TLP:WHITE

NCCIC

Alert (AA18-284A)

Publicly Available Tools Seen in Cyber Incidents Worldwide

More Alerts

Original release date: October 11, 2018

Summary

This report is a collaborative research effort by the cyber security authorities of five nations: Australia, Canada, New Zealand, the United Kingdom, and the United States.[1][2][3][4][5]

In it we highlight the use of five publicly available tools, which have been used for malicious purposes in recent cyber incidents around the world.

To aid the work of network defenders and systems administrators, we also provide advice on limiting the effectiveness of these tools and detecting their use on a network.

The individual tools we cover in this report are limited examples of the types of tools used by threat actors. You should not consider this an exhaustive list when planning your network defense.

Tools and techniques for exploiting networks and the data they hold are by no means the preserve of nation states or criminals on the dark web. Today, malicious tools with a variety of functions are widely and freely available for use by everyone from skilled penetration testers, hostile state actors and organized criminals, to amateur cyber criminals.

The tools in this Activity Alert have been used to compromise information across a wide range of critical sectors, including health, finance, government, and defense. Their widespread availability presents a challenge for network defense and threat-actor attribution.

Experience from all our countries makes it clear that, while cyber threat actors continue to develop their capabilities, they still make use of established tools and techniques. Even the most sophisticated threat actor groups use common, publicly available tools to achieve their objectives.

Whatever these objectives may be, initial compromises of victim systems are often established through exploitation of common security weaknesses. Abuse of unpatched software vulnerabilities or poorly configured systems are common ways for a threat actor to gain access. The tools detailed in this Activity Alert come into play once a compromise has been achieved, enabling attackers to further their objectives within the victim's systems.

How to Use This Report

The tools detailed in this Activity Alert fall into five categories: Remote Access Trojans (RATs), webshells, credential stealers, lateral movement frameworks, and command and control (C2) obfuscators.

TLP:WHITE

This Activity Alert provides an overview of the threat posed by each tool, along with insight into where and when it has been deployed by threat actors. Measures to aid detection and limit the effectiveness of each tool are also described.

The Activity Alert concludes with general advice for improving network defense practices.

Technical Details

Remote Access Trojan: JBiFrost

First observed in May 2015, the JBiFrost RAT is a variant of the Adwind RAT, with roots stretching back to the Frutas RAT from 2012.

A RAT is a program that, once installed on a victim's machine, allows remote administrative control. In a malicious context, it can—among many other functions—be used to install backdoors and key loggers, take screen shots, and exfiltrate data.

Malicious RATs can be difficult to detect because they are normally designed not to appear in lists of running programs and can mimic the behavior of legitimate applications.

To prevent forensic analysis, RATs have been known to disable security measures (e.g., Task Manager) and network analysis tools (e.g., Wireshark) on the victim's system.

In Use

JBiFrost RAT is typically employed by cyber criminals and low-skilled threat actors, but its capabilities could easily be adapted for use by state-sponsored threat actors.

Other RATs are widely used by Advanced Persistent Threat (APT) actor groups, such as Adwind RAT, against the aerospace and defense sector; or Quasar RAT, by APT10, against a broad range of sectors.

Threat actors have repeatedly compromised servers in our countries with the purpose of delivering malicious RATs to victims, either to gain remote access for further exploitation, or to steal valuable information such as banking credentials, intellectual property, or PII.

Capabilities

JBiFrost RAT is Java-based, cross-platform, and multifunctional. It poses a threat to several different operating systems, including Windows, Linux, MAC OS X, and Android.

JBiFrost RAT allows threat actors to pivot and move laterally across a network or install additional malicious software. It is primarily delivered through emails as an attachment, usually an invoice notice, request for quotation, remittance notice, shipment notification, payment notice, or with a link to a file hosting service.

Past infections have exfiltrated intellectual property, banking credentials, and personally identifiable information (PII). Machines infected with JBiFrost RAT can also be used in botnets to carry out distributed denial-of-service attacks.

Examples

Since early 2018, we have observed an increase in JBiFrost RAT being used in targeted attacks against critical national infrastructure owners and their supply chain operators. There has also been an increase in the RAT's hosting on infrastructure located in our countries.

In early 2017, Adwind RAT was deployed via spoofed emails designed to look as if they originated from Society for Worldwide Interbank Financial Telecommunication, or SWIFT, network services.

Many other publicly available RATs, including variations of Gh0st RAT, have also been observed in use against a range of victims worldwide.

Detection and Protection

Some possible indications of a JBiFrost RAT infection can include, but are not limited to:

- Inability to restart the computer in safe mode,
- Inability to open the Windows Registry Editor or Task Manager,
- Significant increase in disk activity and/or network traffic,
- Connection attempts to known malicious Internet Protocol (IP) addresses, and
- Creation of new files and directories with obfuscated or random names.

Protection is best afforded by ensuring systems and installed applications are all fully patched and updated. The use of a modern antivirus program with automatic definition updates and regular system scans will also help ensure that most of the latest variants are stopped in their tracks. You should ensure that your organization is able to collect antivirus detections centrally across its estate and investigate RAT detections efficiently.

Strict application whitelisting is recommended to prevent infections from occurring.

The initial infection mechanism for RATs, including JBiFrost RAT, can be via phishing emails. You can help prevent JBiFrost RAT infections by stopping these phishing emails from reaching your users, helping users to identify and report phishing emails, and implementing security controls so that the malicious email does not compromise your device. The United Kingdom National Cyber Security Centre (UK NCSC) has published phishing guidance.

Webshell: China Chopper

China Chopper is a publicly available, well-documented webshell that has been in widespread use since 2012.

Webshells are malicious scripts that are uploaded to a target host after an initial compromise and grant a threat actor remote administrative capability.

Once this access is established, webshells can also be used to pivot to additional hosts within a network.

In Use

China Chopper is extensively used by threat actors to remotely access compromised web servers, where it provides file and directory management, along with access to a virtual terminal on the compromised device.

As China Chopper is just 4 KB in size and has an easily modifiable payload, detection and mitigation are difficult for network defenders.

Capabilities

China Chopper has two main components: the China Chopper client-side, which is run by the attacker, and the China Chopper server, which is installed on the victim web server but is also attacker-controlled.

The webshell client can issue terminal commands and manage files on the victim server. Its MD5 hash is publicly available (originally posted on hxxp://www.maicaidao.com).

The MD5 hash of the web client is shown in table 1 below.

Table 1: China Chopper webshell client MD5 hash

Webshell Client	MD5 Hash
caidao.exe	5001ef50c7e869253a7c152a638eab8a

The webshell server is uploaded in plain text and can easily be changed by the attacker. This makes it harder to define a specific hash that can identify adversary activity. In summer 2018, threat actors were observed targeting public-facing web servers that were vulnerable to CVE-2017-3066. The activity was related to a vulnerability in the web application development platform Adobe ColdFusion, which enabled remote code execution.

China Chopper was intended as the second-stage payload, delivered once servers had been compromised, allowing the threat actor remote access to the victim host. After successful exploitation of a vulnerability on the victim machine, the text-based China Chopper is placed on the victim web server. Once uploaded, the webshell server can be accessed by the threat actor at any time using the client application. Once successfully connected, the threat actor proceeds to manipulate files and data on the web server.

China Chopper's capabilities include uploading and downloading files to and from the victim using the file-retrieval tool `wget` to download files from the internet to the target; and editing, deleting, copying, renaming, and even changing the timestamp, of existing files.

Detection and protection

The most powerful defense against a webshell is to avoid the web server being compromised in the first place. Ensure that all the software running on public-facing web servers is up-to-date with security patches applied. Audit custom applications for common web vulnerabilities. [6]

One attribute of China Chopper is that every action generates a hypertext transfer protocol (HTTP) POST. This can be noisy and is easily spotted if investigated by a network defender.

While the China Chopper webshell server upload is plain text, commands issued by the client are Base64 encoded, although this is easily decodable.

The adoption of Transport Layer Security (TLS) by web servers has resulted in web server traffic becoming encrypted, making detection of China Chopper activity using network-based tools more challenging.

The most effective way to detect and mitigate China Chopper is on the host itself—specifically on public-facing web servers. There are simple ways to search for the presence of the web-shell using the command line on both Linux and Windows based operating systems.[7]

To detect webshells more broadly, network defenders should focus on spotting either suspicious process execution on web servers (e.g., Hypertext Preprocessor [PHP] binaries spawning processes) and out-of-pattern outbound network connections from web servers. Typically, web servers make predictable connections to an internal network. Changes in those patterns may indicate the presence of a web shell. You can manage network permissions to prevent web-server processes from writing to directories where PHP can be executed, or from modifying existing files.

We also recommend that you use web access logs as a source of monitoring, such as through traffic analytics. Unexpected pages or changes in traffic patterns can be early indicators.

Credential Stealer: Mimikatz

Developed in 2007, Mimikatz is mainly used by attackers to collect the credentials of other users, who are logged into a targeted Windows machine. It does this by accessing the credentials in memory within a Windows process called Local Security Authority Subsystem Service (LSASS).

These credentials, either in plain text, or in hashed form, can be reused to give access to other machines on a network.

Although it was not originally intended as a hacking tool, in recent years Mimikatz has been used by multiple actors for malicious purposes. Its use in compromises around the world has prompted organizations globally to re-evaluate their network defenses.

Mimikatz is typically used by threat actors once access has been gained to a host and the threat actor wishes to move throughout the internal network. Its use can significantly undermine poorly configured network security.

In Use

Mimikatz source code is publicly available, which means anyone can compile their own versions of the new tool and potentially develop new Mimikatz custom plug-ins and additional functionality.

Our cyber authorities have observed widespread use of Mimikatz among threat actors, including organized crime and state-sponsored groups.

Once a threat actor has gained local administrator privileges on a host, Mimikatz provides the ability to obtain the hashes and clear-text credentials of other users, enabling the threat actor to escalate privileges within a domain and perform many other post-exploitation and lateral movement tasks.

For this reason, Mimikatz has been bundled into other penetration testing and exploitation suites, such as PowerShell Empire and Metasploit.

Capabilities

Mimikatz is best known for its ability to retrieve clear text credentials and hashes from memory, but its full suite of capabilities is extensive.

The tool can obtain Local Area Network Manager and NT LAN Manager hashes, certificates, and long-term keys on Windows XP (2003) through Windows 8.1 (2012r2). In addition, it can perform pass-the-hash or pass-the-ticket tasks and build Kerberos “golden tickets.”

Many features of Mimikatz can be automated with scripts, such as PowerShell, allowing a threat actor to rapidly exploit and traverse a compromised network. Furthermore, when operating in memory through the freely available “Invoke-Mimikatz” PowerShell script, Mimikatz activity is very difficult to isolate and identify.

Examples

Mimikatz has been used across multiple incidents by a broad range of threat actors for several years. In 2011, it was used by unknown threat actors to obtain administrator

credentials from the Dutch certificate authority, DigiNotar. The rapid loss of trust in DigiNotar led to the company filing for bankruptcy within a month of this compromise.

More recently, Mimikatz was used in conjunction with other malicious tools—in the NotPetya and BadRabbit ransomware attacks in 2017 to extract administrator credentials held on thousands of computers. These credentials were used to facilitate lateral movement and enabled the ransomware to propagate throughout networks, encrypting the hard drives of numerous systems where these credentials were valid.

In addition, a Microsoft research team identified use of Mimikatz during a sophisticated cyberattack targeting several high-profile technology and financial organizations. In combination with several other tools and exploited vulnerabilities, Mimikatz was used to dump and likely reuse system hashes.

Detection and Protection

Updating Windows will help reduce the information available to a threat actor from the Mimikatz tool, as Microsoft seeks to improve the protection offered in each new Windows version.

To prevent Mimikatz credential retrieval, network defenders should disable the storage of clear text passwords in LSASS memory. This is default behavior for Windows 8.1/Server 2012 R2 and later, but can be specified on older systems which have the relevant security patches installed.[8] Windows 10 and Windows Server 2016 systems can be protected by using newer security features, such as Credential Guard.

Credential Guard will be enabled by default if:

- The hardware meets Microsoft's Windows Hardware Compatibility Program Specifications and Policies for Windows Server 2016 and Windows Server Semi-Annual Branch; and
- The server is not acting as a Domain Controller.

You should verify that your physical and virtualized servers meet Microsoft's minimum requirements for each release of Windows 10 and Windows Server.

Password reuse across accounts, particularly administrator accounts, makes pass-the-hash attacks far simpler. You should set user policies within your organization that discourage password reuse, even across common level accounts on a network. The freely available Local Administrator Password Solution from Microsoft can allow easy management of local administrator passwords, preventing the need to set and store passwords manually.

Network administrators should monitor and respond to unusual or unauthorized account creation or authentication to prevent Kerberos ticket exploitation, or network persistence and lateral movement. For Windows, tools such as Microsoft Advanced Threat Analytics and Azure Advanced Threat Protection can help with this.

Network administrators should ensure that systems are patched and up-to-date. Numerous Mimikatz features are mitigated or significantly restricted by the latest system versions and updates. But no update is a perfect fix, as Mimikatz is continually evolving and new third-party modules are often developed.

Most up-to-date antivirus tools will detect and isolate non-customized Mimikatz use and should therefore be used to detect these instances. But threat actors can sometimes circumvent antivirus systems by running Mimikatz in memory, or by slightly modifying the original code of the tool. Wherever Mimikatz is detected, you should perform a rigorous

investigation, as it almost certainly indicates a threat actor is actively present in the network, rather than an automated process at work.

Several of Mimikatz's features rely on exploitation of administrator accounts. Therefore, you should ensure that administrator accounts are issued on an as-required basis only. Where administrative access is required, you should apply privileged access management principles.

Since Mimikatz can only capture the accounts of those users logged into a compromised machine, privileged users (e.g., domain administrators) should avoid logging into machines with their privileged credentials. Detailed information on securing Active Directory is available from Microsoft.[9]

Network defenders should audit the use of scripts, particularly PowerShell, and inspect logs to identify anomalies. This will aid in identifying Mimikatz or pass-the-hash abuse, as well as in providing some mitigation against attempts to bypass detection software.

Lateral Movement Framework: PowerShell Empire

PowerShell Empire is an example of a post-exploitation or lateral movement tool. It is designed to allow an attacker (or penetration tester) to move around a network after gaining initial access. Other examples of these tools include Cobalt Strike and Metasploit. PowerShell Empire can also be used to generate malicious documents and executables for social engineering access to networks.

The PowerShell Empire framework was designed as a legitimate penetration testing tool in 2015. PowerShell Empire acts as a framework for continued exploitation once a threat actor has gained access to a system.

The tool provides a threat actor with the ability to escalate privileges, harvest credentials, exfiltrate information, and move laterally across a network. These capabilities make it a powerful exploitation tool. Because it is built on a common legitimate application (PowerShell) and can operate almost entirely in memory, PowerShell Empire can be difficult to detect on a network using traditional antivirus tools.

In Use

PowerShell Empire has become increasingly popular among hostile state actors and organized criminals. In recent years we have seen it used in cyber incidents globally across a wide range of sectors.

Initial exploitation methods vary between compromises, and threat actors can configure the PowerShell Empire uniquely for each scenario and target. This, in combination with the wide range of skill and intent within the PowerShell Empire user community, means that the ease of detection will vary. Nonetheless, having a greater understanding and awareness of this tool is a step forward in defending against its use by threat actors.

Capabilities

PowerShell Empire enables a threat actor to carry out a range of actions on a victim's machine and implements the ability to run PowerShell scripts without needing powershell.exe to be present on the system Its communications are encrypted and its architecture is flexible.

PowerShell Empire uses "modules" to perform more specific malicious actions. These modules provide the threat actor with a customizable range of options to pursue their goals on the victim's systems. These goals include escalation of privileges, credential harvesting, host enumeration, keylogging, and the ability to move laterally across a network.

PowerShell Empire's ease of use, flexible configuration, and ability to evade detection make it a popular choice for threat actors of varying abilities.

Examples

During an incident in February 2018, a UK energy sector company was compromised by an unknown threat actor. This compromise was detected through PowerShell Empire beaconing activity using the tool's default profile settings. Weak credentials on one of the victim's administrator accounts are believed to have provided the threat actor with initial access to the network.

In early 2018, an unknown threat actor used Winter Olympics-themed socially engineered emails and malicious attachments in a spear-phishing campaign targeting several South Korean organizations. This attack had an additional layer of sophistication, making use of `Invoke-PSImage`, a stenographic tool that will encode any PowerShell script into an image.

In December 2017, APT19 targeted a multinational law firm with a phishing campaign. APT19 used obfuscated PowerShell macros embedded within Microsoft Word documents generated by PowerShell Empire.

Our cybersecurity authorities are also aware of PowerShell Empire being used to target academia. In one reported instance, a threat actor attempted to use PowerShell Empire to gain persistence using a Windows Management Instrumentation event consumer. However, in this instance, the PowerShell Empire agent was unsuccessful in establishing network connections due to the HTTP connections being blocked by a local security appliance.

Detection and Protection

Identifying malicious PowerShell activity can be difficult due to the prevalence of legitimate PowerShell activity on hosts and the increased use of PowerShell in maintaining a corporate environment.

To identify potentially malicious scripts, PowerShell activity should be comprehensively logged. This should include script block logging and PowerShell transcripts.

Older versions of PowerShell should be removed from environments to ensure that they cannot be used to circumvent additional logging and controls added in more recent versions of PowerShell. This page provides a good summary of PowerShell security practices.[10]

The code integrity features in recent versions of Windows can be used to limit the functionality of PowerShell, preventing or hampering malicious PowerShell in the event of a successful intrusion.

A combination of script code signing, application whitelisting, and constrained language mode will prevent or limit the effect of malicious PowerShell in the event of a successful intrusion. These controls will also impact legitimate PowerShell scripts and it is strongly advised that they be thoroughly tested before deployment.

When organizations profile their PowerShell usage, they often find it is only used legitimately by a small number of technical staff. Establishing the extent of this legitimate activity will make it easier to monitor and investigate suspicious or unexpected PowerShell usage elsewhere on the network.

C2 Obfuscation and Exfiltration: HUC Packet Transmitter

Attackers will often want to disguise their location when compromising a target. To do this, they may use generic privacy tools (e.g., Tor) or more specific tools to obfuscate their location.

HUC Packet Transmitter (HTran) is a proxy tool used to intercept and redirect Transmission Control Protocol (TCP) connections from the local host to a remote host. This makes it possible to obfuscate an attacker's communications with victim networks. The tool has been freely available on the internet since at least 2009.

HTran facilitates TCP connections between the victim and a hop point controlled by a threat actor. Malicious threat actors can use this technique to redirect their packets through multiple compromised hosts running HTran to gain greater access to hosts in a network.

In Use

The use of HTran has been regularly observed in compromises of both government and industry targets.

A broad range of threat actors have been observed using HTran and other connection proxy tools to

- Evade intrusion and detection systems on a network,
- Blend in with common traffic or leverage domain trust relationships to bypass security controls,
- Obfuscate or hide C2 infrastructure or communications, and
- Create peer-to-peer or meshed C2 infrastructure to evade detection and provide resilient connections to infrastructure.

Capabilities

HTran can run in several modes, each of which forwards traffic across a network by bridging two TCP sockets. They differ in terms of where the TCP sockets are initiated from, either locally or remotely. The three modes are

- **Server (listen)** – Both TCP sockets initiated remotely;
- **Client (slave)** – Both TCP sockets initiated locally; and
- **Proxy (tran)** – One TCP socket initiated remotely, the other initiated locally, upon receipt of traffic from the first connection.

HTran can inject itself into running processes and install a rootkit to hide network connections from the host operating system. Using these features also creates Windows registry entries to ensure that HTran maintains persistent access to the victim network.

Examples

Recent investigations by our cybersecurity authorities have identified the use of HTran to maintain and obfuscate remote access to targeted environments.

In one incident, the threat actor compromised externally-facing web servers running outdated and vulnerable web applications. This access enabled the upload of webshells, which were then used to deploy other tools, including HTran.

HTran was installed into the ProgramData directory and other deployed tools were used to reconfigure the server to accept Remote Desktop Protocol (RDP) communications.

The threat actor issued a command to start HTran as a client, initiating a connection to a server located on the internet over port 80, which forwards RDP traffic from the local interface.

In this case, HTTP was chosen to blend in with other traffic that was expected to be seen originating from a web server to the internet. Other well-known ports used included:

- Port 53 – Domain Name System
- Port 443 - HTTP over TLS/Secure Sockets Layer
- Port 3306 - MySQL
- By using HTran in this way, the threat actor was able to use RDP for several months without being detected.

Detection and Protection

Attackers need access to a machine to install and run HTran, so network defenders should apply security patches and use good access control to prevent attackers from installing malicious applications.

Network monitoring and firewalls can help prevent and detect unauthorized connections from tools such as HTran.

In some of the samples analyzed, the rootkit component of HTran only hides connection details when the proxy mode is used. When client mode is used, defenders can view details about the TCP connections being made.

HTran also includes a debugging condition that is useful for network defenders. In the event that a destination becomes unavailable, HTran generates an error message using the following format:

```
sprint(buffer, "[SERVER]connection to %s:%d error\r\n", host,
port2);
```

This error message is relayed to the connecting client in the clear. Network defenders can monitor for this error message to potentially detect HTran instances active in their environments.

Mitigations

There are several measures that will improve the overall cybersecurity of your organization and help protect it against the types of tools highlighted in this report. Network defenders are advised to seek further information using the links below.

- Protect your organization from malware.
  See NCCIC Guidance: https://www.us-cert.gov/ncas/tips/ST13-003.
  See UK NCSC Guidance: https://www.ncsc.gov.uk/guidance/protecting-your-organisation-malware.
- Board toolkit: five question for your board's agenda.
  See UK NCSC Guidance: https://www.ncsc.gov.uk/guidance/board-toolkit-five-questions-your-boards-agenda.
- Use a strong password policy and multifactor authentication (also known as two-factor authentication or two-step authentication) to reduce the impact of password compromises.
  See NCCIC Guidance: https://www.us-cert.gov/ncas/tips/ST05-012.
  See UK NCSC Guidance: https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services and https://www.ncsc.gov.uk/guidance/setting-two-factor-authentication-2fa.

- Protect your devices and networks by keeping them up to date. Use the latest supported versions, apply security patches promptly, use antivirus and scan regularly to guard against known malware threats.
  See NCCIC Guidance: https://www.us-cert.gov/ncas/tips/ST04-006.
  See UK NCSC Guidance: https://www.ncsc.gov.uk/guidance/mitigating-malware.
- Prevent and detect lateral movement in your organization's networks.
  See UK NCSC Guidance: https://www.ncsc.gov.uk/guidance/preventing-lateral-movement.
- Implement architectural controls for network segregation.
  See UK NCSC Guidance: https://www.ncsc.gov.uk/guidance/10-steps-network-security.
- Protect the management interfaces of your critical operational systems. In particular, use browse-down architecture to prevent attackers easily gaining privileged access to your most vital assets.
  See UK NCSC blog post: https://www.ncsc.gov.uk/blog-post/protect-your-management-interfaces.
- Set up a security monitoring capability so you are collecting the data that will be needed to analyze network intrusions.
  See UK NCSC Guidance: https://www.ncsc.gov.uk/guidance/introduction-logging-security-purposes.
- Review and refresh your incident management processes.
  See UK NCSC Guidance: https://www.ncsc.gov.uk/guidance/10-steps-incident-management.
- Update your systems and software. Ensure your operating system and productivity applications are up to date. Users with Microsoft Office 365 licensing can use "click to run" to keep their office applications seamlessly updated.
- Use modern systems and software. These have better security built-in. If you cannot move off out-of-date platforms and applications straight away, there are short-term steps you can take to improve your position.
  See UK NCSC Guidance: https://www.ncsc.gov.uk/guidance/obsolete-platforms-security-guidance.
- Manage bulk personal datasets properly.
  See UK NCSC Guidance: https://www.ncsc.gov.uk/guidance/protecting-bulk-personal-data-introduction.
- Restrict intruders' ability to move freely around your systems and networks. Pay particular attention to potentially vulnerable entry points (e.g., third-party systems with onward access to your core network). During an incident, disable remote access from third-party systems until you are sure they are clean.
  See UK NCSC Guidance: https://www.ncsc.gov.uk/guidance/preventing-lateral-movement and https://www.ncsc.gov.uk/guidance/assessing-supply-chain-security.
- Whitelist applications. If supported by your operating environment, consider whitelisting of permitted applications. This will help prevent malicious applications from running.
  See UK NCSC Guidance: https://www.ncsc.gov.uk/guidance/eud-security-guidance-windows-10-1709#applicationwhitelistingsection.
- Manage macros carefully. Disable Microsoft Office macros, except in the specific applications where they are required.
  Only enable macros for users that need them day-to-day and use a recent and fully patched version of Office and the underlying platform, ideally configured in line with the UK NCSC's End User Device Security Collection Guidance and UK NCSC's Macro

Security for Microsoft Office Guidance: https://www.ncsc.gov.uk/guidance/end-user-device-security and https://www.ncsc.gov.uk/guidance/macro-security-microsoft-office.

- Use antivirus. Keep any antivirus software up to date, and consider use of a cloud-backed antivirus product that can benefit from the economies of scale this brings. Ensure that antivirus programs are also capable of scanning Microsoft Office macros.
  See NCCIC Guidance: https://www.us-cert.gov/ncas/tips/ST04-005.
  See UK NCSC Guidance: https://www.ncsc.gov.uk/guidance/macro-security-microsoft-office.
- Layer organization-wide phishing defenses. Detect and quarantine as many malicious email attachments and spam as possible, before they reach your end users. Multiple layers of defense will greatly cut the chances of a compromise.
- Treat people as your first line of defense. Tell personnel how to report suspected phishing emails, and ensure they feel confident to do so. Investigate their reports promptly and thoroughly. Never punish users for clicking phishing links or opening attachments.
  NCCIC encourages users and administrators to report phishing to phishing-report@us-cert.gov.
  See NCCIC Guidance: https://www.us-cert.gov/ncas/tips/ST04-014.
  See UK NCSC Guidance: https://www.ncsc.gov.uk/phishing.
- Deploy a host-based intrusion detection system. A variety of products are available, free and paid-for, to suit different needs and budgets.
- Defend your systems and networks against denial-of-service attacks.
  See UK NCSC Guidance: https://www.ncsc.gov.uk/guidance/denial-service-dos-guidance-collection.
- Defend your organization from ransomware. Keep safe backups of important files, protect from malware, and do not pay the ransom– it may not get your data back.
  See NCCIC Guidance: https://www.us-cert.gov/Ransomware.
  See UK NCSC Guidance: https://www.ncsc.gov.uk/guidance/mitigating-malware and https://www.ncsc.gov.uk/guidance/backing-your-data.
- Make sure you are handling personal data appropriately and securely.
  See NCCIC Guidance: https://www.us-cert.gov/ncas/tips/ST04-013.
  See UK NCSC Guidance: https://www.ncsc.gov.uk/guidance/gdpr-security-outcomes.

Further information: invest in preventing malware-based attacks across various scenarios.
See UK NCSC Guidance: https://www.ncsc.gov.uk/guidance/mitigating-malware.

Additional Resources from International Partners

- Australian Cyber Security Centre (ACSC) Strategies - https://acsc.gov.au/infosec/mitigationstrategies.htm
- ACSC Essential Eight - https://acsc.gov.au/publications/protect/essential-eight-explained.htm
- Canadian Centre for Cyber Security (CCCS) Top 10 Security Actions - https://cyber.gc.ca/en/top-10-it-security-actions
- CCCS Cyber Hygiene - https://www.cse-cst.gc.ca/en/cyberhygiene-pratiques-cybersecurite
- CERT New Zealand's Critical Controls 2018 - https://www.cert.govt.nz/it-specialists/critical-controls/
- CERT New Zealand’s Top 11 Cyber Security Tips for Your Business - https://www.cert.govt.nz/businesses-and-individuals/guides/cyber-security-your-business/top-11-cyber-security-tips-for-your-business/

- New Zealand National Cyber Security Centre (NZ NCSC) Resources - https://www.ncsc.govt.nz/resources/
- New Zealand Information Security Manual - https://www.gcsb.govt.nz/the-nz-information-security-manual/
- UK NCSC 10 Steps to Cyber Security - https://www.ncsc.gov.uk/guidance/10-steps-cyber-security
- UK NCSC Board Toolkit: five questions for your board's agenda - https://www.ncsc.gov.uk/guidance/board-toolkit-five-questions-your-boards-agenda
- UK NCSC Cyber Security: Small Business Guide - https://www.ncsc.gov.uk/smallbusiness

Contact Information

NCCIC encourages recipients of this report to contribute any additional information that they may have related to this threat. For any questions related to this report, please contact NCCIC at

- 1-888-282-0870 (From outside the United States: +1-703-235-8832)
- NCCICCustomerService@us-cert.gov (UNCLASS)
- us-cert@dhs.sgov.gov (SIPRNET)
- us-cert@dhs.ic.gov (JWICS)

NCCIC encourages you to report any suspicious activity, including cybersecurity incidents, possible malicious code, software vulnerabilities, and phishing-related scams. Reporting forms can be found on the NCCIC/US-CERT homepage at http://www.us-cert.gov/.

Feedback

NCCIC strives to make this report a valuable tool for our partners and welcomes feedback on how this publication could be improved. You can help by answering a few short questions about this report at the following URL: https://www.us-cert.gov/forms/feedback.

References

- [1] Australian Cyber Security Centre (ACSC)
- [2] Canadian Centre for Cyber Security (CCCS)
- [3] New Zealand National Cyber Security Centre (NZ NCSC)
- [4] UK National Cyber Security Centre (UK NCSC)
- [5] US National Cybersecurity and Communications Integration Center
- [6] OWASP Top 10 Project
- [7] FireEye Report on China Chopper
- [8] Microsoft Security Advisory
- [9] Microsoft - Best Practices for Securing Active Directory
- [10] Digital Shadows - PowerShell Security Best Practices

Revisions

- October, 11 2018: Initial version

This product is provided subject to this Notification and this Privacy & Use policy.