# Dynamite Panda APT Group - Brandefense

Published: 2022-08-08 · Archived: 2026-04-05 19:46:08 UTC

## Threat Group ID

| | |
|---|---|
| **Country** | |
| **Sponsor** | State-sponsored, PLA Navy |
| **First Seen** | 2009 |
| **Motivation** | Information theft & Espionage |
| **Methods** | Flash 0-days, Malware, Phishing Email |

The threat group APT18, operating since 2009, is referenced by various security providers with the following names.

- **APT18** (Mandiant)
- **Wekby** (Palo Alto)
- **Dynamite Panda** (CrowdStrike)
- **Scandium** (Microsoft)

Although not sure, we thought the APT18 might be related to Night Dragon and/or Covert Grove groups.

## Vision, Mission, and Motivation

Operations conducted by the Chinese state-sponsored threat actor APT18 are supported by the People's Liberation Army Navy (PLA Navy) and have been active globally since 2009.

APT18 has been active for years and targets the health, telecommunications, defense, high technology sectors, and human rights groups. It is also known that the group engages in information theft and espionage activities from the targeted sectors.

## Targeted Countries

APT18 has focused its activities on the United States (USA).

Figure 1: Dynamite Panda (APT18) APT Group Targeted Countries

## Targeted Industries

APT18 ran a Community Health Systems campaign that resulted in a data breach. Turning to medical espionage, APT18 seized patient data to target intelligence on medical device development.

APT18 has campaigned for the telecommunications, defense, and high-tech industries serving the United States. APT18 used the Flash 0-day exploit and HTTPBrowser malware developed by the HackingTeam technology company in these campaigns.

## Operations

### 2014

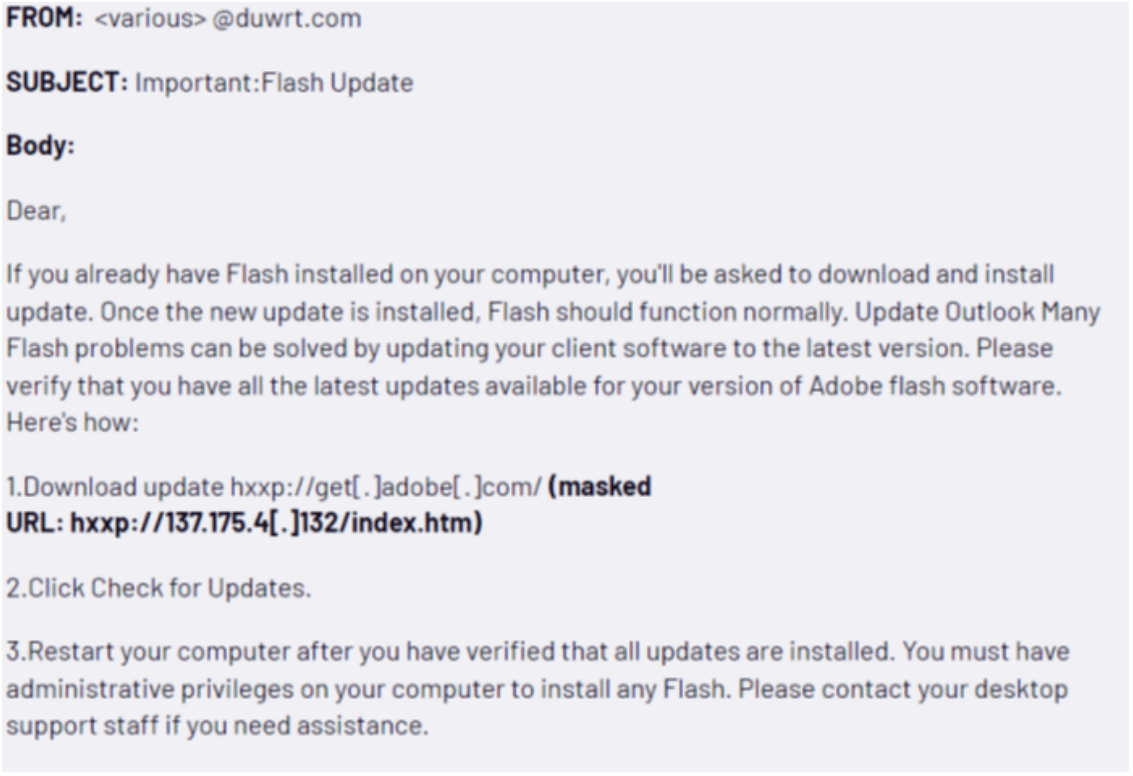
- **Community Health Systems Data Breach**

APT18 has managed to steal information from vulnerable health systems such as patient information, medical device information, and intellectual property rights that could be used to achieve high international standards in various industries and for China’s profit. Among the information obtained from the health systems, it was announced that the identity information of 4.5 million patients was seized by the attackers and the production of medical devices.

**2015-16**

- **Phishing Campaign for Organizations in the United States**

APT18 has carried out attacks against many US-based organizations where Flash 0-day exploit, HTTPBrowser, and Pisloader malware are distributed via phishing emails and URLs.


**FROM:** <various> @duwrt.com

**SUBJECT:** Important:Flash Update

**Body:**

Dear,

If you already have Flash installed on your computer, you'll be asked to download and install update. Once the new update is installed, Flash should function normally. Update Outlook Many Flash problems can be solved by updating your client software to the latest version. Please verify that you have all the latest updates available for your version of Adobe flash software. Here's how:

1.Download update hxxp://get[.]adobe[.]com/ **(masked URL: hxxp://137.175.4[.]132/index.htm)**

2.Click Check for Updates.

3.Restart your computer after you have verified that all updates are installed. You must have administrative privileges on your computer to install any Flash. Please contact your desktop support staff if you need assistance.

Figure 2: An example of an APT18 phishing email using the CVE-2015-5119 vulnerability

## Mitre ATT&CK Threat Matrix

It defines the techniques, tactics, and procedures identified in attacks by the APT18 threat group.

| Tactic ID | Tactic Name | Technique ID | Technique Name |
|---|---|---|---|
| TA0001 | Initial Access | T1133<br>T1566 | External Remote Services<br>Phishing |
| TA0002 | Execution | T1059.003<br>T1053.002 | Command and Scripting Interpreter: Windows Command Shell<br>Scheduled Task/Job: At |
| TA0003 | Persistence | T1547 | Boot or Logon Autostart Execution |

| | | | |
|---|---|---|---|
| | | T1078 | Valid Accounts |
| TA0005 | Defense Evasion | T1070.004<br>T1027 | Indicator Removal on Host: File Deletion<br>Obfuscated Files or Information |
| TA0007 | Discovery | T1083<br>T1082 | File and Directory Discovery<br>System Information Discovery |
| TA0011 | Command and Control | T1071.001<br>T1071.004<br>T1105 | Application Layer Protocol: Web Protocols<br>Application Layer Protocol: DNS<br>Ingress Tool Transfer |

**External Remote Services**

Phishing credentials are the next best option when APT18 fails its malware campaigns. APT18 uses these credentials against resources such as Open Terminal Service / RDP, Web / SSL VPN, and Citrix/Moka5/VNC that provide remote network access.

**Phishing**

APT18 used phishing emails containing malicious URL links with the theme “Flash Update” in some of its campaigns.

**Command and Scripting Interpreter: Windows Command Shell**

APT18 takes advantage of the Windows Command Shell (cmd.exe) feature to execute commands on the target machine. For example;

cmd.exe /c reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v lsm /t reg_sz /d “%appdata%\lsm.exe” /f

**Scheduled Task/Job: At**

The threat actor used scheduled tasks via the at.exe application to move horizontally within the target infrastructure. As part of an example scenario, two files are created for the job at approximately the same time, as follows.

C:\Windows\System32\Tasks\At1

C:\Windows\Tasks\At1.job

The first file is an XML file that is read and can be opened and viewed in a text editor to use the scheduled task. The second file is binary.

**Boot or Logon Autostart Execution**

APT18 uses the following registry key to ensure persistence on the target system.

HKCU\Software\Microsoft\Windows\CurrentVersion\Run

When the first stage malware (dropper) runs, the name of the executable file that will be used to provide persistence is written to this registry path.

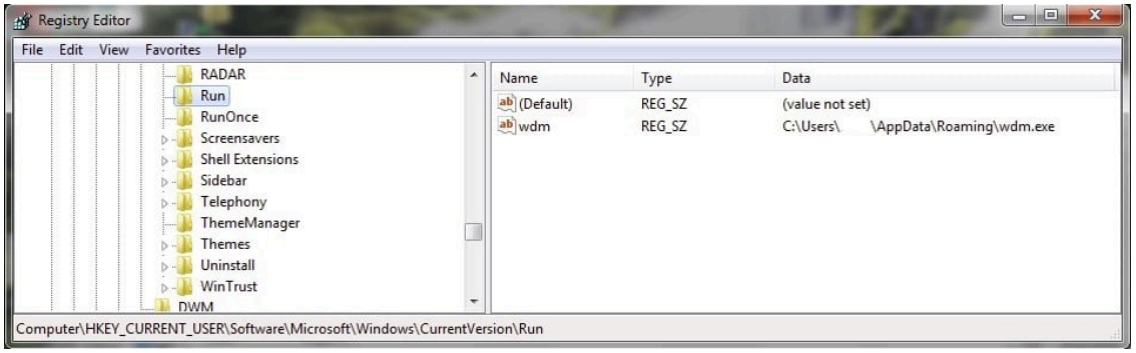



Figure 3: Run registry key record used for persistence

**Valid Accounts**

APT18 uses compromised account information to access services that provide remote network access. Threat actors usually obtain this account information through phishing attacks or data leaked from data-breached systems.

**Indicator Removal on Host: File Deletion**

Tools and scripts to be run by tasks scheduled by APT18 are deleted from the target system. However, even if it deletes after the used files, the remnants of the functionality remain on the target system, reducing the chances of the threat actor being hidden.

**Obfuscated Files or Information**

APT18 has hidden the additional payload data contained in the Pisloader malware used in its campaigns with the Return-Oriented-Programming (ROP) technique. This process involves using garbage assembly instructions that will not affect the program flow and PUSH/RET assembly instructions to navigate to the malicious code location that will run.

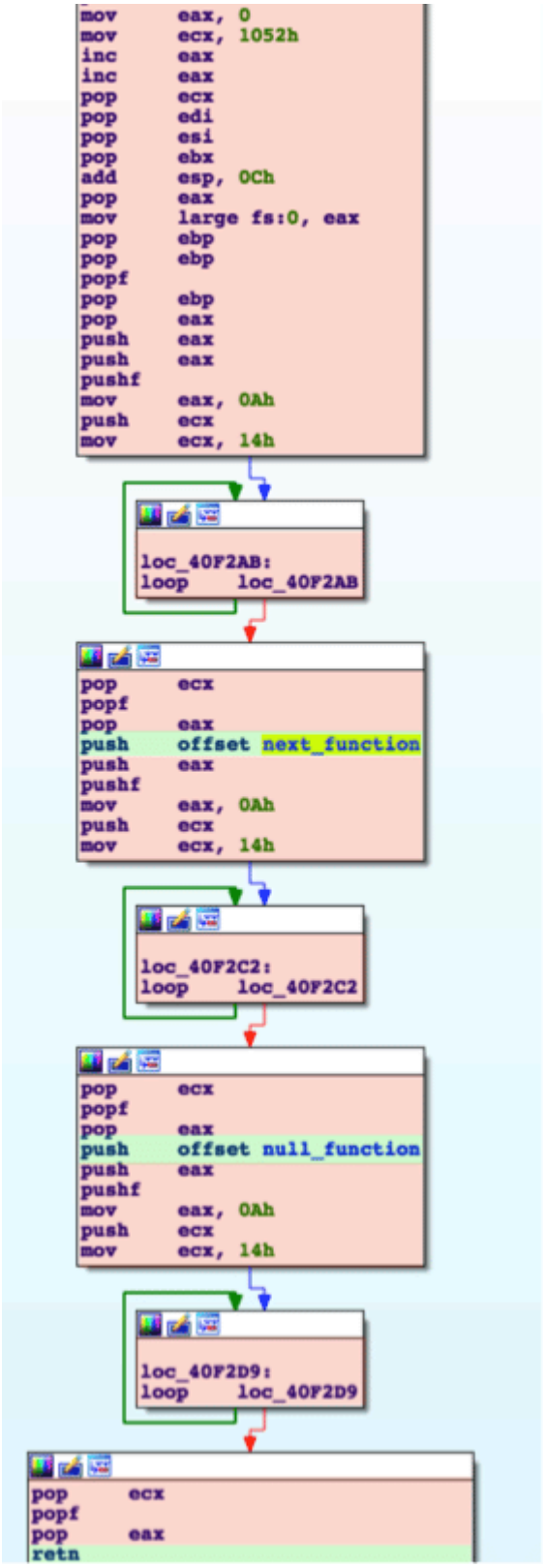



Figure 4: Code fragment using ROP technique to hide payload

**File and Directory Discovery**

The Pisloader malware used by APT18 supports a command called list. This command can list file information for specific directories. For example, listing the contents of the C:\ directory will result in an output like the one

below.

**[+] Sending Command:** list C:\ | Encoded: CNRUXG5BAIM5FY

**[+] Raw Data Received:** QKTUMGAGLAGB6CIUTFMN4WG3DFFZBGS3T4GIYDCNJPGAZS6MRW

**[+] Raw Data Received:** EKNPMGAGL0EAYTIORUGA5DKN34GB6DEMS6

**[+] Raw Data Received:** RKMAMGAGLAGF6GC5LUN5SXQZLDFZRGC5D4GIYDAOJPGA3C6MJQ

**[+] Raw Data Received:** NMSIMGAGL0EAZDCORUGI5DEMD4GI2HYMZSLY

**[+] Raw Data Received:** OHRWMGAGLAGB6EE33POR6DEMBRGUXTAMZPGI3CAMJWHIZDIORQ

**[+] Raw Data Received:** DPDUMGAGL0GJ6DA7BSGJPA

**[+] Raw Data Received:** WIKGMGAGLAGF6GE33PORWWO4T4GIYDCNBPGA3C6MRYEAYDAORS

* Truncated*

**[+] Decoded Data Received:** 0|$Recycle.Bin|2015/03/26 14:40:57|0|22^1|autoexec.bat|2009/06/10 21:42:20|24|32^0|Boot|2015/03/26 16:24:02|0|22^1|bootmgr|2014/06/28 00:21:34|391640|39^1|BOOTSECT.BAK|2015/03/26 16:35:39|8192|39^1|config.sys|2009/06/10 21:42:20|10|32^0|Documents and Settings|2009/07/14 04:53:55|0|9238^1|Example.log|2016/02/09 20:17:55|0|32^1|pagefile.sys|2016/04/25 14:09:20|1660411904|38^0|PerfLogs|2009/07/14 02:37:05|0|16^0|Program Files|2016/02/29 15:59:43|0|17^0|ProgramData|2016/02/02 17:28:04|0|8210^0|Python27|2016/02/25 16:39:37|0|16^0|Recovery|2015/03/26 14:39:57|0|8214^0|System Volume Information|2016/02/29 16:00:19|0|22^0|Users|2015/03/26 14:39:58|0|17^0|Windows|2016/02/12 10:20:21|0|16^^end^

**System Information Discovery**

The Pisloader malware used by APT18 supports a command called **sifo**. This command can collect system information from the target machine. For example;

**[+] Sending Command:** sifo | Encoded: CONUWM3Y

**[+] Raw Data Received:** FUBWMGAGIANQ6TCNZSFYYTMLRRFYYTKMZGMM6VOSKOFVGEUTCW

**[+] Raw Data Received:** PGHRMGAGIBGJHEWSKPJNICAW2KN5ZWQICHOJ2W46TXMVUWOXJG

**[+] Raw Data Received:** MMAZMGAGI0N46TMLBRFQZTE

**[+] Decoded Data Received:** l=172.16.1.153&c=WIN-LJLV2NKIOKP [Josh Grunzweig]&o=6,1,32

**Application Layer Protocol: Web Protocols & DNS**

APT18 can use HTTP and DNS protocols to communicate with C2 servers while extracting the captured information from the target system. DNS as C2 allows Pisloader malware to circumvent certain security products

that do not correctly control this traffic.

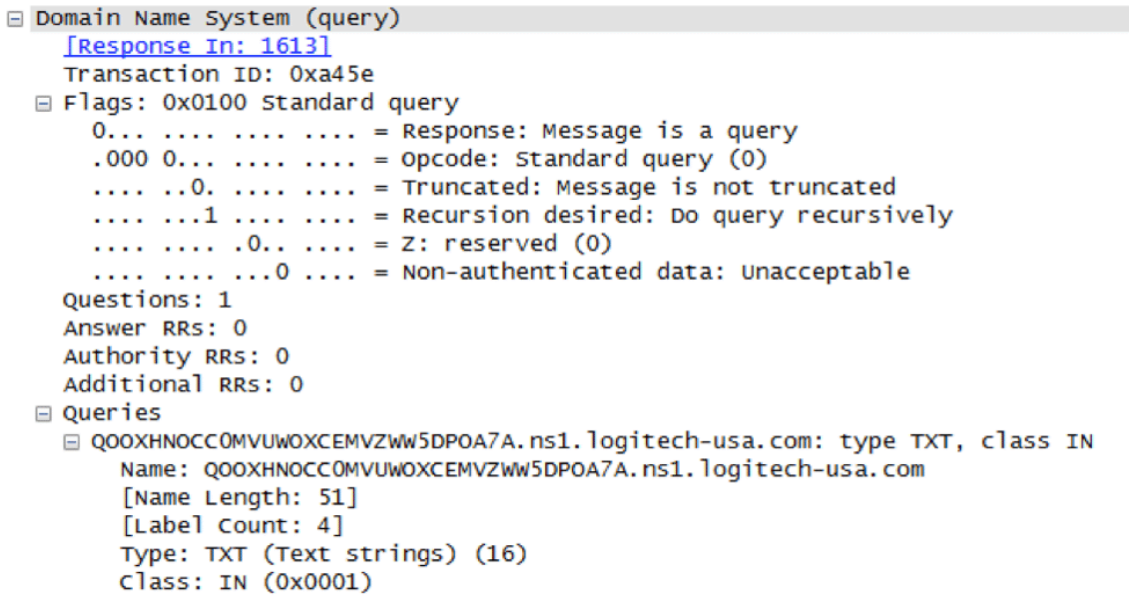



Figure 5: DNS query for TXT record by malware

The DNS TXT record is used to exchange commands to be executed on the target system between the malware and C2.

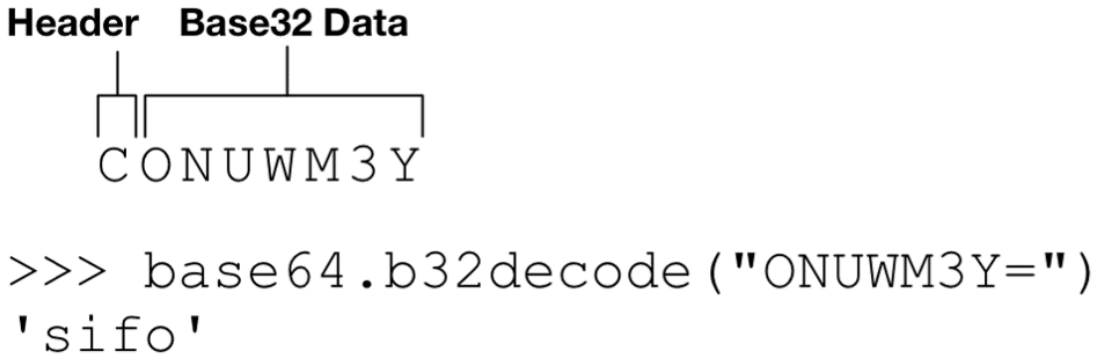



Figure 6: An example TXT response sent by C2

**Ingress Tool Transfer**

The Pisloader malware used by APT18 supports a command called upload. The threat actor can install additional files on the target machine with this command.

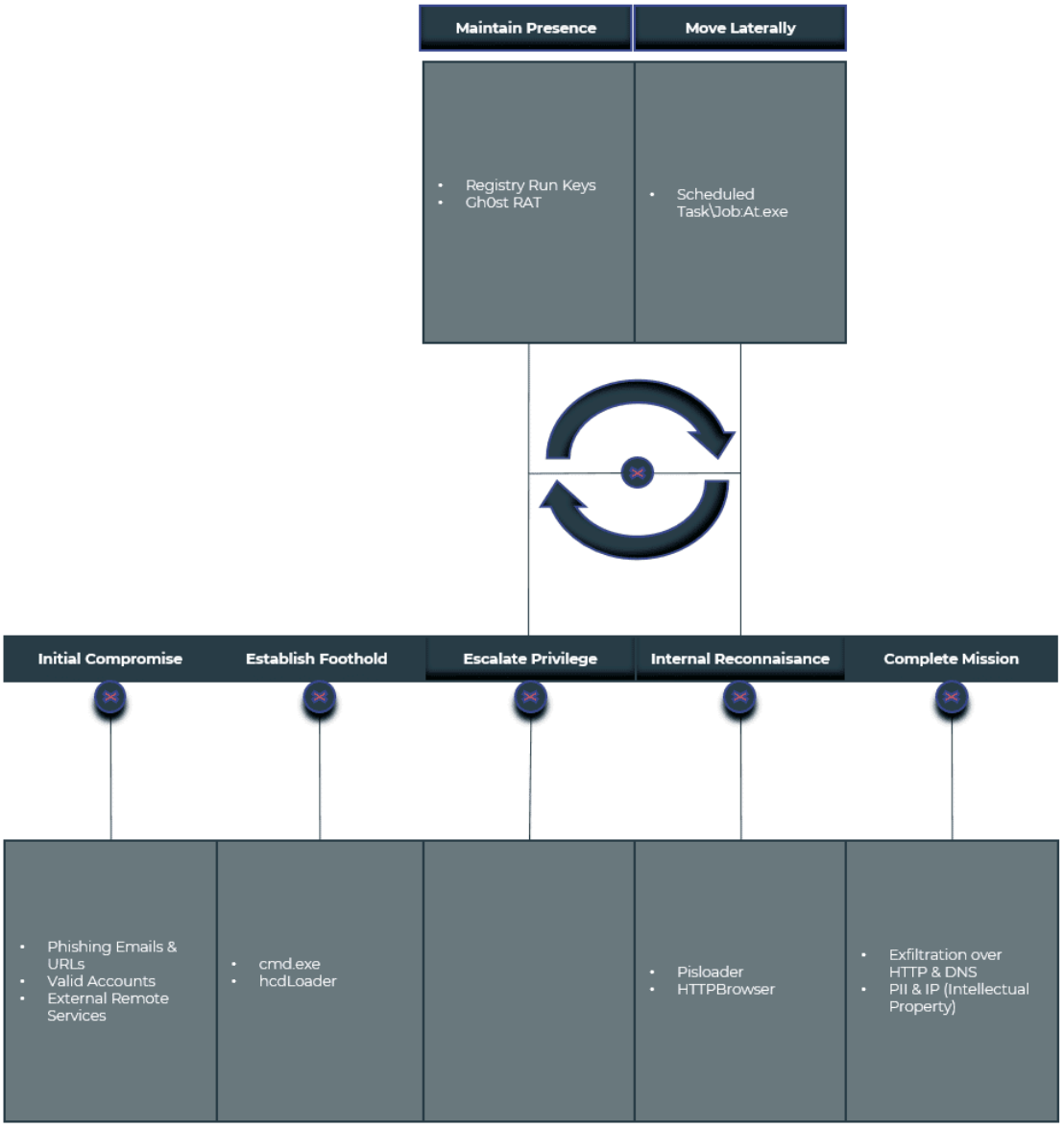



Figure 7: Attack Lifecycle

## Conclusion & Recommendations

Now you have detailed information about the toolkits, malware, techniques, tactics and procedures, targeted countries, and sectors used by the Chinese state-backed threat actor APT18 group in its attacks. By checking whether you are among the potential targets of the APT18 threat actor against the information contained in the report, it is intended to provide scope for what types of interactions you should look for, from gaining initial access to actions taken on compromised systems.

- Network Intrusion Prevention systems, which use network signatures to identify traffic for attacking malware, can help reduce network-level malware activities.
- You can filter DNS requests for unknown, untrusted, or known bad domains and resources. Resolving DNS requests can also detect attempts to hide data within DNS packets.
- You might consider blocking code execution on a system through application control and/or script blocking.

- Disable or block any remotely available services that may be unnecessary.
- You can restrict access to remote services through VPN and other remote access systems.
- Consider using strong two-factor or multi-factor authentication to reduce the threat actor’s ability to use stolen credentials.
- You can prevent direct remote access to internal systems using proxy, gateway, and firewalls.
- You can monitor the commands and arguments executed for actions that can be used to unlink, rename, or delete files.

---