National Cyber Security Centre

General Security Advisory

GSA-2018-133

The National Cyber Security Centre is hosted within the Government Communications Security Bureau

11 October 2018

Joint report on publicly available hacking tools

Introduction

1) This report is a collaboration based on research provided by the cyber security authorities of five nations: Australia, Canada, New Zealand, the United Kingdom (UK) and the United States of America (USA) [1].

2) This report highlights the use of five publicly available tools which have been used for malicious purposes in recent cyber incidents around the world. The purpose of this report is to provide network defenders and systems administrators with advice about limiting the effectiveness of these tools and detecting their use on a network.

Nature of the tools

3) The individual tools detailed in this report serve as examples of the types of tools used by malicious actors and should not be considered an exhaustive or exclusive list when planning network defence.

4) 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, hacking tools with a variety of functions are widely and publicly available, for use by everyone from skilled penetration testers, hostile state actors and organised criminals through to amateur hackers.

5) These tools have been used to compromise information across a wide range of critical national infrastructure sectors, including health, finance, government and defence. The widespread availability of these tools presents a challenge for network defence and actor attribution.

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

7) 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 an actor to gain access. The tools detailed here come into play once a

compromise has been achieved, enabling attackers to further their objectives within the victim's systems.

Report structure

8) The tools detailed fall into five different categories: Remote Access Trojans, Web Shells, Credential Stealers, Lateral Movement Frameworks, and Command and Control (C2) Obfuscators.

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

10) The report concludes with general advice for improving network defence practices.

Remote access trojans: JBiFrost

11) First observed in May 2015, the JBiFrost Remote Access Trojan (RAT) is a variant of the Adwind RAT, with roots stretching back as far as the Frutas RAT, from 2012.

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

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

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

In use

15) JBiFrost is typically employed by cyber criminals and low-skilled actors but its capabilities could easily be adapted for use by state actors.

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

Capabilities

17) The 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.

18) JBiFrost allows 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.

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

Examples

20) Since early 2018, we have observed an increase not only in JBiFrost 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 in our countries.

21) In early 2017, the Adwind RAT was deployed via spoofed emails designed to look as if they originated from SWIFT network services.

22) Malicious actors have also compromised servers located in our countries, notably Canada, 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.

23) 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

24) 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 in network traffic;
    - Connection attempts to known malicious IP addresses; and
    - Creation of new files and directories with obfuscated or random names.

25) Protection is best afforded by ensuring systems and installed applications are all fully patched and updated. The use of a modern anti-virus program with automatic definition updates and regular system scans will also help ensure the majority of the latest variants are stopped in their tracks. Organisations should ensure they are able to centrally collect anti-virus detections across their estate and investigate RAT detections efficiently.

26) Strict application whitelisting is recommended to prevent infections occurring.

27) The initial infection mechanism for RATs including JBiFrost can be via phishing emails. You can help prevent JBiFrost infections by preventing these phishing emails from reaching your users, by helping users to identify and report phishing emails and by implementing security controls so the malicious email does not compromise your device.

Web Shells: China Chopper

28) China Chopper is a widely available, well-documented web shell, in widespread use since 2012. Web shells are malicious scripts which are uploaded to a target host after an initial compromise and grant an actor remote administrative capability. Once this access is established web shells can also be used to pivot to further hosts within an enterprise.

In use

29) The China Chopper web shell is well-known for its extensive use by hostile actors to remotely access compromised web servers, where it provides file and directory management, and access to a virtual terminal on the compromised device.

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

Capabilities

31) The China Chopper web shell has two main components: the China Chopper client, which is run by the actor, and the China Chopper server, which is installed on the victim web server but is also actor controlled. The web shell client can issue terminal commands and manage files on the victim server. Its MD5 hash is publicly available[2].

Web Shell Client	MD5 Hash
caidao.exe	5001ef50c7e869253a7c152a638eab8a

32) The web shell server is uploaded in plain text and can easily be changed by the actor. This makes it hard to define a specific hash that can identify adversary activity.

33) In the last few months, threat actors have been observed targeting public-facing web servers vulnerable to CVE-2017-3066. The activity was related to a vulnerability in the web application development platform Adobe Cold Fusion, which enabled remote code execution. China Chopper was then intended as the second-stage payload, delivered once servers had been compromised, allowing an actor remote access to the victim host.

34) After successful exploitation of a vulnerability on the victim machine, the text-based China Chopper web shell is placed on the victim web server. Once uploaded, the web shell server can be accessed by the actor at any time, using the client application. Once successfully connected, the actor proceeds to manipulate files and data on the web server.

35) 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,

editing, deleting, copying, renaming, and even changing the timestamp of existing files.

Detection and protection

36) The most powerful defence against a web shell is to ensure all the software running on public facing web servers is up to date with security patches applied. It is important to audit custom applications for common web vulnerabilities.

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

38) While the China Chopper web shell server upload is plain text, commands issued by the client are Base64 encoded, although this is easily reversible.

39) 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.

40) The most effective way to detect and mitigate China Chopper is on the host itself (specifically on public-facing web servers within the organisation). 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[3].

41) To detect web shells more broadly, network defenders should focus on detecting either suspicious process execution on web servers (for example PHP binaries spawning processes) or 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 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.

42) It is also recommended to use web access logs as a source of monitoring, for example, through traffic analytics. Observing new, unexpected pages or changes in traffic patterns can act as an early indicator.

Credential stealer: Mimikatz

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

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

45) Although it was not originally intended as a hacking tool, in recent years Mimikatz has emerged as a common tool used by multiple actors to obtain credentials from networks. Its use in many compromises worldwide has prompted numerous organisations across multiple sectors to re-evaluate network defences.

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

In use

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

48) Our cyber authorities have observed widespread use of Mimikatz among hostile actors, including organised crime and state actors.

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

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

Capabilities

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

52) The tool can obtain LAN Manager and NTLM hashes, certificates, and long-term keys on Windows XP (2003) through to Windows 8.1 (2012r2). In addition, the tool can also perform pass-the-hash or pass-the-ticket tasks and build Kerberos Golden tickets.

53) Many of Mimikatz's features can be automated with scripts, such as PowerShell, allowing an actor to rapidly exploit and traverse a compromised network. Furthermore, when operating in memory through the freely available, yet

powerful, 'Invoke-Mimikatz' PowerShell script, Mimikatz activity is very difficult to isolate and identify.

Examples

54) Mimikatz has been used across multiple incidents by a broad range of actors for several years. Notably in 2011, Mimikatz was used by unknown hackers 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.

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

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

Detection and protection

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

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

59) Credential Guard will be enabled by default if:
- The hardware meets Microsoft's Windows Hardware Compatibility Programme Specifications and, Policies for Windows Server 2016 and Windows Server Semi-Annual Branch; and
- The server is not acting as a Domain Controller.

60) It is important to verify your physical and virtualised servers meet Microsoft's minimum requirements for each release of Windows 10 and Windows Server.

61) Password reuse across accounts, particularly administrator accounts, makes pass-the-hash attacks far simpler. Organisations should set user policies which discourage password reuse, even across common level accounts on a network. The freely available Local Admin Password Solution (LAPS) from Microsoft can allow easy management of local admin passwords, preventing the need to set and store passwords manually.

62) Network administrators should monitor and respond to unusual or unauthorised account creation or authentication to prevent Golden Ticket exploitation or network persistence and lateral movement. For Windows, tools such as Microsoft ATA and Azure ATP can help with this.

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

64) Most up-to-date anti-virus tools will detect and isolate non-customised Mimikatz use and should therefore be in use to detect these instances. However, hostile actors can sometimes circumvent anti-virus systems by running the tool in memory, or by slightly modifying the original code of the tool. Wherever Mimikatz is detected, organisations are recommended to perform a rigorous investigation as it almost certainly indicates an actor is actively present in the network, rather than an automated process at work.

65) A number of Mimikatz's features rely on exploitation of administrator accounts. Therefore, organisations should ensure administrator accounts are issued on an as-required basis only. Where administrative access is required, organisations should develop Privilege Access Management principles.

66) Since Mimikatz can only capture the accounts of those logged into to a compromised machine, privileged users (such as domain admins) should avoid logging into machines with their privileged credentials. Detailed information on securing active directory is available from Microsoft.

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

Lateral movement frameworks: PowerShell Empire

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

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

70) The tool provides an 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, Empire can be difficult to detect on a network using traditional anti-virus tools.

In use

71) PowerShell Empire has become increasingly popular among hostile state actors and organised criminals. In recent years, its use has been observed in incidents globally and across a wide range of sectors.

72) Initial exploitation methods vary between compromises, and actors can configure the Empire Framework uniquely for each scenario and target.

73) This, in combination with the wide range of skill and intent within the Empire user community, means 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 malicious actors.

Capabilities

74) Empire enables an 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 flexible.

75) Empire uses modules to perform more specific, malicious actions. These provide the actor with a customisable range of options to pursue their goals on the victim's systems. These include escalation of privileges, credential harvesting, host enumeration, key-logging and the ability to move laterally across a network.

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

Examples

77) During an incident in February 2018, a UK energy sector company was compromised by an unknown actor. This compromise was detected through Empire's 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 actor with initial access to the network.

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

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

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

Detection and protection

81) Identifying malicious PowerShell activity can be difficult, due to the prevalence of legitimate PowerShell on hosts and its increased use in maintaining a corporate environment. Organisations are strongly recommended to log PowerShell including script block logging and PowerShell transcripts in order to identify potentially malicious scripts.

82) Older versions of PowerShell should be removed from environments to ensure they cannot be used to circumvent additional logging and controls added in more recent versions of PowerShell. The Digital Shadows blog provides a good summary of PowerShell security practices.

83) The code integrity features of 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.

84) 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 scripts and it is strongly advised they are thoroughly tested before deployment.

85) When organisations profile their PowerShell usage, they often find use is limited to a few cases or hosts. As such, it may be reasonably low effort to monitor and investigate suspicious or unexpected PowerShell usage.

C2 obfuscation and exfil: HTran

86) Actors will often want to disguise their location when compromising a target. To do this, they may use generic privacy tools such as TOR, or more specific tools to obfuscate their location.

87) 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 actor's communications within victim networks. The tool has been freely available on the internet since at least 2009.

88) HTran facilitates TCP connections between the victim and a hop point controlled by an actor. Malicious cyber 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

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

90) A broad range of cyber 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;
- Create peer-to-peer or meshed C2 infrastructure to evade detection and provide resilient connections to infrastructure.

Capabilities

91) 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.

92) 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 HTran maintains persistent access to the victim network.

Examples

93) Recent investigations by our cyber security authorities have identified the use of HTran to maintain and obfuscate remote access into targeted environments.

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

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

96) This 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.

97) 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:
- 53 - DNS
- 443 - HTTP over TLS/SSL
- 3306 – MySQL

98) By using HTran in this way, the actor was able to use RDP for several months without being detected.

Detection and protection

99) Actors 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 installing malicious applications.

100) Networking monitoring and firewalls can help detect and prevent unauthorised connections from tools such as HTran.

101) In some of the samples that have been analysed, 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.

102) HTran also includes a debugging condition that is useful for network defenders. In the event 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);`

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

General mitigation guidance

104) There are several measures that will improve the overall cyber security of an organisation and help protect it against the types of tools highlighted by this report. Network defenders are advised to seek further information using the links below.

New Zealand National Cyber Security Centre

- Resources and Incidents
  https://www.ncsc.govt.nz/resources/
  https://www.ncsc.govt.nz/incidents/

Government Communications Security Bureau

- Information Security Manual
  https://www.gcsb.govt.nz/the-nz-information-security-manual/

CERT NZ

- Critical Controls 2018
  https://www.cert.govt.nz/it-specialists/critical-controls/
- Top 10 cyber tips for your business
  https://www.cert.govt.nz/business-and-individuals/guides/cyber-security-your business/top-11-cyber-security-tips-for-your-business/

UK National Cyber Security Centre Resources:

- Protect Your Organisation From Malware
  https://www.ncsc.gov.uk/guidances/protecting-your-organisation-malware
- 10 Steps to Cyber Security
  https://www.ncsc.gov.uk/guidance/10-steps-cyber-security

Australian Cyber Security Centre

- Mitigation Strategies
  https://acsc.gov.au/infosec/mitigationstrategies.htm
- Essential Eight
  https://acsc.gov.au/publications/protect/essential-eight-explained.htm

Canadian Centre for Cyber

- Top 10 Security Strategies
  https://cse-cst.gc.ca/en/top10
- Cyber hygiene
  https://www.cse-cst.gc.ca/en/cyberhygiene-pratiques-cybersecurite

US National Cybersecurity and Communications Integration Center

- Homepage
  https://www.dhs.gov/national-cybersecurity-and-communications-integration-center

Footnotes:

[1] The Australian Cyber Security Centre (ACSC), the Canadian Centre for Cyber Security (CCCS), the New Zealand National Cyber Security Centre (NZ NCSC), the UK National Cyber Security Centre (UK NCSC) and the US National Cybersecurity and Communications Integration Center (NCCIC).

[2] Originally posted on hxxp://www.maicaidao.com

[3] A range of useful commands and signatures for tracking China Chopper can be found at www.fireeye.com/blog/threat-research/2013/08/breaking-down-the-china-chopper-web-shell-part-ii.html

The NCSC can be contacted by email via ***info@ncsc.govt.nz****.*
We encourage you to contact us at any time if you require any further assistance or advice.