete cyber risk management regime. There are many effective and comprehensive schemes and open standards that your organisation can apply to support a defence-in-depth strategy, if this approach isn't already implemented.

TECHNICAL FOCUS: CiSP

The Cyber-security Information Sharing Partnership (CiSP), part of CERT-UK, is a joint industry-government initiative to share cyber threat and vulnerability information. It does this in order to increase overall situational awareness of the cyber threat, and therefore reduce the impact of cyber threat on UK businesses.

Mitigating the stages of an attack

We'll look at each stage of an attack in turn, and highlight where the basic security controls mitigate the activities that take place.

Mitigating the survey stage

Any information which is published for open consumption should be systematically filtered before it is released to ensure that anything of value to an attacker (such as software and configuration details, the names/roles/titles of individuals and any hidden data[10]) is removed.

User training, education and awareness is important. All your users should understand how published information about your systems and operation can reveal potential vulnerabilities. They need to be aware of the risks of discussing work-related topics on social media, and the potential for them to be targeted by phishing attacks. They should also understand the risks to the business of releasing sensitive information in general conversations, unsolicited telephone calls and email recipients. The Centre for the Protection of the National Infrastructure (CPNI) have published a guide to online reconnaissance to help put into place the most effective social engineering mitigations[11].

Secure Configuration can minimise the information that Internet-facing devices disclose about their configuration and software versions, and ensures they cannot be probed for any vulnerabilities.

Mitigating the delivery stage

The delivery options available to an attacker can be significantly diminished by applying and maintaining a small number of security controls, which are even more effective when applied in combination.

Up-to-date malware protection may block malicious emails and prevent malware being downloaded from websites. Firewalls and proxy servers can block unsecure or unnecessary services and can also maintain a list of known bad websites. Equally, subscribing to a website reputation service to generate a blacklist of websites could also provide additional protection.

A technically enforced password policy will prevent users from selecting easily guessed passwords and lock accounts after a specified number of failed attempts. Additional authentication measures for access to particularly sensitive corporate or personal information should also be in place.

Secure configuration limits system functionality to the minimum needed for business operation and should be systematically applied to every device that is used to conduct business.

[10] 'Metadata' many programs automatically add metadata to files, including author, their username and the file save location

[11] 'Online reconnaissance', CPNI, May 2013, www.cpni.gov.uk/documents/publications/2013/2013007-online_reconnaissance.pdf?epslanguage=en-gb

Mitigating the breach stage

As with the delivery stage, the ability to successfully exploit known vulnerabilities can be effectively mitigated with just a few controls, which are again best deployed together.

All commodity malware depends on known and predominately patchable software flaws. Effective **patch management** of vulnerabilities ensures that patches are applied at the earliest opportunity, limiting the time your organisation is exposed to known software vulnerabilities.

Malware protection within the **internet gateway** can detect known malicious code in an imported item, such as an email. These measures should be supplemented by malware protection at key points on the internal network and on the users' computers where available. Devices within the **internet gateway** should be used to prevent unauthorised access to critical services or inherently unsecure services that may be required internally by your organisation. Equally, the **gateway** should be able to detect any unauthorised inbound or outbound connections.

Well-implemented and maintained **user access controls** will restrict the applications, privileges and data that users can access. **Secure configuration** can remove unnecessary software and default user accounts. It can also ensure that default passwords are changed, and any automatic features that could immediately activate malware (such as AutoRun for media drives) are turned off.

User training, education and awareness are extremely valuable to reduce the likelihood of 'social engineering' being successful. However, with the pressures of work and the sheer volume of communications, you cannot rely on this as a control to mitigate even a commodity attack.

Finally, critical to actually detecting a breach is the capability to **monitor** all network activity and to analyse it to identify any malicious or unusual activity.

Mitigating the affect stage

If all the measures for the survey, delivery and breach stages are consistently in place, the majority of attacks using commodity capability are likely to be unsuccessful. However, if your adversary is able to use bespoke capabilities then you have to assume that they will evade them and get into your systems. Ideally, you should have a good understanding of what constitutes 'normal' activity on your network, and effective security monitoring should be capable of identifying any unusual activity.

Once a technically capable and motivated attacker has achieved full access to your systems it can be much harder to detect their actions and eradicate their presence. This is where a full defence-in-depth strategy can be beneficial.

I've been attacked, what do I do?

There is no such thing as 100% security and your organisation will probably experience some form of cyber attack at some time. Having an effective **security incident response plan** can help to reduce the impact of the attack, clean up the affected systems and get the business back up and running within a short time. Where relevant, you should also consider the Cyber Security Incident Response services provided by the NCSC.

Closing word: raising your cyber defences

The Internet can be a hostile environment. The threat of attack is ever present as new vulnerabilities are released and commodity tools are produced to exploit them. **Doing nothing is no longer an option; protect your organisation and your reputation by establishing some basic cyber defences to ensure that your name is not added to the growing list of victims.**

Case Studies

On a daily basis, we frequently see computer systems - and the information stored on them - being compromised by malicious attackers. Although the motivations may vary, they nearly always use commodity tools and techniques at some point.

The following three case studies demonstrate how effective these attacks can be to gain access to organisations and, conversely, how widely accepted and cost-effective cyber security controls can disrupt the different stages in the attack model we discussed earlier.

- In the first two case studies, the attackers added malicious code to legitimate websites that staff from the target companies regularly visited. This code compromised their computers, giving the attackers access to the companies' systems.
- The final case study is an example of a single-staged attack that compromised the computer of a system administrator.

All of the mitigations listed in these case studies are covered in detail in the Cyber Essentials Scheme and the 10 Steps to Cyber Security. To reduce the risk of commodity and bespoke attacks on your business, fully implement a comprehensive suite of cyber security controls.

Case study 1: Espionage campaign against the UK energy sector

Attackers used a technique known as a 'watering hole' attack to distribute malware into businesses working in the UK energy sector. The attackers added scripts to legitimate websites frequented by energy sector staff. Many of the websites were managed by the same web design company. Visitors' browsers were automatically and surreptitiously redirected to download malware from an attacker-owned server.

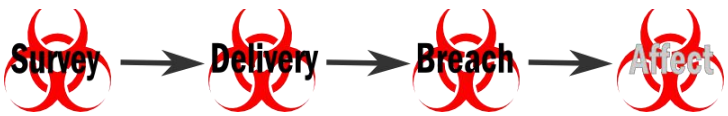
The malware targeted known and patchable vulnerabilities in Java, older internet browsers, and all but the most recent versions of Microsoft Windows. The malware harvested visitors' credentials and computer system information, and sent this information back to the controllers via attacker-owned domains.

How it happened: the technical details

In the **survey stage**, the attackers discovered that a single web design company hosted a number of energy sector businesses' websites. Although we can't say for sure how the attacker **delivered** the attack to breach the site, they may have infiltrated the web design company's networks by masquerading as a legitimate user with credentials stolen through successful spear-phishing, or by exploiting an unpatched vulnerability on the web server.

The attacker compromised the web server and then added code[12] which caused their own website to be loaded whenever the legitimate website was visited. The **delivery stage** then involved the attacker's website delivering the malicious code to the victims' computers. The unpatched browsers were **breached** through known software flaws in Java and common internet browsers.

The attacker's website installed a Remote Access Tool (RAT) on the visitor's computer, disguised as a common type of web application script. The malware then started communicating with the attacker-owned domains by sending 'beacons' to show it was active and to request commands from the attackers. The malware was designed to capture system information, user keystrokes and clipboard contents to enable the attackers to consolidate their position as they moved towards **affecting** their target. However, **security monitoring** of network activity detected command and control messages from malware on the infected computers, and in this case the attack was broken before it could affect the targeted businesses.



We believe that these 'watering hole' attacks were part of a continuing espionage campaign against the UK energy sector.

[12] An 'iframe' was inserted to point to malicious content

Capabilities, vulnerabilities and mitigations

The attackers used a number of commodity techniques to compromise their targets within the energy sector. They probably gained access to the legitimate websites using automated scanning tools and exploit kits to identify and exploit unpatched vulnerabilities, or used social engineering to take advantage of poor user training and awareness. The script hosted on the attacker's website exploited applications with known software vulnerabilities to install a RAT.

Whilst the attack was spotted by **security monitoring**, this control is not 100% effective, as it depends heavily on technology and skills. If the appropriate essential controls had been in place, this attack would not have been successful. However, that's not to say they wouldn't have kept on trying by using different techniques.

The most effective mitigations against this attack (both at the website and within the victim organisation) would have been:

- **network perimeter defences** - deploying a **web proxy**, **web filtering**, **content checking**, and **firewall policies** could have prevented executable downloads and access to known malicious domains on the Internet
- **malware protection** defences - might have detected the commodity attack code used to exploit the victims browser
- **patching** the known software flaws - would have prevented the script from being successful and the malware from running
- **whitelisting and execution control** - would have prevented any unknown software from being able to run or install itself
- **user access control** - could have restricted the malware's capabilities
- **security monitoring** - in this case did identify the suspicious activity

Case study 2: Hundreds of computers infected by remote access malware

This widespread compromise of a large UK company's internal network originated from an exploit hosted on their externally-managed corporate website. This was achieved as a result of poor security practices by the website provider. The attackers used a commonly available RAT to gain information about the internal network and control a number of computers. The widespread malware infection took extensive effort to eradicate and remediate.

How it happened: the technical details

As part of their **survey** of the victim's network and services, attackers discovered that the corporate website was hosted by a service provider, and it contained a known vulnerability. In the **survey** stage of the attack on the service provider, the attackers exploited this vulnerability to add a specialised exploit **delivery** script to the corporate website.

The script compared the IP addresses of the website's visitors against the IP range used by the company. It then infected a number of computers within the company, taking advantage of a known software flaw, to download malware to the visitor's computer within a directory that allowed file execution.

Over 300 computers were infected during the **delivery** stage with remote access malware. The malware then beaconed and delivered network information to attacker-owned domains. The attackers were eventually detected early in the **affect** stage. By this time they had installed further tools and were consolidating their position, carrying out network enumeration and identifying high value users.

Whilst the compromise was successful, it was detected through network **security monitoring**, and a well-defined **incident response** plan made it possible to investigate the incident using system and network logs, plus forensic examinations of many computers.

To eradicate the discovered infection it was necessary, at great cost, to return the computers to a known good state. Further investigation was also required to identify any further malware that could be used to retain network access. To prevent further attacks through the same route, the contract terms with the website provider needed to be renegotiated, to ensure they had similar security standards to the targeted organisation.

Capabilities, vulnerabilities and mitigations

The attackers used a combination of automated scanning tools, exploit kits and technology-specific attacks to compromise the organisation. They took advantage of a known software flaw and the trust relationship between the company and its supplier.

The intensive and costly investigation and remediation of the compromise could have been averted by more effective implementation of the following cyber security controls:

- **patching** - the corporate website would have not been compromised, nor would the malware download script have succeeded, had patching on both the web server and users' computers been up to date
- **network perimeter defences** - the malware could have been prevented from being downloaded and the command and control might not have succeeded with the use of two-way **web filtering**, **content checking** and **firewall policies** (as part of the **internet gateway** structure)
- **whitelisting and execution control** - unauthorised executables such as the exploration tools would have been unable to run if the company's corporate computers were subject to whitelisting and execution control (this could also prevent applications from being able to run from the temporary or personal profile folders)
- **security monitoring** - may have detected the compromise at an earlier stage

Case study 3: Spear-phishing attack targets system administrator

A system administrator within a high profile UK organisation was successfully spear-phished and unknowingly installed a RAT. Taking advantage of the user's privileged permissions, the attackers were able to exfiltrate[13] information about the network and details for multiple business-critical systems.

Fortunately, the compromise was restricted to one computer, and it was detected and effectively investigated as appropriate security monitoring and logging were in place. Identifying and mitigating the lost information impacted the availability of the system to the business and required extensive support from external forensic and technical architecture specialists.

How it happened: the technical details

The attackers identified the system administrator and their personal subjects of interest. They crafted and **delivered** a socially-engineered email to the administrator's personal email address. Accessing personal webmail from the admin computer, the administrator read the phishing email and downloaded a Trojanised document from a file sharing service containing the first stage malware.

When the Trojanised file was opened, the user was prompted to run an executable which then **breached** the defences and installed the first stage malware onto the system. The attacker exploited poor security awareness by repeatedly requesting approval to run until the administrator finally clicked 'OK'. Unpacking itself silently into a temporary folder, this first stage malware hid itself as a legitimate file and changed the system to ensure it continued to run between reboots of the computer. Once installed, it started communicating with attacker-controlled domains.

[13] The unauthorised transfer of data from a computer

After a number of days, the initial malware downloaded a second stage executable (the RAT) and a configuration file. To discover more about the victim organisation, the attackers configured the malware to exfiltrate captured screenshots. Data was covertly delivered for nearly a week until the transfers were detected. The domains were then blocked and the machine was disconnected from the network for forensic analysis.

The compromise was detected before any significant damage could be done. However, the investigation and clean-up operation required the assistance of industry experts and disrupted the day-to-day operation of the organisation.

Capabilities, vulnerabilities and mitigations

The information to identify the system administrator and topics of interest to socially engineer the spear-phish was likely to have been derived from surveying publically available information. The clean-up operation could have been averted by more effective implementation of the following cyber security controls:

- user training education and awareness - would have ensured staff understood how personal information can be openly accessed, and made them suspicious of unsolicited email with unexpected attachments and being asked to run executable files
- user access controls - enforcing these on the basis of least privilege, for high risk activities (such as web browsing), could help to protect privileged accounts; allowing completely open browsing from the admin computer was the critical security weakness
- network perimeter defences - the Trojan and the delivery stage executable should have been detected and blocked by firewall policies, a filtering web proxy or corporate malware protection software, none of which were implemented on the system administration computer
- secure configuration - would have prevented such malware from being able to run

Disclaimer

This document is not intended to be an exhaustive guide to potential cyber threats, is not tailored to individual needs and is not a replacement for specialist advice. Users should ensure they take appropriate specialist advice where necessary.

This document is provided without any warranty or representation of any kind whether express or implied. The government departments involved in the production of this document cannot therefore accept any liability whatsoever for any loss or damage suffered or costs incurred by any person arising from the use of this document.

Findings and recommendations in this document have not been provided with the intention of avoiding all risks and following the recommendations will not remove all such risks. Ownership of information risks remains with the relevant system owner at all times.