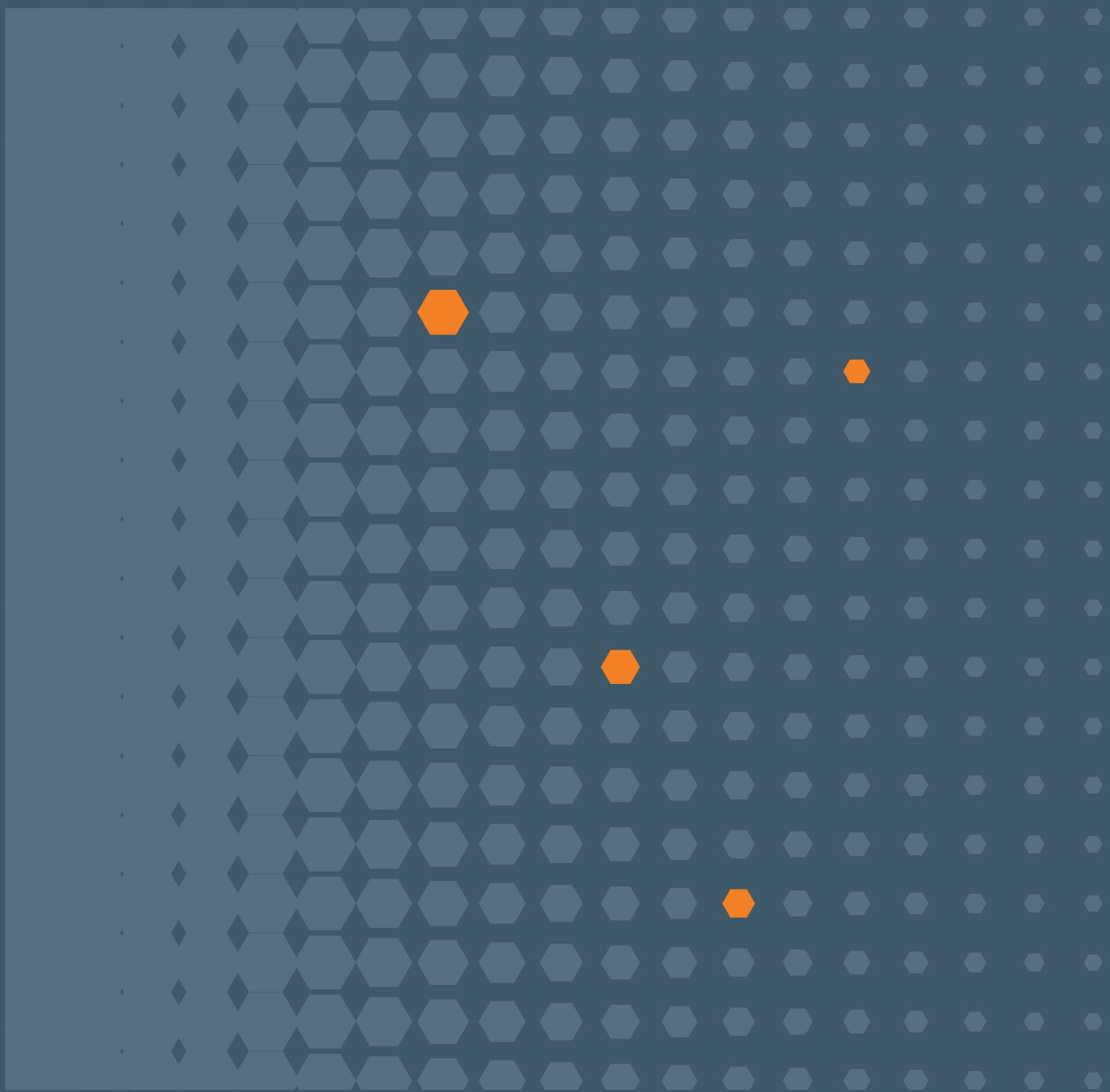
MWR INFOSECURITY

CPNI
Centre for the Protection of National Infrastructure

Detecting and Deterring Data Exfiltration

Executive Briefing Paper

February 2014



There are two disturbing facts that every major organisation needs to accept. First, that it almost certainly possesses commercially sensitive information which – if it fell into the wrong hands – could prove deeply damaging to the future of the enterprise. And secondly, that a sophisticated cyber attack targeting that data is almost certain to succeed.

MWR would like to acknowledge the help and support of CPNI in researching this topic and producing the accompanying products.

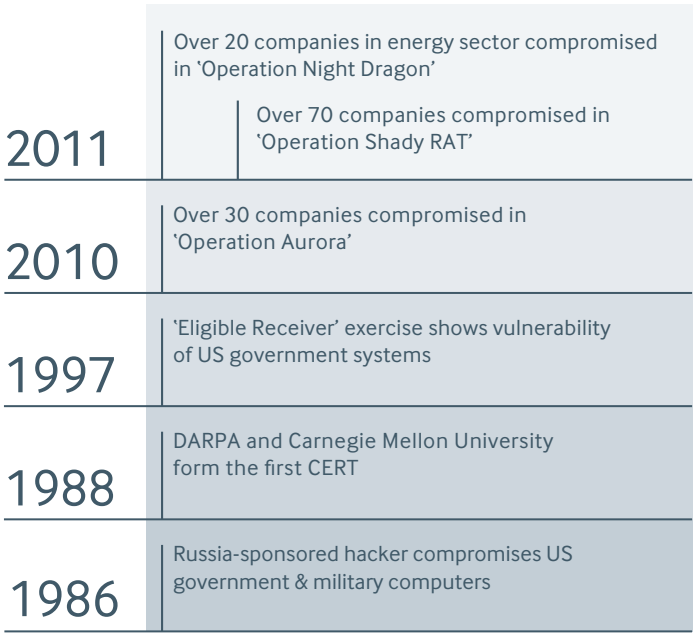
Introduction

In today's world, an organisation's digital resources are likely to be among its most sensitive and valuable assets. If a competitor were to obtain details of research and development, financial information, business processes, or intended developments and acquisitions, it could prove commercially disastrous. Hence foreign nations are investing huge amounts in state-supported cyber attacks to obtain these assets for use by organisations within their own countries.

The attacks are almost always successful. Modern organisations are so large, diverse and complicated that they are frequently unaware of what sensitive documents they possess, let alone how to defend them appropriately. Furthermore, an organisation's network perimeters will be highly porous and susceptible to attack via a host of new technologies, such as remote access, cloud services, home working, partnerships, and so on. The internal networks of modern organisations are also complex and interlinked, having grown from principles of usability rather than security, which means that it can prove extremely difficult to detect attackers once they are within the network. This is partly because detection methods often focus on spotting 'bad' patterns of behaviour, so that attackers can avoid detection simply by restricting themselves to 'good' patterns – such as accessing the CEO's email from the CEO's own laptop.

Data can have real value to attackers, potentially in the region of millions or even billions of pounds where intellectual property and negotiation positions are concerned. Attacker motivation and resourcing, combined with modern networks that are highly complex and porous, mean that it is simply not possible to guarantee the prevention of data exfiltration. If necessary, attackers can spend years slowly mapping out an organisation, observing legitimate behaviour to avoid tripping defences and gradually working towards their objectives. If they come up against defences, the attackers can either learn to bypass the controls directly, or compromise the company that produces a control in order to bypass it.

Timeline of notable events in state-sponsored hacking

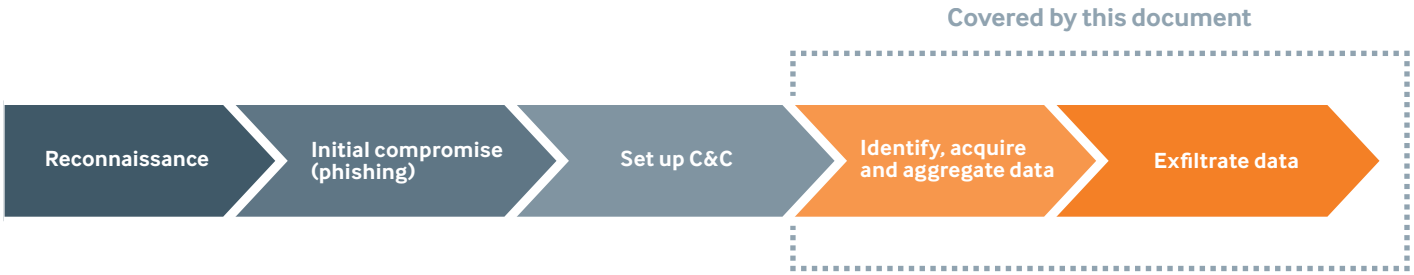


However, organisations can significantly increase the number of opportunities they have to detect and repel attackers. In so doing, they can escalate the cost and complexity for the attacker, reduce the potential business impact on themselves, and even develop advanced strategies that will deter the attacker from targeting them in future.

This executive briefing paper gives a high-level overview of a typical attack (see section 'Anatomy of a Typical Attack') and then discusses the decisions that need to be taken at the top of an organisation (section 'Organisational Decisions'). The key points of the detailed white paper, '**Detecting and Deterring Data Exfiltration: A Guide for Implementers'**, are then summarised (section 'Key Points').

Anatomy of a Typical Attack

Phases of an attack that seeks to acquire data



Attacks typically break down into several phases and some attackers are known to have entirely separate teams to deal with each phase, before handing over to the next team. In a typical attack, an organisation will first be researched and investigated to identify specific individuals to target and the relevant technologies in use. Those individuals will then be targeted with client-side attacks that might be delivered by spear phishing or watering holes (where websites regularly visited by targeted individuals are compromised – and infected with malware for targets to download). Once the targeted individuals have been compromised in this way, attackers will typically set up remote access / command and control malware (C&C) from which to conduct the rest of the attack.

Now in the internal network, the attackers will move horizontally or vertically through the network to gain access to the information they seek. Once they have accessed the data, attackers will frequently collate the information within the network before, finally, they exfiltrate the full set of data.

This document covers the stages after initial compromise and the C&C has been set up. As such, it covers a highly uncomfortable but altogether too common scenario, in which the attackers have already compromised the organisation's perimeter and are now obtaining the targeted information. In many cases, attackers will remain resident in an organisation's network for years, continually acquiring and exfiltrating new data as it becomes available.

Organisational Decisions

Organisations face a significant challenge in responding to well-resourced and strongly motivated attackers. It has been repeatedly shown that such attackers are able to find the cracks in almost any armour – and simply bypass, or even compromise, well-implemented controls.

To stand a realistic chance of detecting and deterring data exfiltration, organisations first need to understand the value of the information they possess; and then to implement a defence-in-depth approach to protecting that data. It is likely that this will require some fundamental changes – in areas ranging from staff culture to network layouts – and those changes will not be easy. They will be even harder if the changes are not driven from the top, as staff will want to know that what is happening is crucial to the future success of the organisation and has backing from the very highest levels.

Many of the organisational changes necessary to protect your organisation's data will prove costly. Expenditure will typically be required for equipment, reconfigurations, redesign and – crucially – skilled defensive staff. Traditionally, this budget has been thought hard to justify, but organisations are advised to consider the financial effect of competitors obtaining bargaining positions, future strategy, intended acquisitions, or details of key products and on-going R&D. Another worthwhile consideration is that a robustly implemented defensive programme can limit exposure to financial penalties such as fines for breaches of data protection regulations, as demonstrating the true extent of a breach will avoid the need to pay maximum fines based on a worst-case scenario. Furthermore, there is increasingly a marketable value to being demonstrably secure.

Regardless of the reasons most applicable to a specific organisation, senior executives are strongly encouraged to allocate a budget sufficient for robust defence; a budget that will help to counter the increasing resources of well-funded attackers.

It is also recommended that the Information Security department becomes a proactive and empowered group, with the remit and budget to take the necessary steps to detect and deter attackers. This might mean creating a new department, or moving an old one, as experience shows that only when Information Security emerges from the shadow of the Information Technology department, and is aware of its distinct role in protecting the organisation, can it effectively tackle the threats of modern-day attacks.

Most organisations will find that staff culture needs to adapt to the new defensive programme. For example, staff in key positions might find that the changes required to protect the organisation's data are restrictive, and hence it's important that they buy into those changes. Meanwhile, staff at all levels will need to become more security-aware, and accept that their role affects the security of the organisation's critical data.

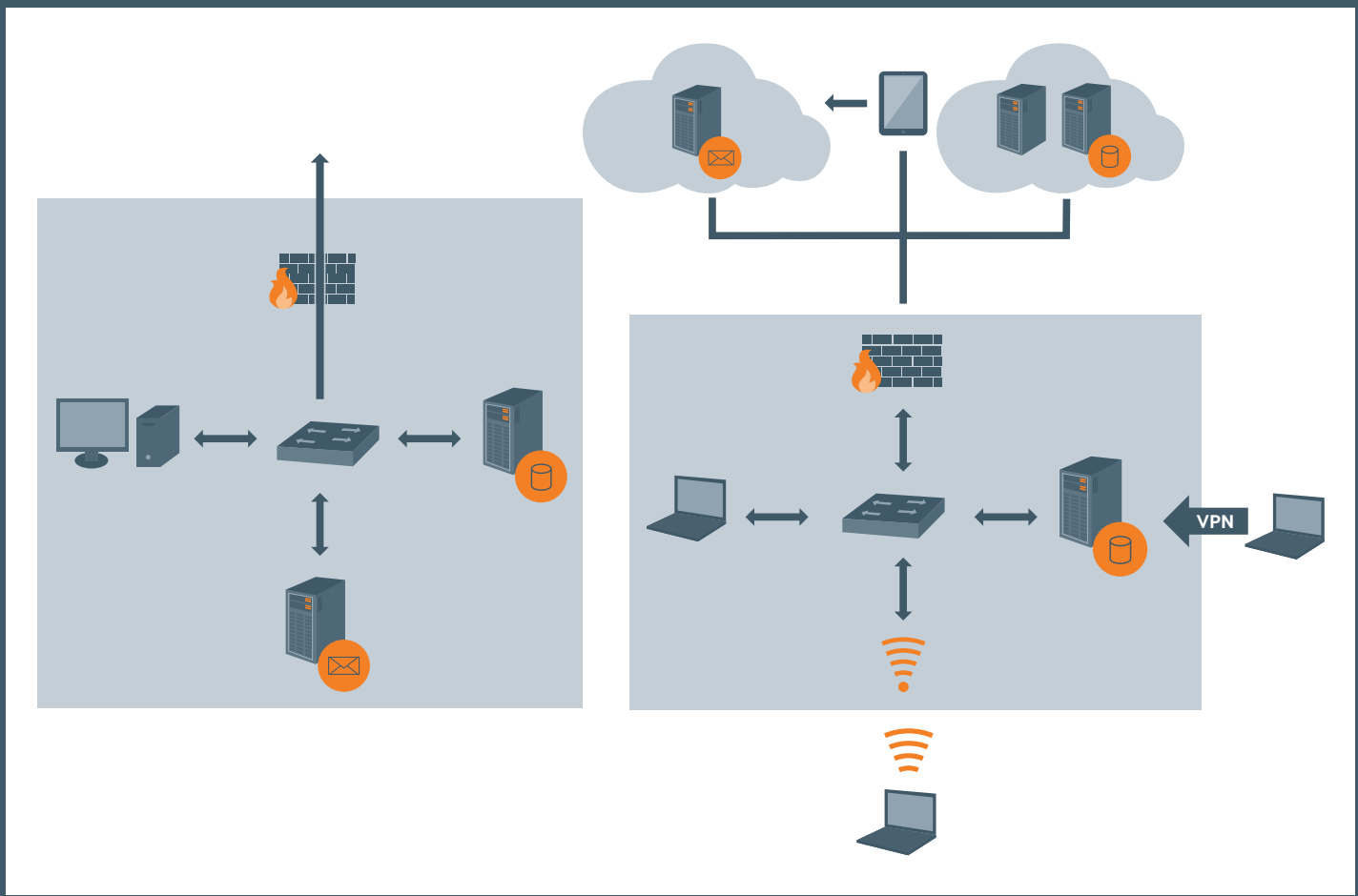
However, despite the challenges, there can be real rewards. By raising the bar for attackers, organisations can increase the effort and resource demanded from an attacker, and this in itself helps to discourage future attacks; by detecting attackers sooner, organisations can reduce the business impact of the attack; and by having a well-implemented and adaptive defence, organisations can help to ensure that the attacker has only to trip a single defence for the organisation to respond.

Key Points for Detecting and Deterring Data Exfiltration

CURRENT METHODS

- Attackers rarely need to use covert methods as few organisations have effective defences
- Attackers use common protocols and even popular third-party cloud websites, which can often go unnoticed in a busy network
- Data loss prevention tools can avert accidental loss, but attackers are able to bypass such technologies to exfiltrate data

Traditional networks had defined perimeters and services contained within that perimeter.
Modern networks are complex and porous, with cloud services, mobile workers, smart phones, and so on



FUTURE METHODS

- If organisations start to implement controls that prevent trivial exfiltration, attackers will need to improve their tactics
- Businesses are likely to dissolve perimeters further with cloud services, managed service products and remote working. Attackers are likely to take advantage in cases where data exists outside the perimeter
- If necessary, attackers can call upon advanced methods, including data hidden in innocuous protocols or even exfiltration channels that bypass the perimeter defences entirely

INCREASING AN ORGANISATION'S RESILIENCE

- Individual controls will not prevent advanced or well-motivated attackers. Instead, organisations need to focus on increasing the opportunities to detect an attacker
- Organisations are advised to understand the true cost of data exfiltration, such as foreign competitors learning intimate strategy or product details
- Organisations must assume that attacks cannot be entirely prevented, and they should instead focus on detecting attacks. However, it is also necessary to accept that detection, too, will sometimes fail, and hence a strategy for investigating a breach, once notified, should be implemented

INFORMATION CLASSIFICATION

- Many organisations will not know what sensitive information they possess, and where it is kept
- A key first step is therefore to understand what data exists within an organisation and how sensitive it might be
- Organisations are advised to assign protective markings to information, to guide how the information is handled and what levels of protection are required

LOGGING

- Logging is the foundation of a number of other controls and provides data with which to perform forensic investigations
- Forensic investigations supported by robust logging can help an organisation to understand what was stolen, and potentially how
- Organisations are advised to design a centralised logging policy, and agree budget both to implement the policy and maintain it as the organisation grows
- To derive the most value from logs, and to detect attackers currently or recently in the network, requires substantial skill and experience

BUSINESS CULTURE

- To tackle data exfiltration effectively requires a broad, defence-in-depth plan that must be driven from the top
- Organisations are encouraged to ensure that the budget and drive exists to complete a defensive programme, and that care is taken not to place too much reliance on individual security products
- Many organisations will need to change their internal culture to one that is more security-aware

SEGREGATION OF NETWORKS

- Commonly, most parts of an organisation's networks are accessible from almost anywhere
- By dividing up the network and allowing only legitimate connections, attackers are forced to take particular routes that can be monitored
- Highly sensitive information can be put on entirely separate networks that do not connect to the internet or wider corporate network

SEGREGATION OF INFORMATION

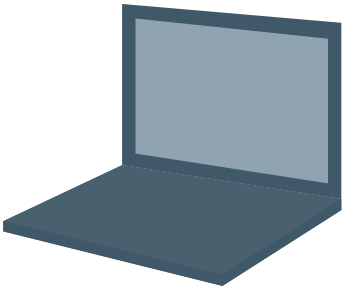
- Attackers often abuse legitimate access to information
- Once classified, sensitive information can be segregated, with access granted to the minimum number of people possible, while still allowing the business to function normally
- It is also possible to segregate understanding, so that staff are able to work on data without understanding its context. This can help to reduce the number of necessary controls on that data, and hence the cost of protecting it

HOST HARDENING

- Attackers often take advantage of weaknesses in personal computer security
- A programme of ensuring that computers used in the organisation are as secure as possible will reduce the actions open to an attacker
- Hardening desktop computers can also provide new opportunities to log and detect attackers

Bluetooth: Attacker can exfiltrate data to nearby devices under their control

3G (built-in or dongle): Attacker can make connections that will bypass internal security controls



Wi-Fi: Attacker can cause connection or creation of networks to exfiltrate data, bypassing any firewalls or proxies

Speaker / microphone: Highly advanced attackers can exfiltrate data to nearby devices

MOVEMENT OF DATA INTERNALLY

- Attackers will often aggregate data on a 'quiet' computer in the network
- Organisations should actively look for signs of an attacker attempting to locate, acquire and aggregate data
- It is often easier to detect an attacker's actions within the internal network than to leave it till they attempt to exfiltrate the data

MOVEMENT OF DATA EXTERNALLY

- The final opportunity to detect an attacker is as they exfiltrate data from the network
- It can be difficult to detect exfiltration as attackers can hide in the noise of a modern network
- Organisations are advised to look for indicators of exfiltration that are harder for attackers to hide

HONEYPOTS

- Honeypots are fake resources (documents, computers or credentials) that are planted by an organisation in the hope that they will be targeted by attackers
- This approach can be highly effective in detecting attacks, but can require significant effort if the honeypots are to be convincing

ADAPTIVE DEFENCE

- Adaptive defence ensures that lessons are learnt from an attack, and opportunities to harden the organisation are rapidly identified
- Misinformation is one of the few tactics that can discourage future attacks
- Collaborating with other organisations at risk of attack allows the sharing of information – such as attacker tactics and indicators

Summary

Modern organisations are highly complex and have valuable digital assets that they need to use in day-to-day business rather than simply store securely. Modern attackers are motivated and can be well resourced by groups that understand the value of the assets they hope to compromise. This combination means that complete prevention of data compromise and exfiltration by advanced attackers simply isn't possible. Instead, organisations must focus on detecting and deterring such attacks, which is still a significant challenge.

With no magic bullets available, an organisation's best option for detecting and deterring data exfiltration by advanced attackers is a comprehensive defence-in-depth strategy. The strategy will not only need to be implemented but also maintained, and must be able to adapt to new business behaviours and changing threats. Such a strategy will require significant resource and is likely to touch much of an organisation's functioning. It therefore needs to be driven from the highest levels of the business.

A defensive programme can be expensive and, in order to justify the cost, an organisation needs to understand what might be lost without it. It also does no harm for senior personnel to remind themselves of this threat occasionally – if only to ensure that on-going defensive measures are not the first thing to be cut when the squeeze comes.

However, if properly implemented, such a strategy will be able to push up the cost to the attacker while simultaneously decreasing the business impact on the organisation. A coherent strategy can work to flip the defender's dilemma (the idea that an attacker only needs to be successful once) into the attacker's dilemma (where a single detection can alert the defender to their presence).

Contributors:

David Chismon

Martyn Ruks

Matteo Michelini

Alec Waters - Dataline Software

MWR InfoSecurity (Head Office)
Matrix House, Basing View
Basingstoke RG21 4DZ
T: +44 (0)1256 300920
F: +44 (0)1256 323575

MWR InfoSecurity (London)
77 Weston Street
London SE1 3RS

MWR InfoSecurity (Manchester)
113-115 Portland Street
Manchester M1 6DW

MWR InfoSecurity (South Africa)
11 Autumn Street, Rivonia
Gauteng, 2128, South Africa
T: +27 (0)10 100 3157
F: +27 (0)10 100 3160

www.mwrinfosecurity.com
labs.mwrinfosecurity.com

Follow us on Twitter:
@mwrinfosecurity
@mwrlabs

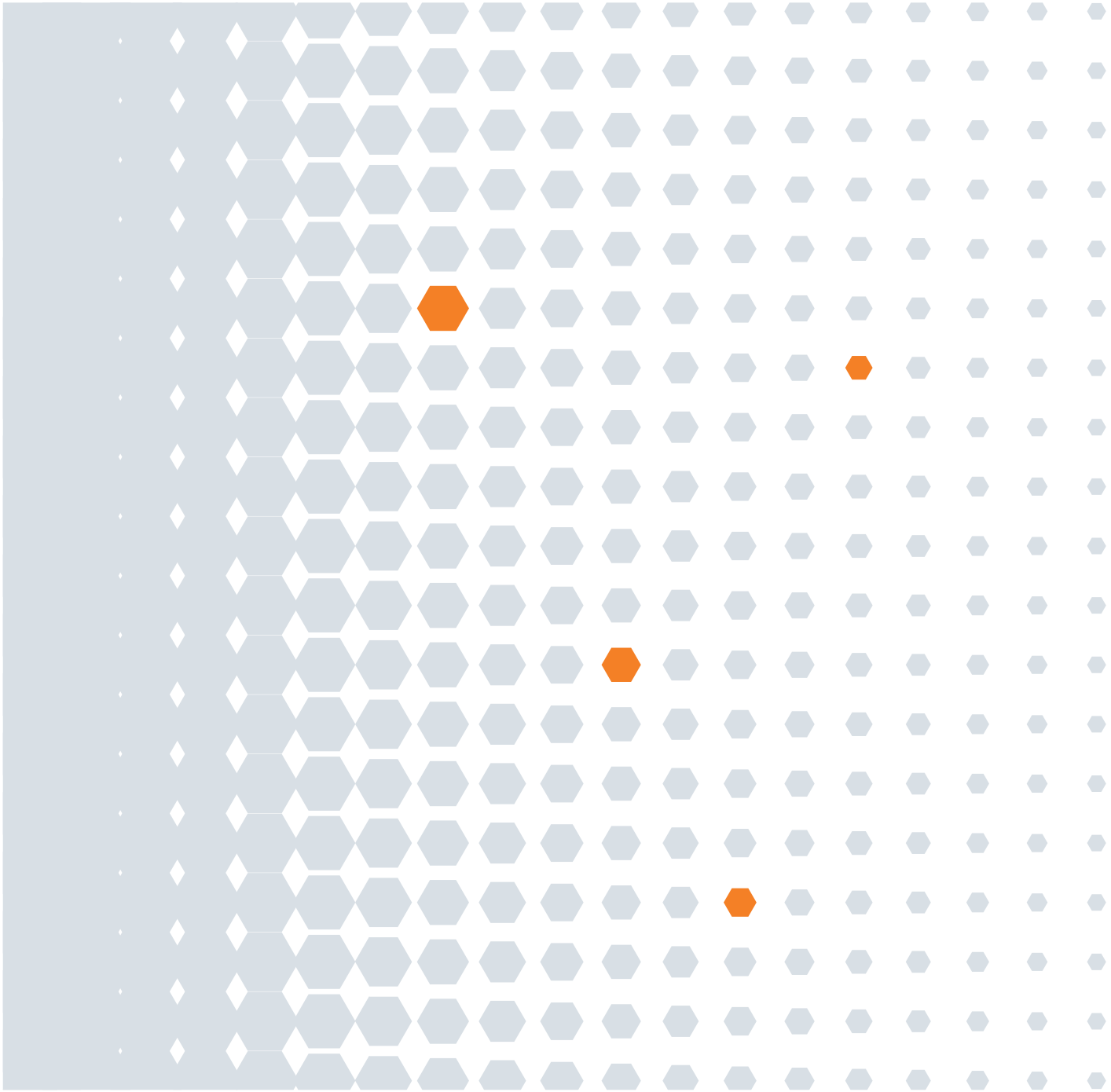
MWR INFOSECURITY

CPNI
Centre for the Protection of National Infrastructure

Detecting and Deterring Data Exfiltration

Guide for Implementers

February 2014



MWR would like to acknowledge the help and
support of CPNI in researching this topic
and producing the accompanying products.

Contents

Introduction

In today's world, an organisation's digital resources are likely to be among its most sensitive and valuable assets. If a competitor were to obtain details of research and development, financial information, business processes, or intended developments and acquisitions, it could prove commercially disastrous. Hence foreign nations are investing huge amounts in state-supported cyber attacks to obtain these assets for use by organisations within their own countries.

The attacks are almost always successful. Modern organisations are so large, diverse and complicated that they are frequently unaware of what sensitive documents they possess, let alone how to defend them appropriately. Furthermore, an organisation's network perimeters will be highly porous and susceptible to attack via a host of new technologies, such as remote access, cloud services, home working, partnerships, and so on. The internal networks of modern organisations are also complex and interlinked, having grown from principles of usability rather than security, which means that it can prove extremely difficult to detect attackers once they are within the network. This is partly because detection methods often focus on spotting 'bad' patterns of behaviour, so that attackers can avoid detection simply by restricting themselves to 'good' patterns – such as accessing the CEO's email from the CEO's own laptop.

Data can have real value to attackers, potentially in the region of millions or even billions of pounds where intellectual property and negotiation positions are concerned. Attacker motivation and resourcing, combined with modern networks that are highly complex and porous, mean that it is simply not possible to guarantee the prevention of data exfiltration. If necessary, attackers can spend years slowly mapping out an organisation, observing legitimate behaviour to avoid tripping defences and gradually working towards their objectives. If they come up against defences, the attackers can either learn to bypass the controls directly, or compromise the company that produces a control in order to bypass it[1].

However, organisations can significantly increase the number of opportunities they have to detect and repel attackers. In so doing, they can escalate the cost and complexity for the attacker, reduce the potential business impact on themselves, and even develop advanced strategies that will deter the attacker from targeting them in future.

This white paper gives a high-level overview of a typical attack (see section on 'Anatomy of a Typical Attack') and then covers the current tactics used by attackers to acquire and exfiltrate data (section 'Current Exfiltration Tactics'). Current business trends and attacker trends are then extrapolated to predict the likely future developments in exfiltration strategy (section 'Future Exfiltration Tactics'). The majority of the white paper, however, focuses on the steps that will give organisations the best chance of detecting and deterring data exfiltration (section 'Increasing Organisational Resilience'), before concluding with a summary. The appendices contain a glossary of terms, recommended further reading, and a list of 'quick wins' that can increase an organisation's resilience while a more comprehensive defence programme is being developed.

The advice given in this document is not intended to be a complete and thorough guide to all the steps needed to build a defensive programme, as each subsection of 'Increasing Organisational Resilience' is a broad topic in its own right. Instead, this document aims to highlight the areas that an organisation needs to consider, and some of the aspects to be aware of when tying them together into a defensive programme.

Timeline of notable events in state-sponsored hacking

2011	Over 20 companies in energy sector compromised in 'Operation Night Dragon' Over 70 companies compromised in 'Operation Shady RAT'
2010	Over 30 companies compromised in 'Operation Aurora'
1997	'Eligible Receiver' exercise shows vulnerability of US government systems
1988	DARPA and Carnegie Mellon University form the first CERT
1986	Russia-sponsored hacker compromises US government & military computers

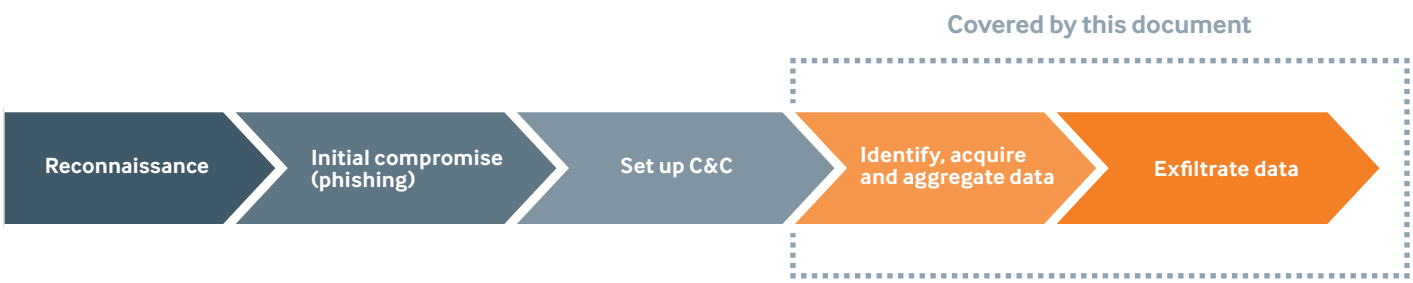
Anatomy of a Typical Attack

Attacks typically break down into several phases and some attackers are known to have entirely separate teams to deal with each phase, before handing over to the next team. In a typical attack, an organisation will first be researched and investigated to identify specific individuals to target and the relevant technologies in use. Those individuals will then be targeted with client-side attacks that might be delivered by spear phishing or watering holes (where websites regularly visited by targeted individuals are compromised – and infected with malware for targets to download). Once the targeted individuals have been compromised in this way, attackers will typically set up remote access / command and control malware (C&C) from which to conduct the rest of the attack.

Now in the internal network, the attackers will move horizontally or vertically through the network to gain access to the information they seek. Once they have accessed the data, attackers will frequently collate the information within the network before, finally, they exfiltrate the full set of data.

This document covers the stages after initial compromise and the C&C has been set up. As such, it covers a highly uncomfortable but altogether too common scenario, in which the attackers have already compromised the organisation's perimeter and are now obtaining the targeted information. In many cases, attackers will remain resident in an organisation's network for years, continually acquiring and exfiltrating new data as it becomes available.

Phases of an attack that seeks to acquire data



Current Exfiltration Tactics

Different Attackers, Different Tactics

A number of groups are known to exist that will target UK industry and government bodies in an attempt to obtain sensitive data. The motivations and tactics of these groups can be varied: some are highly targeted and careful to avoid detection for fear of political fallout, while others are less wary and adopt noisy, low-skilled attacks but in a volume that makes them highly successful at acquiring terabytes of critical data. Although attributing attacks is generally difficult, the tactics can sometimes be distinctive enough to make it possible to identify the group behind the attack. On occasion, experienced analysts are able to identify not just the group, but the subgroup or even the individual perpetrating the attack[2].

The distinctive tactics will often depend on the target under attack – for example, whether it's a specific company or an entire industry sector. Differences in tactics can be observed in the nature of the first entry into the system, the C&C channel (common RAT or custom-written) and, once in the network, the tools used to achieve the objectives. Another key distinguishing tactic is the type of data targeted: whether it is data related to a specific project or current negotiation, or whether the attacker's net is cast wide in an attempt to gain information about the whole of an organisation's key business.

The level of expertise and resources can vary as well. Some attackers have very little skill and low resources but are able to call on more advanced groups when necessary[1]. Other, more skilled groups are able to deploy zero-day exploits (before a patch is available) and custom payloads. Due to this variability, defenders need to be flexible in their defences and, in general, they will benefit from focusing on defending the assets rather than thwarting specific attackers. However, if an organisation is experiencing a heightened threat from a particular group, it can be beneficial to adopt a more threat-centric approach.

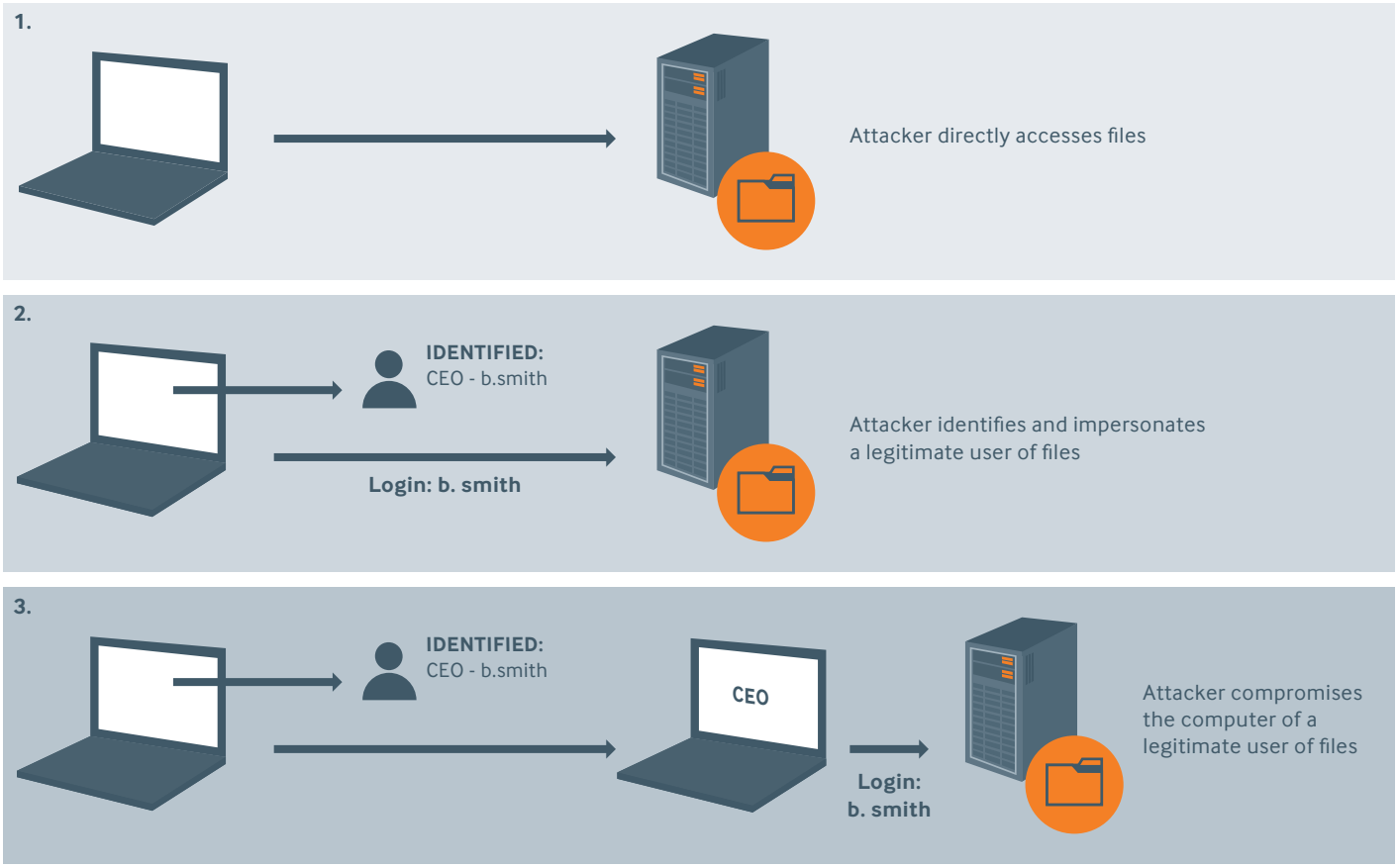
Identification of Data

Once a network has been compromised and the C&C infrastructure set up, attackers will need to seek out the data that is useful to them. This is rarely data that relates solely to a specific project, but will more usually be wider information relating to the organisation, its structure, network topologies, connections to the outside world – and its defences. CPNI has produced comprehensive advice under the title 'Protecting Information About Networks, the Organisation and its Systems (PIANOS)'[3].

To identify information of interest, some attackers will simply list the machines on the domain and then mount the file shares of machines that sound relevant from their hostname or description. Attackers then browse the file shares for folders or documents of potential interest.

More advanced attackers, or attackers who have no success with browsing files, will attempt more targeted identification of information using resources such as wikis and SharePoints. Typically, a great deal of information useful to an attacker is available with low privilege credentials, as details of individuals and organisational structure are usually available to all employees on internal portals or document management systems. Once the individuals with access to the required documents have been identified, attackers will be able to focus on horizontal and vertical movement throughout the network to obtain the remainder of the information they seek. Attackers will use a variety of techniques to move through the network, including keylogging, privilege escalation exploits and password dumping and cracking.

An attacker's techniques will depend on the accessibility of the information and how stealthy the attacker wishes to be



Attackers often focus on the small subset of individuals that have access to the data they need. In one compromise of a large organisation with tens of thousands of employees, the attackers were found on only five computers; however, these five computers allowed access to all information of interest to the attackers, as they belonged to the head of networking, head of research, and so on.

Once key individuals have been identified, common targets for attackers will be mailboxes, shared drives, SharePoint sites, and the contents of the hard drive or individual file storage of those key individuals. There is also evidence of attackers searching such locations as the recycle bin or deleted emails in the hunt for documents of interest. Attackers will search logically (for the location of all projects, for example), but they will also search for a number of keywords, which might include such terms as 'restricted' or 'sensitive'.

Attackers also tend to show considerable interest in defensive plans and hence will target the computers and mailboxes of senior security personnel, as well as attempting to identify details of logging, alerting and SIEM infrastructure. In addition, attackers are often observed attempting to identify relationships with external bodies that might be advising on defence – and to discover what advice those bodies have given.

Aggregation and Preparation of Data

A number of attacker groups also appear to share a tactic of preparing files for exfiltration. Although files will be obtained from throughout the network, they will often be aggregated on a particular host, typically either a system that is not interactively used (such as a printer server), or the host being used for the internal phase of the attack. Files will be hidden there, often in directories that are unlikely to be inspected by anyone who happens to use the host – such as the recycle bin, or Windows system, or temporary folders. More advanced attackers might also attempt to disguise the files, both during the aggregation and exfiltration stages. Tactics seen here include changing the extensions and magic numbers of files, or even packaging files within other file types, such as Microsoft Office documents or executable files.

Once the files have been collected, attackers often prepare them for transport by compressing and potentially encrypting them. The most common method of compressing the files involves built-in Windows functionality such as zip or cab files (which can be created with a tool from Microsoft). Some attackers will use other compression tools or encryption functionality, or occasionally custom-written tools. Compressing files into an archive is advantageous for the attacker for two reasons. First, it means that only a single transfer is required, rather than one for each file; and secondly, it can serve to hide the files on the network and at the perimeter, particularly if the files are also encrypted.

Exfiltration Channels

Controls currently used by most organisations do not prevent simple exfiltration channels and hence attackers are relatively unrestrained when it comes to their exfiltration method. Attackers therefore tend to use simple, reliable, overt, high-bandwidth methods, typically the protocols by which any technical user is likely to transfer a large file.

C&C Channel

During a compromise, attackers will typically install C&C malware from which to attack the internal network. The malware communicates with the attacker's supporting infrastructure, allowing external control. Different C&C tools use different methods to communicate and attackers will often use the C&C channel to exfiltrate data, as they know the connection works and has not been prevented by the organisation's defences. However, C&C channels tend to be used only for small volumes of files, as higher-bandwidth methods are often available for large file archives. CPNI has produced separate guidance regarding the detection of C&C channels[4].

HTTP/S

A common method for uploading files is transfer over HTTP or HTTPS[5]. This is a reliable protocol that enables large file transfers and has the added benefit that it is probably allowed through a web proxy, even if direct outbound connections are prohibited. Many C&C tools use HTTP and HTTPS as a communications channel; however, some have been observed that do not, and yet still use HTTP uploads to exfiltrate files. HTTPS has the additional benefit (for the attacker) that unless organisations are using SSL interception (and the attacker's tool accepts the intercepting certificate), investigators will not be able to determine what was being exfiltrated from network packet captures.

FTP/SFTP

The File Transfer Protocol (FTP) is another reliable method for transferring large files to remote hosts, and one that attackers frequently use to exfiltrate files to their own infrastructure. Rather than attempting to find an FTP server owned by the organisation, and using that, they will often take advantage of a lack of firewall rules preventing outbound connections and simply connect to their own FTP server to upload files. Windows and Linux systems typically come with built-in FTP functionality and so attackers do not need to risk using their own tools, which might be detected.

Some attackers use SSH services such as SFTP (Secure FTP) and SCP (Secure Copy) to transfer files. These utilities are likely to be found on Linux servers that the target organisation might be using, or attackers can use their own tools. Such services are encrypted, meaning that investigators would not be able to tell from packet captures or network taps what was being exfiltrated.

Email

The vast majority of organisations allow email (SMTP traffic) to arbitrary addresses, even when other outbound connections are prevented, and so attackers will sometimes exfiltrate files by this method. Exfiltration by email does not typically require the attacker to supply tools, as the majority of systems that might be compromised will already have the necessary tools. However, many organisations limit the size and nature of attachments, hence attackers will often send the data, obfuscated or encrypted, in many small chunks. Tools are likely to be required to prepare the data appropriately for exfiltration. Alternatively, attackers can use third-party cloud email services (see below) to bypass restrictions put in place by the organisation's mail servers.

Cloud Services

A rapidly emerging vector for exfiltration, and one which attackers are occasionally using for C&C as well as for exfiltration, is the increasing array of cloud services. Many large and reputable companies offer free cloud storage or email with little or no verification of account owners and so threat actors are readily able to open accounts for use in exfiltration. The use of cloud storage has several benefits to an attacker:

- The traffic is often encrypted with SSL, meaning it is significantly more difficult for investigators to analyse.
- The traffic will traverse an HTTP proxy, meaning a direct outbound connection from a compromised machine is not required.
- Employees are likely to use such cloud offerings on a regular basis, making it difficult to detect a threat actor who is using the channel to exfiltrate data.
- The use of a cloud service as a third party will obscure the final destination of the exfiltrated data and make it harder to design indicators of compromise.

Attackers now often bundle tools that can upload data to cloud services, and there are increasing signs that they are using such services as exfiltration vectors.

RDP

Microsoft's Remote Desktop Protocol (RDP) enables a user to log into a machine remotely and control it exactly as if the remote user were sitting directly in front of the machine. Some prolific attacking groups use RDP as a key mechanism for attacking a network once credentials have been obtained. As well as allowing control of a machine, the RDP protocol also enables the remote transfer of files, either by mounting drives from the attacker's machine onto the remote machine or through copy and paste operations. RDP connections are typically encrypted and, although it is possible for investigators to decrypt the traffic, they will first need to obtain the keys from the server.

IRC

Although less common these days, Internet Relay Chat (IRC) is still used for both C&C and exfiltration. The IRC protocol was designed to allow chatting online, and it supports functionality such as file transfers. It remains popular as a C&C mechanism as it lends itself well to controlling multiple targets simultaneously: in such cases, the C&C malware of each target logs into a chat room, where the attacker can issue commands to all infected machines at the same time. Exfiltration of data can then be triggered using the Direct Client Connect (DCC) SEND subprotocol of IRC. IRC can also be tunnelled through SSL, thereby impeding investigators attempting to identify what was exfiltrated from packet captures or network taps.

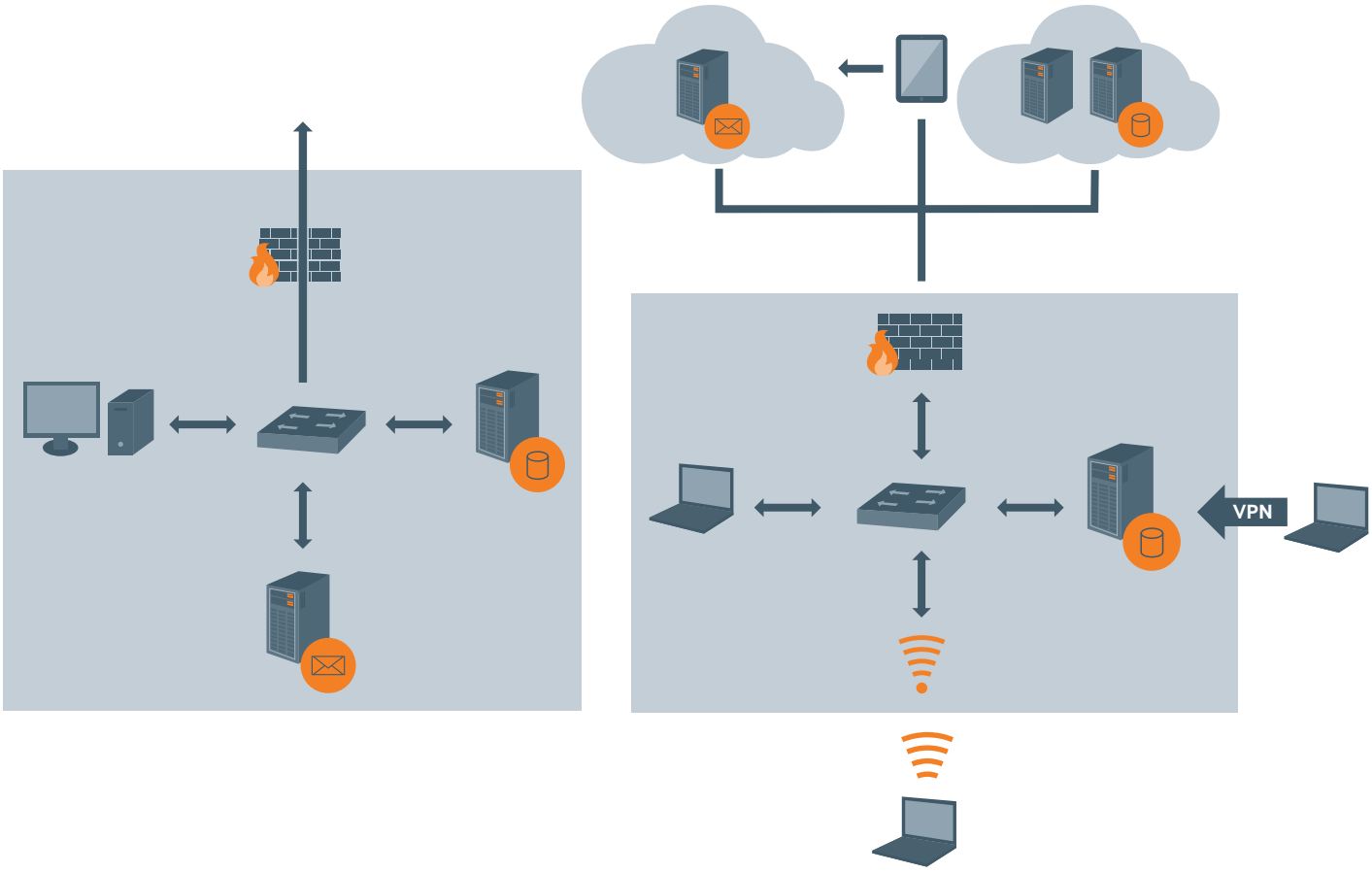
Future Exfiltration Tactics

Currently, attackers are not forced to use particularly advanced techniques, as few organisations beyond government departments dealing with highly classified material have controls in place that detect and deter even basic exfiltration. However, as organisations become more security-aware, attackers will need to use more sophisticated techniques to exfiltrate data.

Current trends suggest that attackers will increasingly utilise services via which organisations allow (or even require) outbound traffic. In this way, attackers will attempt to 'hide in the noise' by using channels that are also used legitimately, making it harder to detect at the perimeter. Such services will typically have a large bandwidth for data exfiltration. For particularly hardened targets, attackers might instead use covert or out-of-band channels, which are very difficult to detect but typically have much lower bandwidth than overt techniques. Hence they tend to be useful only for stealing documents of particular interest, rather than entire data sets.

The controls described in the 'Increasing Organisational Resilience' section will help an organisation to detect or deter attackers regardless of the exfiltration methods used; however, some business trends, such as increased storage of data in third-party clouds and hosted services, can reduce the effectiveness of those controls and that will need to be factored into risk decisions.

Traditional networks had defined perimeters and services contained within that perimeter.
Modern networks are complex and porous, with cloud services, mobile workers, smart phones, and so on.



Changes to Data Aggregation and Preparation

As defensive controls improve, attackers are likely to change their tactics to evade defensive measures. Organisations can expect to see greater abuse of legitimate functionality, as well as greater care taken by attackers when using a targeted account for certain behaviours, in an attempt to avoid detection due to inappropriate access. For example, an attacker dumping the CEO's email to the CEO's laptop will look less suspicious than if the mailbox were dumped to a normal workstation. Alternatively, attackers might attempt to recover the mailbox from the laptop itself, rather than from the mail server.

As many organisations move to service-oriented architectures (SOA), where data is exposed through web services, it may be that attackers start to use these interfaces to gather the data, rather than via traditional views such as websites or GUIs. It is important that defenders do not anticipate a specific method of accessing data, as attackers will then simply use other avenues to avoid detection.

There are indications that attackers are already starting to use forensics tools – for example, file carving utilities – to recover deleted (but not securely erased) files. These earlier versions of files can be useful to attackers, particularly if they contain data that was later redacted or classified and deleted. Advanced attackers have already been seen using forensics tools to hide data when aggregating it prior to exfiltration. Attackers are likely to use locations such as Volume Shadow Copy, unused disk space and alternate data streams (ADS), so that investigators examining a machine that appears to be aggregating do not locate the files being prepared for exfiltration[6].

Currently, attackers rarely go to great lengths to prepare files for exfiltration beyond compressing the files into manageable volumes. It is likely that, in the future, greater effort will be invested in preparing the files for exfiltration, both to obscure exfiltration and also to prevent or delay forensic analysis.

Attackers are likely to make increasing use of encryption, obfuscation and encoding. This might take the form of encryption of volumes prior to transport, or more advanced techniques – such as steganography into images or videos.

The Future is Cloudy

The previous section described how attackers are using public cloud services to exfiltrate data. This is a trend that is likely to continue and develop. Cloud services make excellent exfiltration vectors as they are typically hosted by reputable companies, employees consider them a part of their daily lives, and they increasingly use SSL to protect communications, thus making interception more difficult.

Attackers can be expected to make more use of cloud storage services such as Google Drive, SkyDrive, Dropbox and Amazon S3. Blacklisting specific sites is unlikely to be an effective prevention, as there are a great many cloud storage services and new ones regularly appear. Further use of cloud services such as exfiltrating data by cloud email (Gmail, Hotmail, Yahoo, etc.) is also likely to increase. In addition, cloud collaboration tools could well be used, as they allow similar functionality in uploading documents to a 'trusted' third-party location that the attacker can later access.

This issue can be especially significant if cloud services are used by the organisation, as covered below (see subsection 'Everything as a Service').

Exfiltration by Popular Websites

There are many websites that now form a regular part of people's lives. There is therefore significant pressure, verging on demand, to use those services at work. Many people use social networks throughout the day and, if staff are prevented from doing so, it could cause problems.

However, many popular websites allow uploads of files and text and hence provide a route to exfiltrate data. In particular, where images and videos can be uploaded, it is possible to exfiltrate far larger volumes of information – via data encoded within an image file – than as raw text. Indeed, experiments conducted on major social networks have demonstrated that it is possible to exfiltrate up to 20GB of data in a single file in this way (see box-out).

If attackers move to exfiltrating data through popular websites, it will require a change to controls at the perimeter, since it will be difficult to blacklist or even monitor volumes of traffic when there are often legitimate reasons for large data uploads (for example, an employee uploading holiday photos to a photo-sharing site). However, the remainder of the controls described in the 'Increasing Organisational Resilience' section provide multiple opportunities to detect and deter attackers before they can exfiltrate data using such websites.

MWR chose a number of popular websites and assessed the potential for exfiltration by uploading and retrieving files. The only data-hiding technique used was to append a zip archive of data to the end of each file before uploading. The retrieval of the files – and the zip archives – was then attempted. This technique is not possible where websites resize or re-encode images/videos, as the extra archive is lost. However, in such circumstances, more advanced data hiding can be used; for example, artefacts can be hidden in the image itself. Where more advanced data-hiding techniques are required, this has been marked as *.

WEBSITE	HOW MUCH DATA CAN BE EXFILTRATED
YouTube	20GB as a video
Flickr	200MB as an image, up to 1TB
Vimeo	5GB of videos per week; paid subscription required to retain original file
Facebook	25MB raw file for groups, 1GB as video* if verified profile, text posts
LinkedIn	100MB Office documents
DeviantArt	60MB as an image, up to 250MB
Pinterest	10MB as an image
Tumblr	10MB as an image, 150 photo posts allowed per day, text posts

Everything as a Service

Many organisations are switching to using cloud services such as Software as a Service (SaaS), Email as a Service (typically known as 'hosted email'), and even Infrastructure as a Service (IaaS). These services offer financial and flexibility benefits, including fixed costs per user and guarantees of availability. Unfortunately, the use of these services can leave organisations exposed, as their data is now outside their control. For example, in 2009 an employee of Twitter had the credentials to their corporate Gmail (and therefore Google Docs) account compromised, giving the attacker access to hundreds of Twitter's confidential documents[7].

It is now common for large amounts of highly sensitive data, such as customer relationships, financial documents, emails, or even systems, to exist outside an organisation's control. There is also the increasing risk that as these services become aggregators of critical data from a variety of organisations, they will become targets of nation state-sponsored attackers – if they are not already. Organisations are forced to trust that the service providers are taking all the desired precautions with their data.

Unfortunately, it is impossible for organisations themselves to apply many of the critical controls to cloud/managed services, as the service operators typically allow only limited control. For example, many of the controls recommended in the following 'Increasing Organisational Resilience' section, such as control of individual firewall rules, alerts on specific accesses or even extensive logs for forensics purposes, simply aren't available for the majority of cloud and managed services. Another significant issue is that there is no perimeter to defend if the data is stored in a cloud service. Cloud services are typically accessible from everywhere, hence an attacker in a foreign nation who has compromised an employee's credentials is likely to be able to log in and exfiltrate all data.

Best practices for cloud and managed services are outside the scope of this document. However, it is recommended that the increased risk of having valuable data in managed services is balanced against the business advantage of doing so. Should a decision then be made to use such services, it is important that the limitations of that decision are documented – so that usage of the service doesn't 'sprawl' and expose the organisation to more risk than was intended during the original risk management decision.

Mobile Devices and Remote Working

The increasing use of mobile devices and remote working presents opportunities for data exfiltration. A key issue is that potentially sensitive data can legitimately be accessed remotely when, in the past, it was probably only accessed from within the corporate network[8].

Once attackers have gained access to the corporate network (for example, by spear phishing), they might well seek to understand the mobile and remote working capabilities of the organisation to provide relatively unrestricted access to an organisation's network, and hence conduct further attacks or exfiltrate data. A further benefit to attackers is that employees might legitimately transfer large volumes of files while working remotely, making it more difficult to detect malicious activities. As with cloud services, the primary issue with mobile devices and remote working generally is the expansion or dissolving of the perimeter, and the effect that has on security controls that assume a hardened outer perimeter.

Mobile devices themselves can potentially provide additional routes for both attack and exfiltration. There are indications that attackers are compromising mobile devices in order to launch an attack once those devices are connected to corporate computers or networks. It is also plausible that attackers will seek to compromise devices with access to secure areas and segregated networks, in order to exfiltrate data onto the mobile device for recovery at a later period.

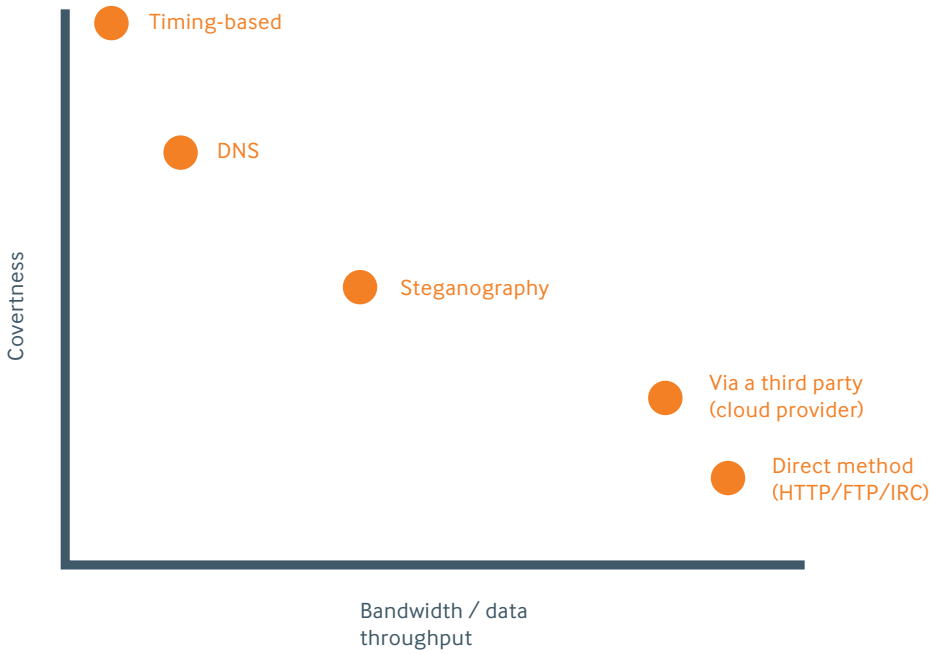
Covert Channels

Attackers targeting hardened organisations – or hardened networks within organisations – might use covert channels. There is a sizable body of literature surrounding covert channels for exfiltration, covering such topics as hiding data within common protocols (DNS, for example) and even low-level packet manipulation, such as hiding data by modifying TCP headers. Furthermore, research has been done on exfiltrating data through the timing of packets to locations, rather than the contents of the packets[9].

Detecting exfiltration through these routes tends to be very difficult; however, attackers will be greatly limited by bandwidth, as these methods are typically highly inefficient (although a notable exception is where attackers disguise their data as allowed protocols: for example, by tunnelling over SSL).

Organisations stand the best chance of detecting and deterring data exfiltration via covert channels by developing a defence-in-depth approach. For example, an attacker using such exfiltration channels will require custom tools, which might be more easily detectable.

Graph showing the trade-off between covert methods and those with high data throughput. Typically, the more covert a method the lower the bandwidth



Out-of-Band Channels

If defences are significantly increased, attackers might still find success by using out-of-band techniques to exfiltrate data, i.e. using channels other than via the traditional network. This aims to defeat controls such as segregated and air-gapped networks, or tightly controlled networks where much traffic is monitored or restricted. As with covert channels, there is a body of literature detailing both hypothetical and actual methods by which attackers could exfiltrate data without going through the network's perimeter. Examples include the physical recovery of printed documents, faxing, the use of mobile devices, optical or audio transmission of data, and setting up new wireless networks[10 11].

These methods are relatively low bandwidth and require a significant time investment before they can be used in the field. Hence attackers are only likely to use such techniques when attempting to compromise high-value targets that have significant defences – such as air-gapped resources – in place.

Increasing Organisational Resilience

To stand the best chance of detecting or deterring data exfiltration, organisations need to have a defensive programme based on defence in depth, as individual controls can be circumvented. The programme should not focus on preventing data exfiltration, as this must be considered impossible, but on making attacks more difficult while increasing the number of opportunities to detect an attacker's activity.

A key aspect of such a defence is ensuring a coherent, organisation-wide plan that benefits from an overview of assets and risk (see section 'Business Considerations'). This provides an environment for the defensive strategies to have the greatest chance of success. The first task the majority of organisations will then face is assessing the sensitivity of information in their possession, and how that information is used within the organisation (see 'Information Classification').

A control that underpins much of the defence against data exfiltration and advanced attacks in general is logging (see 'Logging'). This allows forensic analysis of an attacker's actions and achievements and also provides the framework for auditing and alerting, by which organisations can aim to detect attackers. Logging should be considered from a high level and then built into all further stages.

Once information has been classified and logging policies decided, organisations can begin to restrict access to that information (see section 'Segregation of Information') and the systems that have access to that information (see 'Segregation of Networks'). Hosts can be hardened to both impede attackers, and to force their behaviour down routes that allow for better protective monitoring (see 'Host Hardening').

Communications on the internal network can be monitored to identify the data acquisition and aggregation phases of an attack (see 'Movement of Data Internally'), and data monitored at the perimeter as a final attempt – where all previous controls have failed – to prevent the active exfiltration of data from the network (see 'Movement of Data at Perimeter').

Honeypots, i.e. assets intended to be compromised, are a highly effective tool to lure attackers into revealing their presence (see 'Honeypots') and, finally, more advanced defensive strategies can be considered, to detect and possibly deter advanced attackers (see 'Adaptive Defence').

Critical Security Controls

At the start of each of the following subsections, reference is made to the relevant Critical Security Controls that can guide organisations in implementing both 'quick wins' and deeper protective measures.
For full details of these 20 controls, see: http://www.cpni.gov.uk/advice/cyber/Critical-controls/ and http://www.counciloncybersecurity.org/practice-areas/technology

Business Considerations

CRITICAL SECURITY CONTROLS 9, 18

Introduction

Detecting advanced attackers who are locating and exfiltrating data is a difficult challenge. To have a realistic chance of responding, organisations will typically need to implement many controls and changes to current processes. Only a well thought-out and robustly implemented defence-in-depth approach will offer a chance of detecting advanced attackers, and there are several high-level areas that organisations will want to consider when designing such an approach.

Driven From the Top

The nature of the controls and the changes to everyday business will be wide-ranging and potentially disruptive, and staff therefore need to know that the defensive programme is a core organisational strategy driven from the highest levels. The importance of the defensive programme and the efforts to detect and deter advanced attackers need to be communicated as critical to the organisation's continued position and growth. It is advisable to align security objectives closely to business objectives, a level of vision that has to come from the top of the business.

Furthermore, a top-level coordinator for defence and threats is recommended since, in a complex organisation, issues can go unresolved due to 'buck passing' and complicated organisational territories. By having a single person who owns all defence and incidents, there will always be someone able to delegate an issue to the correct team in the event of confusion.

Where Should Information Security Sit?

Often, the IS team will have emerged as a side function of the IT team and hence will be organisationally within its remit. While this has benefits – as the staff will be intermingled with the IT staff, helping to expedite some security functions – there are several additional challenges from having IS as a subdivision of IT:

- Budgetary: IS department budget will come from within the main IT budget, hence there will be occasions where IT has to choose, for example, between new equipment and security expenditure. Staff might well prefer new tablets to the segregation of a network.
- Authorisation: if IS is a subdivision of IT, it might lack the authority to force change when it's needed.
- Vision: although insider knowledge can be useful, being immersed in an environment can also prevent one from spotting its weaknesses.

It is recommended that IS is placed organisationally (and potentially geographically) with departments that have an overarching remit and are primarily tasked with protecting the organisation as a whole. Examples of such departments are Legal, Risk, or Regulatory Compliance. The IS department will need a functional relationship with IT, hence seconded officers in both directions should be considered and necessary steps taken to ensure that the relationship between the departments is positive and constructive.

Funding

Many of the organisational changes necessary to detect and deter advanced attackers will prove costly. In many cases, the expenditure might be on-going and significant; for example, the need for more staff. Organisations therefore need to ensure that this budget is understood and available, and signed off at the highest levels, and it is not advisable to take the expenditure directly from IT budgets. This is because IT and IS have quite distinct roles: whereas IT drives the organisation's efficiency and enables new business behaviours, IS is fundamentally protective. Organisations frequently find it hard to justify IS expenditure, which is seen to be offsetting a potential risk, until the organisation has itself suffered an attack.

The following considerations can help to justify the expenditure:

- The cost of projects collapsing, where those projects are likely to be of interest to foreign nations; for example, projects in foreign nations or in competition with large organisations of a foreign nation.
- Potential fines or regulatory action as a result of data loss. A robustly implemented defensive programme can limit fines, as demonstrating the true extent of a breach will avoid the need to pay maximum fines based on hypothetical loss.
- The contractual requirements of clients or partners.
- The reputational and potential sales benefits of being able to demonstrate that security is a core part of the business.

Culture

To detect or deter advanced attackers from compromising data requires a level of understanding and investment from all staff, especially those who deal with sensitive data. The necessary controls can be restrictive, and can change how aspects of the organisation function, so it is important for staff to grasp the reasons for the changes.

It is recommended that organisations make security awareness a part of their culture, by introducing specific security sessions as part of the induction process – as well as for existing staff – and by potentially factoring security awareness into career paths.

Security training can be seen as dull and uninvolving by staff if not done correctly. This can serve to 'switch off' staff to security issues, so organisations are encouraged to ensure that security training is engaging and interesting. Some organisations report successes with 'gamification' of security, such as introducing levels of award (e.g. a 'black belt in security'[12]), while experience shows that staff often respond well to live demonstrations of the threats and attacker capability. As part of this, stories of successful and unsuccessful attacks against the organisation can help to make the threats real to employees. Organisations may benefit by bringing in external partners, such as design agencies, where the skillset does not exist within the organisation to communicate security training appropriately.

Information Classification

CRITICAL SECURITY CONTROL 15

Introduction

Modern networks are highly complex and often porous, meaning security departments are forced to accept that they will not be able to prevent all data exfiltration attempts. Instead, organisations should focus on protecting the information that is critical to them and direct the majority of their efforts to ensuring that such data does not fall into the hands of motivated adversaries. However, an important issue is that many organisations do not fully know what critical data exists across their organisation.

The first step is for an organisation to identify what is critical to them. Once the data has been classified in this way, the process of identifying the instances and locations of critical information can begin.

Experience shows that the majority of private organisations, even the more security-aware, classify little of their data and have either no protective markings or merely a 'restricted' or 'confidential' marking for data such as medical records or payment information. Furthermore, some organisations base their classifications solely on the premise that the data might be leaked or otherwise made publically available, and do not account for the scenario whereby the data is acquired covertly by a knowledgeable adversary, such as a competitor or nation state. By contrast, government organisations have a well-developed classification system that is embedded in the mindsets of employees who work with highly sensitive data. In these cases, the controls required to protect the information are typically well understood by those who work with the data[13].

Government Classifications

Although previously complex – with a range of five classifications, each with different protective measures required – the revised classification system as of April 2014 has just three markings: OFFICIAL, SECRET and TOP SECRET. This is intended to allow the majority of work to take place with 'OFFICIAL' information and hence fewer protective controls, while focusing effort and time-sensitive or expensive controls on the 5% of information that is either SECRET or TOP SECRET.

How to Implement

Information classification across a large, complex organisation can be daunting and difficult owing to the complexity of functions, people and information. It is therefore recommended that individuals experienced in such assessments guide the classification. Classification is usually accomplished by means of a business impact analysis (BIA), derived from business continuity studies, which seeks to identify critical functions.

A typical analysis will look at many types of risk facing the organisation and, while it might be thought desirable to conduct a full BIA, for the purposes of managing loss through data exfiltration the focus is likely to be on the confidentiality of assets. The analysis will identify the information relating to critical functions and assign impact levels by creating an impact table. This gives details of each impact level, and defines what qualifies information to be assigned to that level. Although often done by individuals, there are tools and products available to support the assessment. Crucially, however, no single impact table or framework will be appropriate for every business. It needs to be a custom exercise that is supported by the very highest levels of management.

Break down the problem

The first step is to break the problem down into manageable pieces. The nature of the pieces will depend on the organisation. It might, for example, be appropriate to break an organisation down by business unit, or perhaps by country and then business unit – while large groups might find it necessary to replicate the process across their various companies.

Workshop(s) to identify critical information

Once the organisation has been broken down into units, workshops can be held to identify the critical information. The organisation might wish to hold a single, large workshop with all involved, or might prefer to hold separate workshops for the various units. However, workshops should be attended by key staff at different levels within the unit.

The presence of senior staff is important, as is the involvement of 'ground-level' representatives. During the workshop, the participants will work through the business-critical functions and identify the information assets that – if compromised – would have severe impact. It is advisable for this process to be driven by balance sheets / profit and loss, to identify the areas that generate revenue. Staff should be encouraged to consider specific scenarios, such as competing organisations acquiring that information during negotiations or regulatory impacts. The output should be a list of critical assets, as seen by the unit, with comments as to the threats and criticality.

Creation of an impact table

An impact table can either be created prior to a workshop, and be used to guide the workshop, or it could instead follow on from the workshop once critical information has been identified. Either way, the exercise is best conducted by board-level staff who have an overview of the business. Experience has found that departments often incorrectly value their assets and overall importance to the organisation's success and so a top-down view is essential in appraising assets correctly. The assets that have been identified during the workshop(s) can be studied and compared, in order to sort the information according to a high-level view of the organisation's critical data.

The exercise should aim to decide on the number of impact levels and corresponding protective markings that works for the organisation. For some this will be a very small number, while others will benefit from more granular impact levels. There is no 'right number' of levels, as it depends on the organisation's appetite for complexity. Too many levels could confuse staff, increasing protective efforts but gaining little against motivated and skilled attackers, while too few might not allow effective classification in a complex organisation.

It is recommended, however, that impact tables include a category at least as high as 'ORG SECRET' (where the organisation's name replaces ORG), as all organisations are expected to have information that could prove crippling if it ended up in the hands of a motivated adversary.

The exercise should seek to identify what characteristics would cause information to be classified at a particular level. Some characteristics might be based on financial loss, or loss of market share. Full BIA impact tables will include other characteristics, such as the impact on employee motivation. An example table is given below. Once again, the involvement of board-level staff is critical as, in many instances, they are personally liable and should therefore have significant input to the risk tables.

An example impact table

RISK AREA	ORG RESTRICTED	ORG SECRET	ORG TOP SECRET
Legal impact	Fines up to £500k	Fines over £500k	Criminal case
Media coverage	Local complaints	Negative national media coverage	Negative international media coverage
Effect on research projects key to future growth	Project delayed by up to 6 months	Project delayed by up to 1 year	Beaten to market by competitor
Loss of revenues from collapsed negotiation	Up to £1 million	Between £1m and £10m	Over £10m

Assign impact levels / label information assets

Once impact levels and corresponding protective markings have been decided, assets should be compared with the table and protective markings assigned. This can be a difficult process. An initial challenge is to decide what is being labelled – whether it is a document, or the information itself. The labelling process will need to be integrated into business processes or it will not be effective. Newly generated information can be easier to classify, as impact tables and instructions can be distributed to the individuals who will be involved in the creation of sensitive data, enabling them to classify information correctly as it is created. However, the classification scheme should be rolled out through the organisation at the earliest opportunity.

Classifying historical data can be more difficult, as it's likely to exist across the entire organisation and it will be necessary to calculate whether the information remains sensitive. In some cases, older information will no longer be critical; for example, bids for projects that were completed several months previously are probably of little use. However, if a bid contains information detailing the organisation's unique approach, or supporting R&D work, it might remain sensitive in relation to future projects.

Considerations

- Top-down support from the highest levels of an organisation is critical for several reasons: the changes introduced are likely to impact people's workflows, so staff need to recognise that the changes have high-level support; top-level staff are frequently personally responsible for an organisation's activities and therefore need to be able to control the risk; and only top-level staff are likely to have the overview necessary to ensure that classification is appropriate to the organisation's assets and needs.
- Organisations are advised to adopt an information-focused approach. Details of where the information is stored or how it is used should not be considered during this phase; instead, attention is more usefully focused on the data itself.
- There can be a period of increased risk to assets once they have been classified but before protective controls have been applied. This is because attackers can simply search for 'ORG SECRET' or other highly classified documents. Hence the details of the classification process and the documents identified as being highly sensitive should be thoroughly protected (i.e. kept on a dedicated computer that is not on the network) until the controls can be put in place to protect the documents correctly. Organisations might even wish to work on paper, rather than digitally, for particularly sensitive parts of the process.
- Organisations should ensure that staff know how to apply classifications correctly. Over-classified information becomes harder to use and will require costly and time-consuming controls. Under-classified information will not be adequately protected and hence the confidentiality of that data could be at risk.
- Companies that deal (or are ever likely to deal) with government-protected documents are advised to ensure that their markings are easily distinguishable from government markings. For example, using 'ORG SECRET' (where ORG is replaced by the name of the organisation) is recommended over 'SECRET'.
- Large, multinational organisations might require more complex classifications to take local laws into account, for example when it comes to the movement of personal information outside the country. In such cases, instead of simply an 'ORG SECRET' marking, it might be necessary to implement an 'ORG GB SECRET' classification, for example. Similar issues can exist where individual companies within a group need to be firewalled from each other.

Logging

CRITICAL SECURITY CONTROLS 5, 14, 16

Introduction

A large number of organisations become aware of a breach not through their own defensive efforts but by third-party breach notifications. Once aware of an attack, an organisation can begin to hunt for signs of what was done, and whether the attacker still has a foothold in the network. However, this requires detailed historical logs that allow investigators to track an attacker's activity. These logs must capture the correct pieces of information, avoid having their integrity compromised by an attacker, and be retained so that past attacks can be analysed. Many organisations lack such measures, and so a key aspect of a defensive programme is to ensure that reliable and effective logging is implemented.

Once a suitable logging programme is in place, organisations can look to building on that programme proactively. By having analysts periodically reviewing the logs, it might be possible to identify recent attacks and then to set up systems to monitor for particular events – and generate alerts when they take place – thereby detecting current attacks. However, an effective logging scheme is the foundation for these more advanced activities[14].

Logging should be considered from a high-level, asset- and threat-centric approach – and then built on, to increase an organisation's resilience strategically.

How to Implement

Commencing a logging programme

Organisations will need to design a tiered, organisation-wide logging policy, which includes the degree to which different classes of system will be logged. This process should involve both network and risk staff. Where organisations do not already have one, a centralised logging system or systems will need to be built and configured to handle both current and expected logging load; plus tools will be required to enable analysts to perform both monitoring and investigation functions. Logging can then be developed to achieve specific goals, e.g. to 'log all successful and failed domain logins'.

The budget for an extensive logging programme can be significant – and can grow as further log sources are added – and will therefore need to be agreed for the programme, phased over a number of years as the scheme builds. An effective logging programme is likely to require people to implement and analyse, hardware for storage, and analysis and SIEM software to aid in analysis and alerting.

What to log

In complex environments, there will be a multitude of data sources that can be logged. Organisations are encouraged to log as many events as possible, for as long as possible, but complete coverage is rarely realistic. Logging should therefore be threat- and impact-driven, or asset-driven.

For example, organisations are advised to identify sensitive information and segregate it. The segregated networks should then be heavily monitored, ideally with full packet capture, and that data stored for as long as possible. Hosts that store sensitive information should also be thoroughly monitored. Major network ingresses, egresses and branch points (such as domain controllers, as they will contact the majority of hosts on the network) are also worth logging as thoroughly as possible. Logs that contain fewer events but are of greater use to investigators should similarly be prioritised: for example, alerts generated by host-based antivirus. A list of recommended log sources is given in the accompanying box-out.

Commonly Useful Log Sources:

- Firewall
- HTTP proxy
- DHCP leases
- DNS requests
- Domain authentications
- Antivirus alerts
- Internal NetFlow data
- File access
- Binaries not typically used (net.exe, ipconfig, route, etc.)

Tiered storage policies are strongly recommended. For example, while full packet captures should be kept for as long as practically possible, packet header data can perhaps be kept for far longer, to give investigators as much of a history and timeline as possible[15].

How to log

An important aspect of logging is to ensure that a centralised time source is used by all systems that provide logs, so that events can be correlated. Where possible, the time source should be verified and protected so that an attacker cannot trick or influence it.

Advanced attackers will sometimes attempt to delete or modify logs to hide their activities and to frustrate investigators. Hence logs for important systems or important compromise indicators such as antivirus are best stored centrally, i.e. on a separate hardened host. For less critical systems, it can be acceptable to store logs on the system itself; however, organisations should select specific low-volume events for which to export logs (such as successful or failed logins). Access to log aggregation systems should be restricted to a subset of employees, and organisations should consider managing the systems separately from the domain and network. This will both preserve the evidence value of the logs and prevent attackers from frustrating investigatory efforts.

Where cost and other resources allow, it is advisable to back up and archive logs offline on a regular basis, so that historical data is preserved where possible.

What to do with logs

The primary purpose of logs is to aid investigations. However, once the data is collected, organisations can turn the raw log data into information and then into insight. This can be used to drive auditing or 'hunting' for signs of past compromise, or for setting up alerts for current compromise. Analysts will need to identify the characteristic signs of an attack and then set up views of logs to help draw out that information.

An example might be failed logins across domain administrator accounts indicating online brute-forcing. Meanwhile, tying logs together to identify patterns can prove extremely useful; for example, a 'switchport up' event from a switch would normally be followed by an 802.1X authorisation from the RADIUS server and then a DHCP lease request to the DHCP server. This pattern would represent a user plugging in a machine and, if one of those events were to happen in isolation, it might be a cause for suspicion. It will be necessary for analysts to communicate with system owners to identify 'normal' patterns of behaviour and hence what deviates from the norm. Also, it is desirable for analysts to hunt proactively for potential compromise, rather than just review logs, as looking at the same logs every day can often cause analysts to become blind to what is occurring. Automated review should be used where possible in these situations.

It is recommended that organisations ensure that investigatory teams are not overwhelmed by a great number of alerts. An effective way to manage this is to have ratings, so that a 'critical' alert will be responded to very rapidly, while a lower-rated alert will be addressed within a longer agreed time frame.

Organisations are likely to find that some events generate a large number of alerts that are almost entirely false positives. In this case, it is recommended that such events are simply logged and not raised as alerts, while regular reviews of alert ratings should be conducted in collaboration with analysts who might be able to suggest new events that should trigger an alert. Organisations might also consider generating, for example, a 'medium' alert if a significantly increased number of low-rated alerts is seen to occur.

Considerations

- The validity of network monitoring logs can be difficult to prove in court[16]. Best efforts should be taken to preserve the evidence potential of log information and hence it's recommended that an organisation's legal counsel is involved in the process of designing the corporate logging strategy.
- Defenders need to assume that attackers will be attempting to identify or disrupt defensive plans; hence alert thresholds are best stored and calculated on hardened aggregation hosts, rather than the hosts themselves, so that attackers can't establish what will generate an alert. Defenders can also assume that attackers are likely to attempt to compromise the log aggregation and monitoring servers.
- Experience shows that different log collection and monitoring tools can produce different results. Therefore, where it is possible and feasible, organisations should not be averse to having multiple tools that do similar jobs.
- Where time and resources allow, organisations can benefit from periodically having their forensic team or third-party provider 'wargame'. Hosts can be picked that are 'compromised' and investigators then check whether the correct logging is in place that would have let them identify that host from a third-party breach notification. Furthermore, all real investigations should conclude with an 'After Action Review' to determine any new logging that should be implemented to better aid a similar investigation in future.

Segregation of Information

CRITICAL SECURITY CONTROLS 12, 15, 16

Introduction

Once critical information has been identified and classified, it can be segregated based on the principle of 'need to know'. This process is also known as compartmentalisation. Compartmentalising information is traditionally seen as a way to mitigate insider threat, as few individuals can see all the information and hence a compromised individual is limited in the information they can expose. However, compartmentalisation also has significant benefits when considering remote attackers as, should an attacker compromise an individual's access to data, they will be limited in the scope of information they can access. If the attacker seeks more than compartmentalised fragments of information they will either need to compromise the access of multiple, lower-level employees, or compromise someone with a higher level of access. Both activities present opportunities for the defensive team to detect the attacker. Furthermore, segregating information has benefits when segregating network resources, as clusters of information and access requirements will already have been identified.

How to Implement

Hardening access control

When protecting information, organisations will often focus on preventing access to that information. However, sensitive information will be needed in the course of business and so attackers will typically compromise someone who has legitimate access to documents and then abuse this access.

Access control throughout the organisation should therefore be locked down as tightly as possible to reduce the number of people with access, and this applies to multiple technologies. An important stage is to harden the domain or other organisation-wide authentication and authorisation systems, as much access to individual systems or information will come from domain permissions[17]. Access to individual documents and information stores such as wikis, file shares and SharePoints[18] (that will have been identified as part of the information classification phase) should also be controlled. Many of these technologies are able to offer robust and granular access control, which can be used to restrict the files that individual users are able to access, although this might require recent versions of the product.

A common problem is administrative access as, by their very nature, administrators will have access to everything. Organisations are therefore advised to reduce the number of actions that require an administrative account, by creating accounts with permission to perform specific activities. Administrative accounts can then be subjected to very high levels of auditing and alerting.

Organisations might also choose to have separate information stores or domains for logically different units – for example, separate domains and file stores for each country operation or even business unit. This helps to segregate information and access more fully as, for example, in a global organisation, an administrative account in country A will not have access to sensitive files in country B.

By restricting access, organisations can focus their logging on the accounts that have access to sensitive documents, whether as administrators or users. Logging can also focus on attempts to gain access to those accounts, such as failed logins, or logins outside normal business hours.

Segregation of understanding

Organisations might consider segregating understanding, as well as information itself. This means that lower-level employees will only have visibility of things that fall under their professional purview. To implement this approach, an organisation will need to take the critical and sensitive information that has been identified, and understand the different members of staff who are involved in the production and consumption of that data. Some members of staff might only require access to subsets of the data, or indeed views or extrapolations of the data.

A 'View of the Data'

This is where a presentation of sensitive information is prepared that allows the user to obtain the information they need, without revealing the entire data set. One example might be an executive who needs to see sales trends, rather than details of the sales themselves.

Take the example of an analyst, who is working on a set of figures but doesn't need to know what project those figures relate to. In this case, an attacker would need to compromise more than just the analyst's access in order to have a contextual view of the data.

Considerations

- If information and understanding have been segregated, forensic events will need to be supported by staff that can identify the relevance of any compromised data – as it might not be obvious to investigators.
- Where sensitive information is purged from systems where it doesn't need to exist, secure erasure software should to be used to ensure attackers can't simply recover the 'deleted' files forensically.
- Organisations will want to ensure that segregation of understanding doesn't negatively affect how employees treat the data. There can be a risk that if employees do not understand the context of what they are working on, they will not treat it with the required sensitivity.
- Where views of data are created, organisations should be aware that the views might still be highly sensitive, as information that is of use to their own analysts will be of similar – or greater – use to competitor or nation state analysts.
- Highly sensitive data often needs to be shared with external entities, such as auditors or companies as part of a merger. Such sharing will require extreme care, as these third parties are unlikely to protect the data to the organisation's own standards. Cases exist where attackers have compromised law firms and other supporting third parties to gain access to their targeted data. It is recommended that where possible, less sensitive views of the data are prepared and shared and, where it is necessary to share the sensitive data itself, the third party should be provided with a hardened laptop containing the data – with measures to prevent data being removed. A technical member of staff will be required to facilitate any necessary sharing.

Segregation of Networks

CRITICAL SECURITY CONTROLS 10, 11, 13, 19

Introduction

Once information has been classified and the critical information identified, organisations will want to ensure that they are preventing inappropriate access to that information. A common issue with many organisations is a lack of effective segregation of networks. This means that once an attacker has a toehold in the organisation, their movements are likely to be poorly restrained (see section 'A Day in the Life of an Attacker and a Defender').

In fact, many organisations have an entirely flat network where even business units in different countries have full network access to the full resources of a UK business. As well as a lack of effective network segregation, it is rare to find organisations with effective information segregation, as organisations will typically have large repositories of information (such as file shares, SharePoint or wikis) with few access restrictions. The outcome is that attackers have few boundaries to overcome in locating, accessing and aggregating information that will be of use to them.

The core issue here is that networks were often initially designed for convenience, based on the premise that the internal network is trusted – as are the staff. Much of an organisation's security efforts will therefore have been focused on keeping attackers from breaching the network perimeter. This approach, however, is insufficient in dealing with advanced threats, such as from nation states. In a complex organisation, it is highly likely that an advanced attacker will be able to gain access to the internal network via client-side exploits, phishing campaigns or by exploiting a weak service. Organisations are now forced to assume that a sufficiently funded and motivated adversary will be able to gain access to the internal network.

To increase the difficulty for the attacker, and also increase the number of opportunities to detect malicious activities, internal networks need to be segregated and hardened. Access to both networks and information is best based on the principle of 'need to know' and 'least privilege', whereby users are only allowed access to information (and indeed the servers where the information is stored) if they need that access for their job. This philosophy will help to prevent a trusted user's compromised credentials being used to access widespread information and can also help combat insider threats (which are not directly dealt with in this document).

Organisations will want to decide on an appropriate level of segregation, along with controls that prevent trivial access to inappropriate data but still allow the business to function effectively. This can be guided by the results of the information classification phase, with sensitive documents protected by hardened networks and resources, while less restrictive protections are placed on the main business network.

How to Implement

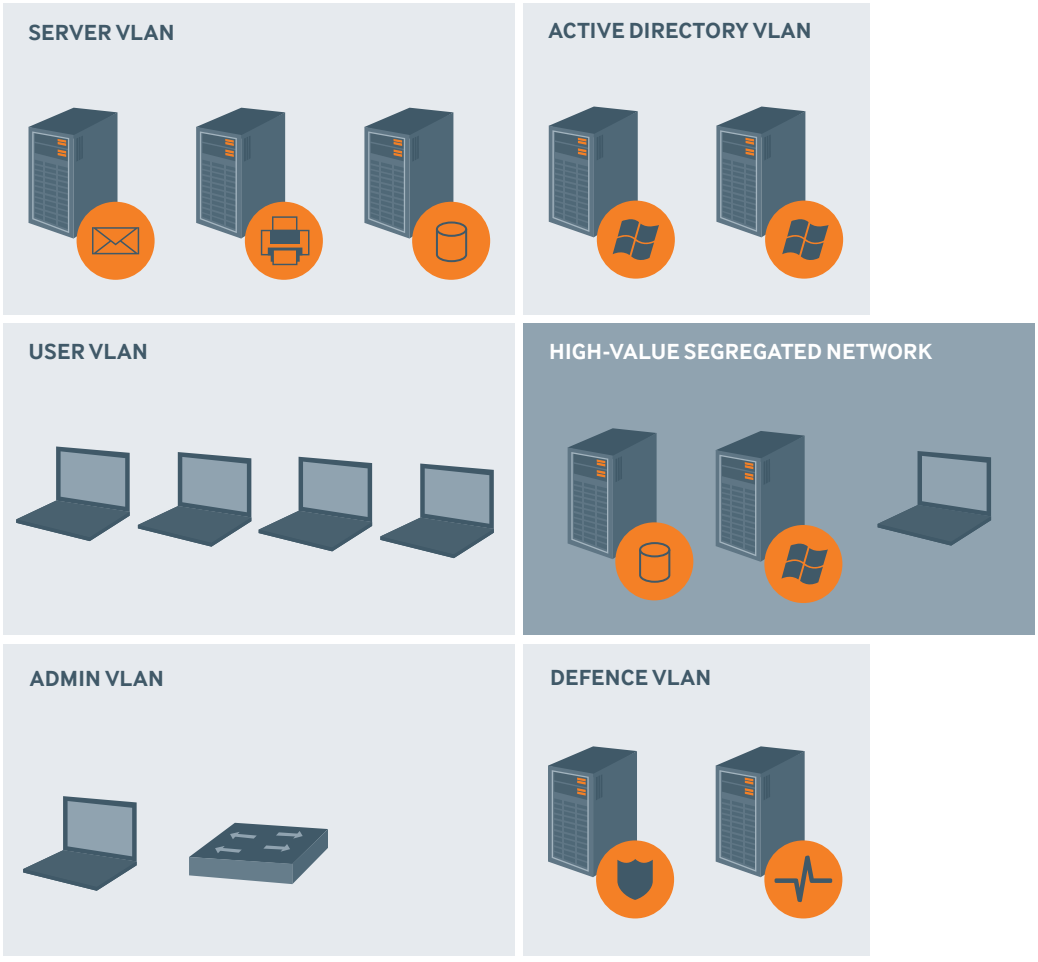
General network segregation

Ideally, the business network should be divided up into VLANs or physically separate networks. Although this is a significant project to implement fully, quick wins can be obtained by segregating the significant units. For example, in many organisations the majority of desktops only require access to a small number of services: Active Directory, file shares, proxies, etc. Once requirements are understood, these can be placed into VLANs. It is therefore advisable for organisations to start by understanding what needs to communicate with what, and this can potentially be achieved by parsing log data or NetFlow data as well as by talking to the people involved.

Once broad VLANs have been applied, organisations can progressively tighten the restrictions and granularity of ACLs, implementing firewalls at key junctions to support these ACLs. The aim is to reach a point where, for example, a desktop machine can only talk to the relevant ports on the required servers it needs, and nothing else. Individual servers should also be locked down, so that they can only communicate with the hosts and ports they require.

Network segregation will make the attacker's work significantly more difficult, as it will impede movement around the network. Unless the attacker is willing to restrict their movement to the allowed routes, they will be forced either to compromise the switching and routing equipment or to seek another means for movement, such as via USB drives. For example, instead of being able to move directly from a compromised helpdesk user's desktop to the CEO's desktop, they will need to move through the domain controller that is able to talk to both. If this action is limited by ports, the attacker will only be able to use RPC and SMB services and will not be able to access the domain controller via RDP. This increases the effort for the attacker and also increases the number of detection opportunities for the defensive team. To gain the most benefit from network segregation, the junction points between VLANS and networks, i.e. hosts that can be used to communicate with other hosts, should be identified and monitored thoroughly for signs of compromise or abuse.

Example segregation of logical resources into VLANs and a high-value network



High-value resources and networks

An output from the classification phase will be information identified as highly sensitive and even critical to the organisation's successful functioning. The information thus identified is expected to be significant to the point where loss of confidentiality could destroy deals critical to the company's future plans, or it might constitute key elements of the company's major products, hence it is worth putting substantial effort into protecting these assets. The process is likely to incur significant cost and effort to implement and maintain; however, only if done correctly will the organisation have a chance of protecting its most valuable information from nation state actors.

It is recommended that such assets are placed on entirely separate, air-gapped networks and resources. This is to prevent attackers from compromising critical assets even in cases where they have completely compromised the primary network.

For the highest level of assets, entirely separate laptops and even network infrastructure are recommended. VLAN segregation will not suffice, as a remote attacker might compromise switches, and then remap the ports to gain access to the desired VLAN. For the purpose of transferring information (such as software updates) to the secure network, organisations can look to using either read-only media, or data diodes, which allow updates into a network but do not allow data to leave. The complexity of the secure network will depend on the number of staff who require access. A separate domain might be needed or, if only a small number of individuals will have access to the information, local administration may suffice. Network and host controls (which are covered in more detail in a later section) should be based on assured products, such as those found on the CESG CPA[19]. Where remote access is essential, it is strongly recommended that this should only be provided by assured VPN solutions. However, organisations are advised to avoid arbitrary VPN connectivity if at all possible, and instead use only dedicated site-to-site VPNs.

Considerations

- Foreign intelligence organisations have highly advanced tools and methodologies that can defeat many controls, and their capabilities should not be underestimated when building secure networks. For example, there is evidence of malware that can cross air gaps using USB keys, and there are informal reports of malware that can steal data from the secure network by using audio exfiltration. All that is needed is for an infected 'secure' laptop to be in the same room as an infected 'normal' laptop. Social attacks should also be considered, such as using a compromised senior staff member's corporate email account to contact a user of the secure network, demanding to be emailed a file from the secure network.
- To be effective, the secure network(s) will require many behavioural changes by users, who will therefore need to be inducted into the controls, the risks and the value of the assets with which they are working. Giving employees real-world examples of attacks by nation states can be useful in helping employees to understand the capability and level of risk, confronting the all-too-common "but who would actually do that?" attitude.
- Users of the secure network are likely to discover that controls occasionally prevent them from undertaking activities that are important for their jobs. If their issues are not quickly resolved, they might be unable to perform appropriately – or they might attempt to bypass the controls themselves. Hence a dedicated helpline or contact could be required – one that is quickly able to address such issues in a secure manner.
- Some organisations find that their network cannot readily be segregated. This is often the case where a network has simply grown with the organisation and there is no longer oversight of the whole network. Where this is the case, preliminary work on the network might be necessary. The NSA's 'Manageable Network Plan' can aid organisations in these preliminary steps[20].

Host Hardening

CRITICAL SECURITY CONTROLS 2, 3, 17

Introduction

Modern, advanced threat actors are highly capable when it comes to gaining access to machines through activities such as spear phishing and obtaining valid credentials. Despite the fact that organisations need to assume an attacker with sufficient skill and motivation will be able to succeed in these endeavours, host hardening is nevertheless a useful tactic, as it will make it far more difficult for the attacker to locate critical data or to penetrate further into the network.

A number of hardening measures can be applied to standard desktops and servers that will impede attackers without a negative effect on normal business activities. Meanwhile, more restrictive measures are recommended for machines that will be used for the storage of highly sensitive data.

How to Implement

Verified build

Security teams are advised to design a standard build of the major operating systems used in the organisation. These should be locked down and hardened to the highest level that permits core business to function. Various guides exist for advice on the configuration, such as Microsoft's Security Compliance Manager (SCM) and the NSA's operating system hardening guides[21], and it is recommended that the areas detailed below should be considered for the build. Separate high-security builds can then be created from the baseline by further hardening and restricting non-essential functionality.

Once a build has been created and the software typically used in the organisation installed, it will need to be assessed by an attacking team. The team will seek to identify areas that could be exploited by advanced attackers, along with further hardening opportunities.

Following approval of the build, it can be rolled out through the organisation in phases. New systems should be based on the highest security build possible for normal business activity and older systems gradually hardened or replaced. Any decision to 'weaken' the build to allow a specific function should be carefully considered and documented.

Antivirus

Builds should include antivirus / endpoint protection software to guard against common malware and tools that could be used post-exploitation. Many threat actors are known to use common hacking tools, which are often detectable using AV. Organisations might wish to consider using a range of anti-malware products in their business, to increase the diversity of detection and ensure that attackers can't simply learn to bypass a single AV. Where possible, AV is best configured to the maximum level of heuristic detection. Although this will produce more alerts, each of which will need responding to, it provides greater information for reactive incident analysis. AV should also be configured to log remotely, in order to prevent attackers from modifying logs on local machines following compromise.

OS kernel hardening

To make software exploitation more difficult and to prevent certain post-exploitation behaviours, it is recommended that kernel hardening is included in standard builds of operating systems. This is possible in Linux with enhancements such as SELinux and grsecurity[22]. In Windows, this can be achieved with the Enhanced Mitigation Experience Toolkit (EMET)[23].

Kernel hardening can mean increased deployment efforts, as some software packages require configuration of the hardening to work properly.

Authorised software and application whitelisting

Organisations are advised to decide on a list of authorised software and permitted configurations (such as disabling features that increase the attack surface) for that software. Software known to be commonly exploited, such as Java, is best omitted from the approved software list.

Software that is typically overlooked as part of the standard build is secure erasure software. As attackers are known to be using forensic tools to recover 'deleted' files, providing the workforce with the ability to securely delete files can help prevent data being exposed to attackers. Organisations might wish to consider software that ensures that any deletion activity triggers a secure erasure; however, it's worth bearing in mind that this can prove problematic for internal forensics investigations – and might even be used by the attackers themselves.

Once software has been approved, application whitelisting can help protect against malware and post-compromise activities by allowing only specific programs to run. Although this will not protect against exploitations of software vulnerabilities, it can prevent users and attackers from running applications not on the approved list, forcing other behaviours. Effective whitelisting is possible in recent versions of Windows by using AppLocker[24], and less effectively in older versions with Software Restriction Policies.

DLP

Data loss prevention tools can help prevent data exfiltration. However, organisations should be aware that they are not single solutions to the problem, as it is typically possible to bypass or otherwise evade DLP solutions given enough time and effort. They are nevertheless useful in preventing accidental leakage of data, which is beneficial in that it will help to avoid accidental movement of data from a secure compartment to a less secure compartment, thereby exposing it to the attacker. It will also increase the effort needed by the attacker to extract information.

To be effective, DLP solutions can require a significant investment of effort in tagging and tracking data. However, much of this effort will already have been expended in the earlier stages of data classification. DLP solutions can be found as third-party products, some of which integrate into other endpoint protections, or are included as features in modern versions of Windows and related packages.

Logging

Logging is covered in a separate section; however, it is important that minimum levels of logging are established and that standard builds are configured to log correctly. Logging should allow investigators to have the necessary data at their disposal to investigate an incident, with the logging data aggregated on a separate host to prevent attackers from locally destroying or modifying logs.

High-security builds will require a significantly higher level of logging, with the logging data securely stored for a longer period of time.

Encryption

Organisations are advised to decide on a level of encryption for mobile devices, such as laptops, to help prevent data loss from a stolen device. This should include robustly implemented full disk encryption. Organisations might also wish to investigate controls to ensure that any data transferred to devices such as USBs or CDs is suitably encrypted. This is to prevent an attacker who transfers data to such devices from recovering the data once the storage device has left the secured area.

High-security machines can benefit from having encrypted software containers as well as full disk encryption. Sensitive data can then be stored in the encrypted container, which can be unlocked when the data is required. Ideally, the container would be decrypted using a smart card or similar token-based system to prevent simple capture of the password. This will impede an attacker who has gained remote access to a secure machine, by increasing the effort needed to access the files within the container.

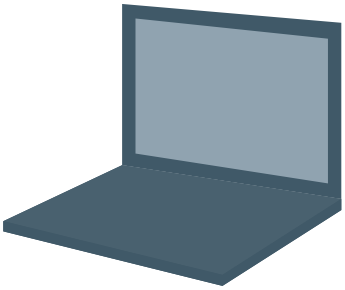
Media restriction

It is recommended that organisations restrict the devices that can be connected to hosts. This is to prevent movement of malware and documents within an organisation, thereby breaking compartmentalisation. Devices that are unlikely to be required at all should be restricted at the OS and BIOS levels, including FireWire, ExpressCard, and Bluetooth connections. Wi-Fi should be locked down to prevent connection to arbitrary networks, and the ability to host wireless or ad-hoc networks is best prevented entirely. Organisations might wish to restrict USB devices and the movement of data by CD/DVD using either group policy or third-party products.

High-security machines should have all connectivity disabled unless explicitly required. It is unlikely that such machines will need Wi-Fi or Bluetooth and hence it should be disabled at the OS and BIOS levels. It will probably be desirable to prevent USB drives entirely, or to allow only certain devices, and it is recommended that – where possible – those devices are accessed through a write blocker. This will prevent malware from writing data to the USB drive, which an attacker might use to exfiltrate the data from a secure to a less secure environment. CDs can be used where it is necessary to transfer data out of the secure environment, although this process should be monitored and recorded.

Bluetooth: Attacker can exfiltrate data to nearby devices under their control

3G (built-in or dongle): Attacker can make connections that will bypass internal security controls



Wi-Fi: Attacker can cause connection or creation of networks to exfiltrate data, bypassing any firewalls or proxies

Speaker / microphone: Highly advanced attackers can exfiltrate data to nearby devices

Two-factor authentication

A common strategy used by attackers for horizontal and vertical movement is to obtain credentials. This can be achieved by dumping and cracking hashes, extracting them from memory when users are logged in, or via keyloggers. Organisations can increase the difficulty level by requiring two-factor authentication wherever possible. The second factor should not be simply a PIN or secondary password, but something separate from password authentication. Examples include token generators, smart cards, USB dongles or services using secondary devices, such as mobile phones.

Considerations

- Host-based restrictions can occasionally prevent certain legitimate functions. Hence there needs to be a team nominated to handle issues where restrictions are preventing such functionality. Staff should be made aware of the team and the escalation process so that they don't engage in dangerous practices to bypass restrictions. If hardening prevents legitimate use, and issues are not responded to rapidly, the scheme will quickly lose buy-in.
- Organisations will occasionally need to update builds as vendors release new security features. It is recommended that named staff members are given ownership of the project to ensure builds are maintained.

Movement of Data Internally

CRITICAL SECURITY CONTROL 17

Introduction

When attempting to detect data exfiltration by network monitoring, many organisations will focus on the external perimeter. However, monitoring at this stage is often too late and, owing to the nature of a modern business, it can be hard to detect the actual exfiltration events. Instead, dedicating effort to monitoring the internal network can be a useful way to detect the information acquisition and aggregation stages of an advanced attack. Furthermore, the internal network can often lend itself better to monitoring.

How to Implement

Volumes of data

A useful indicator to monitor is the volume of data transfer between network compartments or even hosts. An internal network is likely to have certain patterns of network traffic, despite fluctuating with changing projects, etc. For example, data transferred from a file share will fluctuate as people require different documents, but a large data exfiltration from a file share is perhaps less common – and hence noteworthy, regardless of the destination.

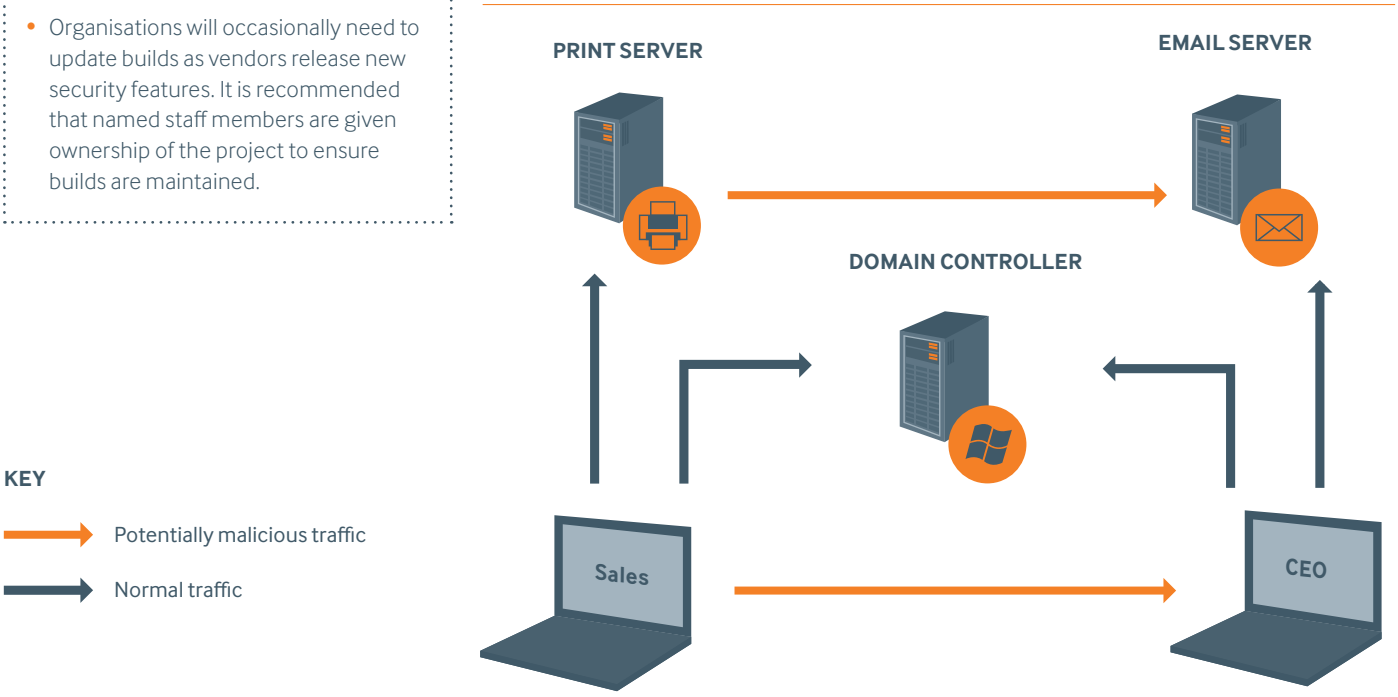
Organisations are advised to consider monitoring volumes of data transfers from either sensitive hosts (such as mail stores or file shares) or sensitive VLANs. It might also be worth monitoring data transfer from other groups of hosts, such as desktop to desktop, as transfer volumes here are expected to be low.

NetFlow or IP flow data can be useful in obtaining metrics on data volumes[25]. An alert generated by excessive data transfer can then be investigated as a mid-level alert.

Endpoints

Organisations might also want to monitor the nature of hosts that are communicating with each other. Once the network has been fully understood, it should be possible to derive assumptions and rules for network behaviour. For example, 'a desktop should not need to connect to a desktop' or 'only the domain controller need initiate a connection to senior management laptops'. These rules should be enforced with firewall rules and router ACLs.

Examples of normal and potentially malicious traffic



Other rules will emerge that are more variable, such as 'servers will rarely need to contact servers' or 'desktops in one business unit will rarely need to contact servers in another unit'. It might be decided to implement firewall rules in such cases or, instead, NetFlow and IP flow could be used to alert on events where these rules are broken. Such alerts can then be investigated as low- or mid-level alerts.

Organisations are also advised to use network monitoring to trigger alerts for any instances where rules that are protected by firewall rules are broken. This is in case attackers have reconfigured the firewall rules – and alerts of this sort should be categorised as high-level alerts.

Traffic types

Organisations are likely to find that certain types of traffic are common on the internal network, while others are either uncommon or unseen. For example, files might regularly be zipped using the Windows zip utility, whereas other zipping algorithms, such as gzip, are perhaps seen only rarely. Data that is encrypted – or encrypted using particular systems – might be uncommon except through particular protocols.

Deep packet inspection tools can be used to identify the encryption/compression types used and hence to alert on any deviance from the organisation's normal pattern of behaviour (these alerts would be categorised as medium- or low-level alerts). However, deep packet inspection can be difficult and costly, so organisations are advised to focus efforts on key systems or networks.

DLP / AV

Network-level DLP and AV solutions can be used to identify either accidental transfer of sensitive data or less advanced attackers. In lieu of a DLP solution, a degree of success can be had with a network-level AV system that has been given the organisation's protective markings as virus definitions. For example, an alert might be generated if a document containing 'ORG SECRET' is detected on the network. These should be viewed as mid-level alerts.

IDS

Network IDS can be used to detect attacker activity on the internal network. However, for an IDS to be useful, it needs a well-updated and maintained rule set. Furthermore, it is likely to detect only lower-skilled attackers, as more advanced threat actors will be well versed at IDS avoidance and will ensure their behaviour appears as normal activity. Hence an organisation should not rely on an IDS, but might wish to consider one as part of its defences. IDS-generated alerts should be considered as mid- to low-level alerts.

Considerations

- Organisations need to be aware that attackers are likely to attempt to understand the defensive monitoring in place. Hence organisations should protect the alert-generating servers to ensure that attackers are not able to identify the criteria that trigger an alert. This can be achieved by exporting raw data from endpoints to a dedicated monitoring host, and then having alerts generated on that host, which can be hardened and monitored.
- Defensive hosts, particularly AV and DLP, can themselves become sensitive if rule bases are specific. For example, if organisations are monitoring for certain words or phrases in documents, the nature of those words or phrases could be highly sensitive. Hosts therefore need to be adequately protected and monitored.
- Internal monitoring can produce information overload. Organisations are advised to aim for generating as many alerts as they are reasonably able to investigate, and simply store details of other events for either periodic review, or after-the-fact investigation.

Movement of Data at Perimeter

CRITICAL SECURITY CONTROL 17

Introduction

The final opportunity to detect or prevent an exfiltration event is at the perimeter, as the data is leaving. This can be difficult as modern organisations will have a large number of communications with the internet and a significant proportion of it will be encrypted (HTTPS). A key defence in detecting and deterring data exfiltration is to ensure that hosts are not able to connect to the internet directly, but only through a proxy.

How to Implement

Restrict traffic

By configuring perimeter and internal firewalls to ensure all outbound traffic must go through a proxy, it is possible to restrict traffic to those protocols that are business-critical. This will force attackers to use protocols of the defender's choice and prevent simple exfiltration. It also becomes possible to log and analyse all outbound traffic. Companies are likely to find that a very small number of protocols are genuinely required, such as HTTP/S and SMTP. Hosts that require additional protocols can be identified and the proxy or firewall configured to allow just those hosts to communicate on the necessary protocols.

SSL / encrypted traffic

A common issue with enforced proxies is how to handle encrypted traffic. If encrypted traffic such as HTTPS is allowed without interception, attackers can simply use that to exfiltrate data. However, intercepting comes with significant cost, bandwidth and privacy implications, as well as technical challenges. To intercept all HTTPS connections is possible, but will require expensive proxies owing to the computational power that is needed. Unless budgets are significant, proxies are likely to be overwhelmed by even a reasonable number of connections (see 'Fail open or fail closed', below). Importantly, staff will also have an expectation of privacy when using HTTPS. In addition, there are technical challenges when considering how to respond to invalid certificates.

If organisations choose to intercept encrypted traffic, they are advised to ensure that staff are made fully aware of this fact. It might be desirable to consult staff beforehand, and have signed agreements in place, or to consider injecting a banner or consent screen. Responses should be prepared: for example, if the certificate of the target site is invalid, how will users be informed?

Meanwhile, if an organisation chooses to intercept SSL connections selectively, it is advised to compile a whitelist of sites that are not intercepted – although many sites that users will hope to access without interception could potentially be used as exfiltration vectors. However, a whitelist is greatly preferable to a blacklist (of sites that are intercepted), since in this latter instance an attacker could simply create their own site.

Fail open or fail closed?

An important decision to consider when intercepting any traffic is under what conditions the proxy will fail open, and under what conditions it will fail closed. Failing open will allow an attacker to cause the proxy to hit that condition (for example, by overwhelming it with requests), and then exfiltrate their data while the proxy is inoperable. Conversely, while failing closed will prevent exfiltration of this sort, it could also prevent legitimate business function – something that could prove highly costly and damaging.

A potential compromise is to configure systems to fail open, yet ensure that such an event generates a high- or critical-level alert that is immediately investigated by response staff. Such an event is likely to be caused by a current exfiltration or an overload of resources, both of which will require an immediate response.

Monitor traffic

After traffic has been directed through a proxy, it is possible to analyse it for signs of compromise. This can include an analysis of the volume of data to identify large exfiltration events regardless of the destination address: a useful indicator that does not require SSL interception. Organisations can also monitor for communications with suspicious endpoints, such as those identified in private and public lists of known attacker hosts and, again, this does not require SSL interception. If there is to be SSL interception, however, organisations can consider deep packet inspection, analysing the content of data leaving the network for indicators of exfiltration. Examples of such indicators include the use of non-interceptable encryption, non-standard compression algorithms, or even plaintext sensitive documents.

Considerations

- Organisations are advised to see outbound restrictions merely as a measure to increase the effort required from an attacker, forcing them down routes that can be more easily monitored.
- Care should be taken with the configuration of proxy servers. Experience with exfiltration has shown that even subtle misconfigurations of proxy servers can allow easy exfiltration. Meanwhile, assumptions regarding supposedly 'safe' protocols should be avoided, as even protocols such as DNS can be abused to exfiltrate data.
- Compiling a whitelist of approved destination IP addresses can prevent trivial exfiltration, but even many whitelisted sites can still be used for this purpose.
- Advanced threat actors might directly attack either firewalls or the proxy to allow their communications. Organisations are advised to ensure that such devices are suitably hardened and monitored.

Honeypots

Introduction

Monitoring the access or use of sensitive resources can prove difficult, because of the legitimate use of the same resources throughout the working day. Hence staff involved in monitoring can find themselves spending large amounts of time sorting legitimate from illegitimate access. This often results in attempts to identify specific patterns representing 'bad access', as opposed to 'good access', and alerting on the former. However, an attacker then needs only to remain within a 'good' pattern to escape detection.

Honeypots avoid this problem by creating resources that appear to be sensitive but in fact have no legitimate use. This addresses the problem of monitoring, as any attempt to access the resource is highly likely to be an indicator of compromise.

Different definitions of 'honeypot' exist, including a full computer, or a file on a computer, but for the purposes of this document it will be assumed that honeypots can be created within any resource that an organisation might wish to monitor. However, some resources lend themselves particularly well to honeypotting.

How to Implement

Emails

The mailboxes of senior members of staff are common targets for attackers, since they will typically contain highly actionable information, from attachments incorporating sensitive data to informal reports of project status or defensive plans. Organisations might therefore wish to consider creating an email account for a fictional high-level employee. Considerations will include the extent to which the fictional employee is publicised; for example, adding them to public webpages might cause legal difficulties, particularly in the case of executives, and yet their absence could alert attackers to the honeypot.

The mailbox can initially be populated with real emails, or it could simply be a clone of a similar high-level employee's mailbox. The address can then be added to related groups, so that new emails flow into the account and an attacker identifying individuals through their membership of groups will find the honeypotted account. Organisations might wish to develop the project by ensuring the fake individual appears in locations such as SharePoint, the organisational chart, and other places an attacker might look to identify a suitable individual.

Mail servers or networking equipment can be set up to trigger an alert at any attempt to access the honeypotted mailbox. This should then be treated as an active breach, as other executive mailboxes are likely to be attacked at the same time.

Files

Once file stores and other repositories of sensitive information have been identified, organisations might choose to place files within them that would appear tempting to an attacker. These files could contain terms related to projects, organisational plans, defensive strategies or other keywords likely to be sought by an attacker. A range of honeypot files can be created to cover differing ranges of words that attackers might seek.

Files should be placed in locations where attackers are likely to find them. An example is where project updates for executives are stored; a 'strategic project plan' or similarly enticing file can be added to the same store. The same principle can be applied to database records, with records that need not be accessed during normal business functions placed within sensitive data sets.

The hosting file system or server can then be configured, potentially at the OS level, to alert when the file is accessed. An alert should likewise be triggered by an attacker who copies the entire data set.

Credentials

There are likely to be many administrators or privileged accounts within an organisation. Attackers will often seek to compromise one of these accounts to allow easy access to aggregated information such as file shares. It is by compromising highly privileged accounts that attackers aim to defeat compartmentalisation.

Organisations could therefore decide to create privileged credentials and monitor domain controllers for any attempted use of those credentials. They might even wish to go further by making the password for some such accounts deliberately vulnerable to offline cracking, so that attackers compromise the intended credentials before other accounts. This defensive activity can be supported by attempts within the organisation to crack its own passwords, helping to ensure there are no valid accounts with weaker passwords.

Machines / network resources

Honeypotted machines, networks and network resources are other options open to the defending organisation. For example, a machine named 'backup file share' could be tempting to an attacker, and could contain apparently useful data, while the approach can be reinforced by including the machine in network diagrams, as well as in the Active Directory and similar plausible locations.

The machines themselves, and potentially even the network infrastructure (such as switches/routers), should be configured to trigger an alert if there are any attempts to connect to them.

Another approach is that of monitoring for connections to non-existent IP addresses in the range of legitimate target machines. For example, if file-sharing servers are within a particular subnet, attempts to scan that subnet would ideally trigger an alert, as they could represent an attacker attempting to find more targets.

Considerations

- For the defence to be successful, an attacker needs to be lured into accessing or interacting with the honeypot. As such, it needs to be well implemented, i.e. tempting and locatable. This can be achieved by identifying where a legitimate document or machine is referenced within the organisation – and referencing the honeypot there as well. Knowledge of common attacker targets (see section 'Adaptive Defence') can aid in determining suitable resources.
- Advanced attackers are known to study the defensive tactics of an organisation, hence the nature and even mere existence of honeypots must be treated with the highest possible level of secrecy. Organisations might even choose to keep all related discussions and documentation off computer resources entirely.
- Organisations should not be averse to using real information for the honeypot, even though the information might therefore be at a higher risk. Attackers are highly likely to gain access to the confidential information regardless of its location, and so learning of the attack via a triggered honeypot will at least allow the organisation to be aware of, and to respond to, the attack.
- An alert from a honeypot needs to be treated as a highly critical alert. To be effective, particularly where honeypotted credentials or files are used, staff will need to respond rapidly and a mechanism should be designed to allow this to happen. If curious staff are triggering too many alerts, the honeypot might need to be redesigned, or staff in appropriate roles verbally instructed as to the exercise.

Adaptive Defence

CRITICAL SECURITY CONTROL 20

Introduction

There are many defensive strategies that can be adopted to provide general defence and raise the bar for attackers. However, once an effective defence-in-depth programme has been implemented, defence that is aware of specific threats can provide an enhanced level of protection.

To ensure that defences are appropriately threat-driven requires an understanding of the specific threats that face the organisation. Once threats and the associated tactics are understood, organisations can seek strategies that offer significant defensive successes for minimal cost and risk.

How to Implement

Threat actors

Different threat actors will have subtly or even wildly different techniques and goals, the nature of which will depend on the target organisation – and which will probably change over time. Many organisations are targeted by nation states as a result of becoming involved in that country, or competing with one of the foreign nation's own organisations. In such cases, the attacker's primary objective is often to acquire information relating to the current situation (e.g. negotiations, projects, acquisitions, etc.). This idea can guide defensive plans by ensuring that defenders are aware of the currently sensitive projects, or those most likely to attract hostile attention, and focusing greater resources on the key information while the projects are at a critical stage. This could be achieved by classifying information relating to those projects at a higher level than would otherwise be the case, until the critical period has passed, after which it can be reclassified to a lower marking.

Once the key information has been obtained, some nation state-sponsored attackers tend to remove themselves from the network to reduce the risk of discovery and the associated adverse political and media coverage. Other attacking groups will instead penetrate further into the organisation and obtain information periodically over a number of years. The latter group can be better countered by the defences described in this paper, as the longer they are in the network, the greater the chance of detection.

Finally, some organisations will be concerned about the threat of non-nation-sponsored attacks, such as by hacktivists or cybercriminals. It is important that organisations with these concerns understand the tactics used by such groups, and ensure their defences would prevent the better-known tactics. For example, cybercrime actors will often attempt to extract financial records from the database to obtain data such as credit card numbers. Attacks of this sort frequently make use of vulnerabilities in the public websites that connect to the databases. This tactic of exploiting a web app vulnerability to extract credit card data is rarely something that would be attempted by a nation state actor, hence the data set might be classified at too low a level if the specific threats are not considered.

Covert defence

Many advanced and nation state level attackers are observed attempting to identify the defensive plans of an organisation, as part of their initial information-gathering activity after penetrating a network. This often includes identifying the logging and alerting in place; any relevant third parties who might be aiding the organisation; rule sets for firewalls, proxies, etc.; and key defensive individuals whose mailboxes can then be targeted. Organisations are therefore advised to ensure that any attempt to identify defensive information alerts the defensive team.

It is also recommended that organisations ensure their defensive plans and, where possible, resources are 'off the grid', so that a network-based attacker can't compromise them. This might require paper and verbal communication for the most crucial aspects of plans, or machines that are managed from entirely air-gapped networks and are not on the corporate domain.

Organisations would also be wise to ensure that the majority of their defensive thresholds and capabilities are hidden from attackers. For example, in his talk 'Attack-Driven Defense', Zane Lackey of Etsy explored the idea of both defensive rootkits (i.e. hidden host agents) and network devices that do not alert, but rather send mass data reports to logging systems (see Further Reading). The actual alerting can then be done by aggregation systems, so that attackers are unable to identify alert thresholds by compromising network devices. To understand the behaviours that would generate an alert, an attacker would need to compromise the log aggregation system, which would offer an extra chance for the defence team to detect the attack.

Wargaming and learning lessons

Experience in dealing with advanced attackers is an extremely useful asset for an organisation. It can take the form of either experienced staff, who can be hired, consulted or contracted, or organisational experience – which must be learnt. All investigations of breaches should include a period of 'After Action Review', where the defensive teams try to identify the lessons to be learnt[26]. These should include the controls that would have prevented the attack, alerting that would have detected the attacker, and logging that could have made investigation easier. It is recommended that organisations have a defined process for rolling these lessons back into the security plan.

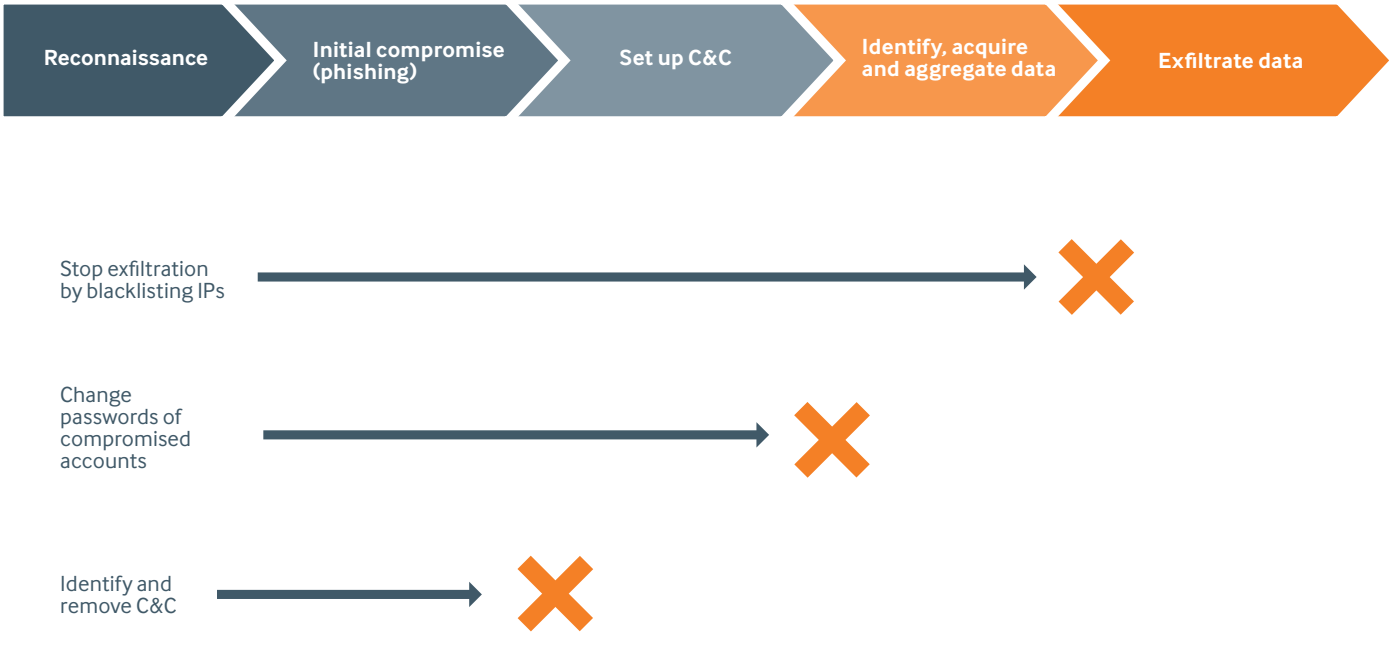
If there are no on-going breach investigations, defensive staff can 'wargame'. This can be a hypothetical exercise, whereby an attacker is imagined and the teams see whether defences would thwart them, or allow for their detection after the fact. Alternatively, security staff or external providers can conduct real-world attacks, either from an external perspective or by setting up an internal C&C and then compromising documents – while seeing how long it takes defenders to locate them once they are told of the attack. This process can also be used to generate understanding of the routes currently open to an attacker, and hence allowing these routes to be closed or honeypotted.

Delaying or deterring further attacks

If an organisation has managed to locate an attack, it is important not to remove the attacker immediately (by changing passwords, for example) unless there are significant business reasons for doing so. By taking time to understand the true extent of the breach, and how the attacker has gained entry and persistence, a more effective response can be prepared.

Organisations are advised to push an attacker as far back along the intrusion as they can. As an example, if an attacker is caught accessing a file and the organisation blocks access to that file, then the attacker is still acting on objectives. If, however, the command and control infrastructure and initial points of entry can be identified and successfully remedied, the attacker might be pushed back to the initial reconnaissance phase and forced to identify a new route in. This will increase the time and cost to the attacker and, although it might not necessarily prevent a future attack, it could buy the defensive team time to conduct further analysis and to better understand their weaknesses – as well as the attacker's likely future tactics.

By carefully planning the response to an attack, the threat actor can be pushed further back along the attack path



One of the few tactics that can successfully deter future attacks is misinformation. If attackers invest time and resources in compromising an organisation, only to obtain information that later proves to be useless or misleading, they are less likely to attack again.

There are two distinct approaches to take with misinformation. Tactical misinformation is where organisations have data, typically related to a current bid or project, that they believe will be exfiltrated, hence they plant misinformation to prevent threat actors from benefiting from the attack. Examples could include multiple versions of a negotiating position that the organisation suspects will be stolen, with only one containing the correct figures. Actors stealing the data will not know which is the correct set of figures and so cannot rely on the information they have acquired.

Meanwhile, strategic misinformation is more complex and involves planting false information over a longer term, causing the adversary to pursue a false line of thinking if the data is stolen and acted upon. If that line of thinking causes the adversary to expend time and effort before discovering the data is false, they might be dissuaded from stealing further information as there is a risk they will again waste effort. A successful misinformation campaign can be difficult to achieve, however, as it requires an understanding of the attacker's objectives to be successful. Some organisations combine misinformation with honeypots (see section 'Honeypots') in an attempt to thwart attackers.

Considerations

- While there can be great benefit in ensuring defences are designed for specific threats, organisations need to be careful to ensure both a good general level of defence and that their understanding of specific threats is accurate. If threat assessment is inaccurate, it can lead to excellent defences against one specific threat, while leaving the organisation vulnerable to another, equally real, threat.
- Although it is sometimes highly effective, misinformation can be a risky strategy. A key risk is that staff and partners believe the misinformation is real and make strategic decisions accordingly. The time and cost to implement and maintain a successful misinformation scheme can also be significant, if not well managed, and there is an additional challenge in that an analyst working for a competitor might be able to determine which of the planted data sets is most likely to be accurate.
- Organisations should consider partnerships with other organisations that face advanced persistent attacks. These partnerships can help organisations to share threat intelligence, experience, solutions, tools and indicators of compromise. The Cyber Security Information Sharing Partnership (www.cisp.org.uk) is an organisation that allows government and industry to share such information.

Summary

Modern organisations are highly complex and have valuable digital assets that they need to use in day-to-day business rather than simply store securely. Modern attackers are motivated and well resourced by groups that understand the value of the assets they hope to compromise. This combination means that complete prevention of data compromise and exfiltration by advanced attackers simply isn't possible. Instead, organisations must focus on detecting and deterring such attacks, which is still a significant challenge.

With no 'magic bullets' available, an organisation's best option for detecting and deterring data exfiltration by advanced attackers is a comprehensive defence-in-depth strategy. The strategy will not only need to be implemented but also maintained, and must be able to adapt to new business behaviours and changing threats. Such a strategy will require significant resource and is likely to touch much of an organisation's functioning. It therefore needs to be driven from the highest levels of the business.

A defensive programme can be expensive and, in order to justify the cost, an organisation needs to understand what might be lost without it. It also does no harm for senior personnel to remind themselves of this threat occasionally – if only to ensure that on-going defensive measures are not the first thing to be cut when the squeeze comes.

However, if well implemented, such a strategy will be able to push up the cost to the attacker while simultaneously decreasing the business impact on the organisation. A coherent strategy can work to flip the defender's dilemma (the idea that an attacker only needs to be successful once) into the attacker's dilemma (where a single detection can alert the defender to their presence)[27].

Glossary

ACL	Access Control List
AV	Antivirus
BIA	Business Impact Analysis
BIOS	Basic Input / Output System – The software that directly interfaces with hardware in a computer
CERT	Computer Emergency Response Team – Developed by Carnegie Mellon University
CESG	The Information Security arm of GCHQ
CPA	Commercial Product Assurance – A certification scheme by CESG
DHCP	Dynamic Host Configuration Protocol – A protocol used by servers to allocate IP addresses to computers
DLP	Data Loss Prevention – Software to detect data loss at either computer or network level
DNS	Domain Name Service – System by which human-readable URLs (www.site.com) are linked to IP addresses
EMET	Exploit Mitigation Experience Toolkit – Advanced exploit preventions for Windows
FTP	File Transfer Protocol – An older but regularly used system for transferring files. Typically unencrypted
GUI	Graphical User Interface – The visual interface of a program as opposed to the command line interface
gzip	A tool for compressing data
HTTP/S	Hypertext Transfer Protocol / Secure – The underlying protocol by which web pages are delivered
IDS	Intrusion Detection System – Software working at either computer or network level to detect signs of compromise. Typically compares activity to a list of known 'bad' activities
IP flow	A system to show packet flows between hosts and not the actual content of packets
IRC	Internet Relay Chat – A system to allow a number of people to chat online in a virtual chat room
IS	Information Security
OS	Operating System
RAT	Remote Access Tool – Malware to allow remote control of a computer
RDP	Remote Desktop Protocol – Microsoft's system for allowing remote usage of a Windows machine
RPC	Remote Procedure Call – System for allowing programs to trigger actions on remote computers
SCP	Secure Copy – Allows encrypted transfer of files
SELinux	A version of Linux with additional functionality to prevent exploitation
SFTP	Secure FTP
SIEM	Security Incident and Event Management – Software to allow correlation and investigation of alerts
SMB	Server Message Block – System for accessing resources on remote computers, including files and RPC
SMTP	Simple Mail Transfer Protocol – Protocol underpinning email
SSH	Secure Shell – Remote and encrypted command line access to systems
SSL	Secure Sockets Layer – Unencrypted protocols can be tunnelled through SSL to provide encryption
TCP	Transmission Control Protocol – A protocol used in sending data in the form of message units
VLAN	Virtual Local Area Network – Allows logically distinct networks to share the same physical hardware
VPN	Virtual Private Network – Allows physically distinct networks to communicate securely, as if physically connected

Quick Wins

A comprehensive defensive programme such as that described in this paper is time-consuming to define and agree, let alone to implement. However, while this process is being undertaken, there are several steps that IS staff can take to achieve a rapid improvement in resilience against data exfiltration.

The 'quick wins' described below are designed to help increase an organisation's overall defence against data exfiltration. In most cases, they assume the attackers are already in the network or soon will be, and hence they are generally designed to aid investigation following a third-party breach notification. The quick wins should be considered as temporary measures, while a full programme is in its early stages. All are likely to be circumventable by an advanced attacker, yet they could prove effective if the organisation is compromised by a less advanced attacker.

- **Ensure the network is manageable**
  A defensive programme or incident response will require accurate and updated network maps, and details of hosts and devices on the networks. IS and IT staff should ensure such maps are available. The Manageable Network Plan can be used to guide this process[20]. CPNI advice on Protecting Information About Networks, the Organisation and Staff (PIANOS) can be consulted to help protect the information adequately.
- **Logging throughout the organisation**
  To aid an investigation, IS staff are advised to ensure that as much log file data as possible is available for investigators. A cheap – but easily compromised – option is to have devices log data locally, monitoring such activities as the use of programs that are potentially useful to attackers: net.exe and ipconfig, for example. Where budget or surplus equipment is available, key devices should be set up to log data centrally, even if the logs aren't used for alerting.
- **Audit domain accounts**
  IS staff are advised to conduct audits for suspicious behaviour of domain accounts. This can include multiple failed logins or the creation of new administrative accounts. IS staff could also audit for weaknesses, such as active accounts for departed staff, or accounts not used for one month. The password strength of accounts can be audited by attempting to crack the passwords – and informing users if their password proved to be susceptible.
- **Separate network into VLANs**
  In some networks, broad VLAN segregation can be achieved without impacting services or requiring new hardware. As time and budget allow, segregation can become more granular and restrictive. Adding network segregation can provide critical new opportunities to log an attacker's horizontal and vertical network movements.
- **Use network-based AV or IDS as crude DLP**
  Many organisations have network-level antivirus or a computer that can be used as such. By adding sensitive keywords as virus definitions, the AV will generate alerts that help the IS team to see and understand the flow of sensitive documents in their organisation. Bear in mind, however, that if attackers compromise the AV host, they will gain access to the words and the alerts – which could prove useful to them.
- **Basic host hardening**
  Quick wins can often be achieved by hardening hosts through group policy, hence requiring no additional software. Staff are advised to investigate technologies such as EMET, and application whitelisting through AppLocker. An example of a quick win is that AppLocker can be configured to allow only software signed by specific companies to run (although the use of some third-party software can then prove problematic). By allowing only Microsoft and the manufacturers of approved software, attackers can be deterred from using their own tools. The hardening of operating systems, and third-party software, can be introduced gradually, as time and resources allow.
- **Make the most of current tools**
  Experience shows that many organisations have a number of security and usability tools that they are not fully utilising. By auditing the tools in place, an organisation can begin to gain maximum value from them.
- **Honeypots**
  Implementing honeypots (see section 'Honeypots') can be an effective quick win, and many types of honeypot do not require significant time or resources to implement. For example, intentionally weak domain credentials or sensitive-sounding documents can be quick to create without impacting the rest of the business – and hence might not require top-level authorisation.

A Day in the Life of an Attacker and a Defender

MWR conducts penetration testing for clients to validate defences and identify routes that attackers might use. The following is hybridised from interviews with MWR consultants and client defence staff, describing two network penetrations. In the individual cases, only particular controls needed to be overcome and by combining the tactics used, it is believed the majority of organisations would be susceptible. Consultants were careful to avoid any logging and alerting in place, although it was later established that neither organisation had effective alerting – hence steps have been left out for succinctness. Despite being security-aware organisations, neither target had an effective defence strategy for more advanced attackers, meaning no zero-day exploits were required and no covert actions were detected by the targets.

We got into the network through phishing emails with a link to a malicious webpage. We were targeting staff at a specific location, as we believed that proxy filtering was in place, so the malicious payload caused the infected laptops to connect to a Wi-Fi network that had been set up outside the building. We considered using DNS tunnelling for the initial payload as we then wouldn't need to be near the building, but decided it would be slow – and we only had limited time. We probed one of the systems connecting to us and used an unpatched Windows vulnerability to escalate privileges to local administrator. We then packed all our tools using a custom encryptor to avoid AV, but used built-in Windows tools where we could.

We have a number of alerts on a typical day, rarely anything serious and normally the standard drive-by, download-style attacks. We are alerted to phishing emails by staff, although the AV catches a lot of them first. No alerts came in that morning.

We used the browser of the machines to download benign files that were designed to be detected by the antivirus, and we waited until a domain administrator remotely logged into the machine to inspect the source of the alerts. At that point, we used the domain administrator's security token to add ourselves to the domain as administrators. Evidence of the C&C was then cleaned up with a script, so that the investigating administrator would only see that the browser had accessed some odd files.

We had a number of malware alerts from a particular host and so one of our team logged in to check it. He looked at the AV logs and running executables and didn't find anything suspicious. The files weren't malicious, but things like EICAR to test AVs with. He started a deep AV scan just to be safe and logged off.

We then accessed one of the other machines that had connected to the Wi-Fi network as a result of the spear phishing. Settings were inspected to determine details of the web proxy, and the domain administrator credentials were used to log into the proxy and view the rule set. We found a mistake in a rule that meant outbound traffic would be allowed to any address as long as it contained a particular string. We registered the relevant domain, and reconfigured the compromised hosts to communicate back to us using the new domain, meaning we could leave the vicinity of the building.

We are replacing one of the firewalls at the moment, as it has reached end of life, and so much of the morning was taken up with testing the build and making sure the old options will map over to the new OS – as there have been some changes between versions.

We used the local user's credentials to access the central SharePoint and identify the individuals who would have access to the targets specified by the clients. Security staff were also identified, and we used domain admin credentials to connect directly to the security staff's laptops and browse documents to establish the alerting and monitoring in place in the organisation. Domain admin credentials were then used to log into workstations of the individuals who were believed to have access to the target documents. In many cases, the target files required by the clients were found in the local hard drives of the targeted individuals' computers. However, for some documents this was not the case, and so we extracted plaintext passwords from the machines of the individuals. These passwords were then used to log into email accounts to search for evidence of the documents required.

We review logs daily, based on what our filters have pulled out. One of our web apps had hit the threshold of 5xx error codes so we had a look at its logs – but it didn't seem to be malicious.

Access to a specific system was required as evidence, so we installed screen-capturing software on a user of the system, and watched their access to determine how to use the system and navigate it appropriately. Once convinced that the system could safely be used without tripping any alerts, we connected using the compromised credentials and extracted the information. Data was collated on the C&C host and then zipped into an archive. The archive was then exfiltrated using HTTPS through the proxy to the domain that had been set up.

Case Studies

Misunderstanding the Threat

An organisation in the corporate services sector managed its risk based on the perceived primary threat of competitors hoping to gain an advantage, or other insight into their client relationships. As such, the organisation believed its primary assets were its financial data and client contacts.

An investigation found that it had been compromised by at least one attacker thought to be funded by a nation state – and that the attacker was compromising not the organisation's own data but its clients' data. In other words, by holding intimate details of its clients' businesses, the organisation had become a target itself.

Exfiltration Can be Easy

Attackers do not always need to exfiltrate data through advanced methods. One organisation was compromised by attackers who were primarily after email content. An investigation found that attackers had compromised credentials for the email accounts of senior members of staff, and then set up email forwarding rules so that a copy of every email received was sent to an account at a cloud provider. This traversed the outbound proxy and was found to have been active for several months.

Exfiltration Can be Advanced

Attackers tend to take the easiest routes available to them, to avoid exposing their more advanced capabilities. However, should it be required, attacker groups have shown that they can call on advanced methods. Examples of this include attackers that have assessed segregated environments for protocols that are permitted to cross the network boundary – and then rewritten their tools to use those protocols. There are also examples where attackers have successfully crossed air gaps, using such techniques as compromising the USB media that the organisation's staff were using to transfer data into an environment. Researchers have also demonstrated proof of concepts that use ultrasound via a device's built-in speakers and microphone to cross an air gap[28].

No Magic Bullets

Many products exist that claim to prevent advanced attacks and hence organisations can place too much reliance on a particular product, rather than implementing a robust defence-in-depth approach. An example is the 'Hidden Lynx' hacking campaign reported by Symantec. A military contractor in the U.S. was using an application whitelisting tool by Bit9. This was preventing attackers from running their own tools, so the attackers simply shifted their focus to Bit9 itself – stealing the Bit9 code-signing certificates, which enabled the attackers to sign their tools with Bit9's certificate. Hence they were readily able to run their own tools on systems protected by Bit9.

Further Reading

Hidden Lynx – Professional Hackers for Hire (Symantec) and Global Energy Cyberattacks: 'Night Dragon' (McAfee)
Two detailed reports of attacks that are believed to be nation state-sponsored
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/hidden_lynx.pdf
http://www.mcafee.com/uk/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf

CESG's Good Practice Guides (GPGs)
A number of guides to relevant aspects of security, available from CESG
GPG No.13 – Protective Monitoring for HMG ICT Systems
GPG No.18 – Forensic Readiness
GPG No.24 – Security Incident Management
GPG No.35 – Protecting an Internal ICT Network

Digital Evidence, Digital Investigations and E-Disclosure (IAAC)
A guide for organisations on ensuring forensic readiness
http://www.iaac.org.uk/itemfiles/DigitalInvestigations2013.pdf

Sexy Defense: Maximizing the home-field advantage (Iftach Ian Amit)
Guidance on effective defence
http://www.iamit.org/docs/sexydefense.pdf

Wirewatcher Blog – Blog on network security
http://wirewatcher.wordpress.com/

Attack-Driven Defense (Zane Lackey)
A recommended talk by Zane Lackey of Etsy on defending like an attacker
http://www.youtube.com/watch?v=_4vSurKPl6I
or
http://mwr.to/zane

Burn it Down! Rebuilding an INFOSEC Program
A talk by Dave Kennedy of TrustedSec that gives a good overview of why a robust defensive programme is needed to beat advanced attackers
http://www.youtube.com/watch?v=bojVsGlda50
http://mwr.to/kennedy

Lockheed Martin's Cyber Kill Chain®
A defence process that maps cyber attacks onto a military 'Kill Chain' model
http://www.lockheedmartin.co.uk/us/what-we-do/information-technology/cyber-security/cyber-kill-chain.html

HMG IA Standard No. 1 (CESG)
Government guidance on technical risk assessment
www.cesg.gov.uk/publications/Documents/is1_risk_assessment.pdf

Information Hiding Techniques: A Tutorial Review (Sabu M Thampi)
An overview of some information-hiding techniques by Sabu M Thampi of the LBS College of Engineering, Kasaragod
http://arxiv.org/ftp/arxiv/papers/0802/0802.3746.pdf

References

[1] **'Meet Hidden Lynx: The most elite hacker crew you've never heard of' by Dan Goodin on arstechnica**
http://arstechnica.com/security/2013/09/meet-hidden-lynx-the-most-elite-hacker-crew-youve-never-heard-of/

[2] **Mandiant Intelligence Center Report 'APT1: Exposing One of China's Cyber Espionage Units'**
http://intelreport.mandiant.com/

[3] **Guidance on Protecting Information About Networks, the Organisation and its Systems (CPNI)**
http://mwr.to/pianos

[4] **Guidance on C&C channels (CPNI)**
http://mwr.to/c2

[5] **'Exfiltration techniques: an examination and emulation' by Ryan Van Antwerp**
http://udspace.udel.edu/handle/19716/10145

[6] **'Anti-Forensics: Techniques, Detection and Countermeasures' by Simson Garfinkel**
http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.109.5063&rep=rep1&type=pdf

[7] **'Twitter calls lawyer over hacking' – BBC News 16 July 2009**
http://news.bbc.co.uk/1/hi/8153122.stm

[8] **Guidance on Mobile Devices (CPNI)**
http://www.cpni.gov.uk/advice/cyber/mobile-devices/

[9] **'IP Covert Channel Detection' by Cabuk, Brodley and Shields**
http://www.cs.tufts.edu/research/ml/docs/cabuk-covert-channels-tissec.pdf

[10] **'Advanced Data Exfiltration' by Iftach Ian Amit**
http://www.iamit.org/blog/2012/01/advanced-data-exfiltration/

[11] **'Hacking Exposed Wireless' by Cache, Wright and Liu**
Book on wireless security secrets and solutions

[12] **'Gamifying Security Awareness' blog by Ispitzner on SANS Securing the Human website**
http://www.securingthehuman.org/blog/2012/01/17/gamifying-security-awareness

[13] **Extract from HMG IA Standard No.1 – Business Impact Level Tables**
www.cesg.gov.uk/publications/Documents/business_impact_tables.pdf
HMG Security Policy Framework
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200552/HMG_Security_Policy_Framework_v10_0_Apr-2013.pdf
Government Security Classifications April 2014
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf

[14] **'I love it when a plan comes together' by Alec Waters on Wirewatcher**
http://wirewatcher.wordpress.com/2014/01/09/i-love-it-when-a-plancomes-together/

[15] **'When it comes to troubleshooting and threat detection, NetFlow AND packet capture trump all' by Jay Botelho for Network World**
http://www.networkworld.com/news/tech/2013/102813-packet-capture-complements-netflow-275434.html?page=1

[16] **'Si(EM)lent Witness' by Alec Waters on Wirewatcher**
https://wirewatcher.wordpress.com/2010/06/23/siemlent-witness/

[17] **'Best Practices for Securing Active Directory' – Microsoft**
http://www.microsoft.com/en-gb/download/details.aspx?id=38785

[18] **SharePoint – Microsoft**
http://office.microsoft.com/en-us/sharepoint-server-help/introduction-control-user-access-with-permissions-HA101794487.aspx

[19] **'CPA certified products' by CESG**
http://www.cesg.gov.uk/servicecatalogue/CPA/Pages/CPA-certified-products.aspx

[20] **'Manageable Network Plan' from NSA**
http://www.nsa.gov/ia/_files/vtechrep/ManageableNetworkPlan.pdf

[21] **'Operating Systems' by NSA**
http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml

[22] **'SELinux and grsecurity: A Side-by-Side Comparison of Mandatory Access Control and Access Control List Implementations' by Fox, Giordano, Stotler, Thomas**
http://www.cs.virginia.edu/~jcg8f/SELinux%20grsecurity%20paper.pdf

[23] **The Enhanced Mitigation Experience Toolkit (EMET)**
http://support.microsoft.com/kb/2458544

[24] **Windows AppLocker**
http://technet.microsoft.com/en-us/library/dd759117.aspx

[25] **'Log anomaly detection tools' blog by Antti Ajanki on Futurice**
http://blog.futurice.com/tech-pick-of-the-week-log-anomaly-detection-tools

[26] **'Private Investigations' by Alec Waters on Wirewatcher**
http://wirewatcher.wordpress.com/2010/05/25/private-investigations/

[27] **'Defender's Dilemma vs. Intruder's Dilemma' blog by Richard Bejtlich on TaoSecurity**
http://taosecurity.blogspot.co.uk/2009/05/defenders-dilemma-and-intruders-dilemma.html

[28] **'Ultrasound data transmission via a laptop' on Anfractuosity**
http://www.anfractuosity.com/projects/ultrasound-via-a-laptop/

Contributors:

David Chismon

Martyn Ruks

Matteo Michelini

Alec Waters - Dataline Software

MWR InfoSecurity (Head Office)
Matrix House, Basing View
Basingstoke RG21 4DZ
T: +44 (0)1256 300920
F: +44 (0)1256 323575

MWR InfoSecurity (London)
77 Weston Street
London SE1 3RS

MWR InfoSecurity (Manchester)
113-115 Portland Street
Manchester M1 6DW

MWR InfoSecurity (South Africa)
11 Autumn Street, Rivonia
Gauteng, 2128, South Africa
T: +27 (0)10 100 3157
F: +27 (0)10 100 3160

www.mwrinfosecurity.com
labs.mwrinfosecurity.com

Follow us on Twitter:
@mwrinfosecurity
@mwrlabs