



March 2022

Updates released in March of 2022 to Cisco cloud-based machine learning global threat alerts:

- [Additional Threat Detections, on page 1](#)

Additional Threat Detections

We've added more new threat detections to our portfolio, including:

- Cyclops Blink
- FormBook
- Gamaredon
- MuddyWater

Numerous lower-risk threat detections have also been enriched.

Cyclops Blink

Cyclops Blink is a malicious Linux ELF executable, targeting Small Office / Home Office network devices. It has 4 built-in modules, allowing it to upload and download files, discover system information (T1082) and update malware versions. More modules can be installed using C2 commands. It maintains persistence through a firmware update process (T1542.001) and executes downloaded files through Linux API calls (T1059.004). Each sample contains a list of IP addresses and port numbers (T1571). After execution, it modifies the system firewall (T1562.004) to enable C2 communication through these IP addresses and ports.

To see if Cyclops Blink has been detected in your environment, click [Cyclops Blink Threat Detail](#) to view its details in global threat alerts.

Figure 1:

Cyclops Blink

Linux based malware targeting SOHO network devices

High Severity
Confirmed
5+ affected assets in 5+ companies

Cyclops Blink is a malicious Linux ELF executable, targeting Small Office / Home Office network devices. It has 4 built-in modules, allowing it to upload/download files, discover system information (T1082) and update malware version. More modules can be installed upon C2 commands. It maintains persistence through firmware update process (T1542.001) and executes downloaded files through Linux API calls (T1059.004). Each sample contains a list of IP addresses and port numbers (T1571). After execution, it modifies system firewall (T1562.004) to enable C2 communication through these addresses and ports.

Category: Malware - botnet

FormBook

FormBook is an info-stealer and form-grabber that can exfiltrate information from an infected device (TA0010). This malware is distributed using spam emails with malicious attachments (T1566.001). FormBook is malware-as-a-service, an attacker can buy a PHP control panel, with customization options for features and settings. A newer version is also known as XLoader. The malware can access credentials (TA0006), capture screenshots (T1113), monitor clipboard (T1115), log keystrokes (T1056.001), clear browser cookies, download and execute files, reboot and shut down the system, and more.

To see if FormBook has been detected in your environment, click [FormBook Threat Detail](#) to view its details in global threat alerts.

Figure 2:

FormBook

Personal data stealer

High Severity
Confirmed
5+ affected assets in 5+ companies

FormBook is an info stealer and form grabber that can exfiltrate information from the infected device (TA0010). This malware is distributed using spam emails with malicious attachments (T1566.001). FormBook is Malware-as-a-service, an attacker can buy a PHP control panel, with customization options for features and settings. A newer version is also known as XLoader. The malware can perform credentials access (TA0006), screenshots capturing (T1113), clipboard monitoring (T1115), keystrokes logging (T1056.001), clearing browser cookies, downloading and executing files, rebooting and shutting down the system, and more.

Category: Malware - data leak

Gamaredon

Gamaredon, also known as Primitive Bear, is a nation state actor often targeting government organizations for cyber espionage. After rising tensions between Russia and the Ukraine, group activities have increased. Gamaredon often leverages malicious office files (T1204.002), distributed through spearphishing (T1566.001), as the first stage of their attacks. They are known to use the Powershell (T1059.001) beacon called PowerPunch to download and execute (T1204.002) malware for the ensuing stages. Pterodo (S0147) and QuietSieve are popular malware families they deploy for stealing information (TA0010) and various other actions.

To see if Gamaredon activity has been detected in your environment, click [Gamaredon Activity Threat Detail](#) to view its details in global threat alerts.

Figure 3:

Gamaredon Activity

Russian State Actor with Cyberespionage Capabilities

Critical Severity
Confirmed
10+ affected assets in 5+ companies

Gamaredon, also known as Primitive Bear, is a nation state actor often targeting government organizations for Cyberespionage. After rising tensions between Russian-Ukrainian relations, group activities has been observed to increase. Gamaredon often leverages malicious office files (T1204.002) distributed through spearphishing (T1566.001) as first stage of their attacks. They are known to use Powershell (T1059.001) beacon called PowerPunch to download and execute (T1204.002) malware for further stages. Pterodo (S0147) and QuietSieve are popular malware families they deploy for stealing information (TA0010) and various actions on objective.

Category: Attack Pattern - malicious file communication

MuddyWater

MuddyWater is an advanced persistent threat (APT) group that seems to be based in Iran and has been active since 2017. The attack vector is usually spear-phishing emails (T1566.001) to drop files into the victim's device. Some of the techniques used by MuddyWater include side-loading DLLs (T1574.002) and the use of PowerShell scripts (T1059.001). MuddyWater activities are related to espionage, stealing of data, and ransomware attacks.

To see if MuddyWater activity has been detected in your environment, click [MuddyWater Activity Threat Detail](#) to view its details in global threat alerts.

Figure 4:

Activity related to MuddyWater

Malicious activity related to Muddy Water APT group

Critical Severity

Confirmed

10+ affected assets in 5+ companies

Muddy Water is an APT group that seems to be based in Iran and has been active since 2017. The attack vector is usually spear-phishing emails (T1566.001) to drop files in the victim's device. Some of the techniques used by Muddy Water includes side-loading DLLs (T1574.002), use of PowerShell scripts (T1059.001). Muddy Water activities are related to espionage, stealing of data and ransomware attacks.

Category: Attack Pattern - data leak