REPORT

Incident trends report (October 2018 - April 2019)

Cyber incident trends in the UK with guidance on how to defend against, and recover from them.

10 September 2019

This report provides technical details of some of the most common incident trends observed in the UK, across all sectors, by the NCSC's Incident Management Team, in recent months.
For each incident type, we also provide detailed technical guidance on how to defend against them, and recover from them.
This report covers the period from October 2018 to April 2019.

Sources

The incident types we explore are not in themselves new, and the guidance we offer is readily available, both on the NCSC website and from other sources.
However, the combination of trends and guidance, backed with unique NCSC analysis, provides targeted and easily actionable advice.
With this information to hand you should be able to review your security posture and, where necessary, make improvements.

Adversaries

The trends are adversary agnostic, with each type of attack used widely by a range of different cyber adversaries.
All the incident types noted have resulted in compromises within the UK, some significant in nature.

Incidents and their mitigation

We cover five main trends affecting UK organisations.

Office 365

Cloud services, and Office 365 in particular, have become the primary target observed in recent months. While traditional models of on-premise IT services were frequently isolated from the internet, the widescale move to cloud services has put the IT of many enterprises within reach of internet-based attacks. In some cases, these services are only protected by a username and password.

Incident trends

There has been significant use of tools and scripts to try and guess users' passwords. This has almost become the daily norm for Office 365 deployments.

Attacks can now be mounted at scale across the Internet without ever having a foothold within the corporate infrastructure. A successful login will give access to corporate data stored in all Office 365 services. For example, both SharePoint and Exchange could be compromised, as well as any third-party services an enterprise has linked to Azure AD.

Password spraying

The most common attack affecting Office 365 is password spraying, which attempts a small number of commonly used passwords against multiple accounts over a long period of time. This doesn't tend to trigger account lockouts because the limit of failed attempts is not reached, and as a result can make it much harder for IT security teams to spot.

In most cases, attackers aren't after just one specific account, and using this method can target a large number of accounts in one organisation without raising any security suspicion.

Credential stuffing

On a smaller scale, we have also seen credential stuffing. This takes pairs of usernames and passwords from leaked data sets and tries them against other services, such as Office 365.

This is difficult to detect in logs as an attacker may only need a single attempt to successfully log in if the stolen details match those of the user's Office 365 account.

Attacker's goals

The intent varies across each of the attacks we see.

Common goals are:

- **accessing data and inboxes**
  this is usually for the purposes of intellectual property theft or espionage
- **using one inbox to add credibility to onward attacks**
  whether targeting a high-value individual in the same organisation or pivoting to another via trusted contacts
- **traditional network access**
  by re-using the Office 365 credentials against a corporate VPN service

Any attack will have a significantly higher impact if the compromised account holds administrator status. Further details of brute force attacks are documented by MITRE.

Office 365 remediation

Where possible, organisations using Office 365 should, as a minimum, follow the guidance in the NCSC's recent advisory and Microsoft's published security best practices to better mitigate account compromise.

Organisations should update their password policies inline with NCSC's guidance. This will include the use of Multi-Factor Authentication (sometimes called 2-Factor Authentication) in line with the NCSC's MFA guidance for enterprises. This provides extremely effective protection against username and password theft and the reuse of such credentials.

Organisations should also make sure that legacy authentication protocols are disabled/blocked, and that enough logging is in place to give insight into any attempted or successful breaches. The NCSC's LME project may be able to help you set up a monitoring solution.

Organisations should also configure the Office 365 service to harden it against common attack methods, as described in the advisory, and only log on to the service from trusted devices that are kept updated.

Organisations should securely configure their devices by following the NCSC's End User Device security principles.

As explained in a recent NCSC blog post, larger enterprises and the public sector should follow Microsoft's detailed configuration guidance. This explains how to implement some of the recommendations in our advisory and how some optional Microsoft services can be used to detect and reduce the impact of malicious activity.

Ransomware

Since the WannaCry and NotPetya attacks of 2017, ransomware attacks against enterprise networks have continued to rise in number and sophistication. Small, medium and large organisations across all sectors of industry, academia and government are regular targets.

Ransomware prevents organisations from using their computers or accessing their data, typically by encrypting files and folders via network shares. This causes significant operational disruption, and the financial impact for organisations can be devastating. This is especially true for businesses which have a high-degree of automation, or are very technology dependent.

Incident trends

Historically, ransomware has been delivered as a standalone attack. Today, attackers are using their network access to maximise the impact of the ransomware attack.

Network access allows the attacker to:

- build an understanding of their victim and their ability to pay
- identify system backups and other key systems so that these can be deleted or encrypted, so as to cause maximum impact
- identify and steal potentially valuable data
- ensure that they encrypt as much of an organisation's data as possible

Defences against ransomware should include security measures which can prevent an attacker gaining prior access to the network.

Ransomware tools

Cybercrime botnets such as Emotet, Dridex and Trickbot are commonly used as an initial infection vector, prior to retrieving and installing the ransomware. We have also seen some use of Pen-testing tools such as Cobalt Strike.

Ransomware such as Ryuk, LockerGoga, Bitpaymer and Dharma have been prevalent in recent months. In many cases it's difficult to know the root causes of the preceding compromise, especially when the ransomware can encrypt some of the sources which might be used for such an analysis.

Cases observed by the NCSC often tend to have resulted from a trojanised document, sent via email. The malware will exploit publicly known vulnerabilities and macros in Microsoft Office documents.

Ransomware remediation

Ransomware can usually be prevented by following enterprise security good practice. We describe how to prevent ransomware, and what to do if your organisation is infected in our Ransomware guidance.

Your approach should include:

- **reducing the chances of the initial malware reaching devices**
  you should prioritise defences against phishing attacks as described in our Phishing guidance and our guidance on macro security for Microsoft Office

- **considering the use of URL reputation services**
  including those built into your web browser, and Internet service providers.

- **using email authentication**
  via DMARC and DNS filtering products is highly recommended - in conjunction with Nominet, the NCSC provides a Protective DNS service (PDNS) for government, which can prevent organisations from accessing malicious sites hosting malware

- **making it more difficult for ransomware to run**
  once delivered - as described in our Mitigating Malware guidance

- **having a tested backup of your data**
  it is important that your backup is offline, so that it cannot be modified or deleted by ransomware. Our Securing Bulk Data guidance discusses the importance of knowing what data is most important to you, and how to back it up reliably

- **effective network segregation**
  can make it more difficult for malware to spread across a network and can therefore limit the impact of ransomware attacks - further details can be found in the Cyber security design principles, specifically, section 5.1. Our preventing lateral movement guidance is also useful.

Phishing

Phishing has been the most prevalent attack delivery method seen over the last few years, and particularly in recent months. Just about anyone with an Email address can be a target.

Incident trends

Specific methods observed recently by the NCSC include:

- **targeting Office 365 credentials** - the approach here is to persuade users to follow links to legitimate-looking login pages, which prompt for O365 credentials. More advanced versions of this attack also prompt the user to use MFA
- **sending emails from real, but compromised, email accounts** - quite often this approach will exploit an existing email thread or relationship to add a layer of authenticity to a spear phish
- **fake login pages** - these are dynamically generated, and personalised, pulling the real imagery and artwork from the victim's Office 365 portal
- **using Microsoft services** such as Azure or Office 365 Forms to host fake login pages - these give the address bar an added layer of authenticity

---

Phishing remediation

You should implement a multi-layered defence against phishing attacks. This will reduce the chances of a phishing email reaching a user and minimises the impact of those that get through.
The NCSC's recommended approach can be found in our Phishing guidance. This blog from 2016 explains why technical defences should form the majority of your efforts.
Configure Email anti-spoofing controls such as Domain-based Message Authentication, Reporting and Conformance (DMARC), Sender Policy Framework (SPF) and Domain-Keys Identified Mail (DKIM). Details on how to configure them can be found on our website. The NCSC offers a platform for assessing email security compliance through its Mail Check service.

Vulnerability scanning

Vulnerability scanning is a common reconnaissance method used to search for open network ports, identify unpatched, legacy or otherwise vulnerable software and to identify misconfigurations, all of which could have an effect on security..

Incident trends

We have seen attackers identify known weaknesses in Internet-facing service which they then target using tested techniques or 'exploits'. This approach means the attack is more likely to work first time, making its detection less likely when using traditional Intrusion prevention systems (IPS) and on-host security monitoring. Once an attacker has a foothold on the edge of your infrastructure, they will then attempt to run more network scans and re-use stolen credentials to pivot through to the core network.
Further details of these scanning techniques are documented by MITRE in these papers on Network service scanning and Exploiting public facing applications.

Vulnerability scanning remediation

Port scans and vulnerability scans are normal for any system connected to the Internet. You should ensure that all internet-facing servers that an attacker might be able to find are hardened, and the software running on them is fully patched. This recent blog from the NCSC highlights guidance which can help you to secure your servers.
We recommend following our cyber security design principles when designing your network, so that any initial attack can be easily detected in your logs, and that your attack surface is minimised to reduce the impact of compromise.
A penetration test can be a useful way of determining what an attacker scanning for vulnerabilities could find, and potentially attack. See our penetration testing guidance for more information, and the CHECK scheme for a list of NCSC-approved practitioners.
The NCSC provides a Web Check service that helps public sector organisations find and fix common vulnerabilities in the websites they manage. Public sector organisations can register for the Web Check service by following the link in this page.

Supply chain or trusted relationships

Threats introduced to enterprise networks via their service providers continue to be a major problem. Outsourcing – particularly of IT – often results in external parties and their own networks being able to access and even reconfigure enterprise services. Your network will inherit the risk from these connected networks. Outsourced services often have administrator access and use remote connections, along with tools which have a similar footprint to those used by attackers to “live off the land.” This raises the noise floor for internal SOC teams, making malicious activity more difficult to detect.

Incident trends

In recent months there have been several examples of attackers exploiting the connections of service providers to gain access to enterprise networks.

- NCSC’s own publication on APT10
- the exploitation of Remote Management and Monitoring (RMM) tooling to deploy ransomware, as reported by ZDNet
- the public disclosure of a “sophisticated intrusion” at a major outsourced IT vendor, as reported by Krebs on Security

---

Supply chain or trusted relationships remediation

Supply chain security should be a consideration when procuring both products and services. Our Supply Chain guidance proposes a series of 12 principles, designed to help organisations establish effective control and oversight of their supply chain.
Those using outsourced IT providers should ensure that any remote administration interfaces used by those service providers are secured, by for example using a well-configured VPN.

You should ensure that the way your provider connects to, or administers, your system meets your own organisation's security standards. You should take steps to segment and segregate your networks. This will help to contain the threat if another customer, who shares the same service provider (or the provider themselves) is compromised.

Segmentation and segregation can be achieved physically or logically using access control lists, network and computer virtualisation, firewalls, and network encryption such as Internet Protocol Security. Further detailed guidance is available from our partners at the Australian Cyber Security Centre.

You should document the remote interfaces and internal accesses in use by your service provider to ensure that they are fully revoked at the end of the contract. If they have installed services or software on your network, you should ensure that these can be easily removed at the end of the contract, as it may not be maintained or have security patches applied once that company is no longer involved.

If your supply chain includes the use of cloud services, you should read our blog post describing how to manage the risk of cloud-enabled products. Our Cloud Security Guidance will help you determine whether such a service appropriately protects your data and connected services. Our Software as a Service (SaaS) security guidance, will help you evaluate the security of the cloud-based applications you intend to consume.

PUBLISHED
30 August 2019

WRITTEN FOR

Small & medium sized organisations

Large organisations

Cyber security professionals

Public sector