Timelining GRIM SPIDER's Big Game Hunting Tactics | CrowdStrike

By Eric.John.and.Harlan.Carvey

Archived: 2026-04-05 13:05:36 UTC

The tactic of singling out large organizations for high ransom payouts has signaled a shift in the eCrime ecosystem, with a focus on targeted, low-volume, high-return criminal activity. It's a type of cybercrime operation we refer to as "big game hunting." CrowdStrike® Services has observed that the time from gaining initial access in the victim's environment to launching ransomware can range from days to months. During this time, there are several opportunities to detect an adversary in the process of learning your network – and potentially stop their attack before it occurs. This blog uses the MITRE ATT&CK™ Framework to map WIZARD SPIDER and GRIM SPIDER tactics, techniques and procedures (TTPs) observed across several CrowdStrike Services engagements, illustrating how an attack unfolds and the different stages involved.

Increased Activity Observed

An uptick in activity from GRIM SPIDER, a subgroup of the criminal enterprise CrowdStrike Intelligence tracks as WIZARD SPIDER, has led to the identification of consistent actions employed to carry out their attacks. As part of their initial compromise — usually as a download from a spam email — they gain a foothold with their modular TrickBot malware, which was developed and is principally operated by WIZARD SPIDER. Once TrickBot is executed, new enumeration modules are downloaded onto the compromised machine to facilitate WIZARD SPIDER's spread in search of credentials with the aim of gaining access to the domain controller. The criminal actors use RDP to perform lateral movement and explore the victim environment, with an end result of gaining access to the domain controller. Once this access has been achieved, GRIM SPIDER is able to deploy the Ryuk ransomware to the entire network. These observations come from system log data, CrowdStrike Falcon®® sensor telemetry, and the output of the Falcon Forensic Collector (a customized version of CrowdStrike's freely distributed community tool, CrowdResponse).

Initial Access and Execution

While the use of malicious attachments in spam emails is the most common initial access vector — determined across multiple CrowdStrike investigations — the available data from these investigations had either been removed or "aged off" the systems (i.e., dispersed due to the passage of time) before CrowdStrike Services could confirm the source. In cases where spam attachments could be verified — once a user has opened the attachment and enabled macro functionality — a PowerShell script downloads either Emotet, Bokbot or Trickbot, with the end payload being TrickBot. Within hours of TrickBot being executed, additional TrickBot modules are installed for network reconnaissance and credential theft.

Persistence

Trickbot is installed as a scheduled task, using names like “WinDotNet,” “GoogleTask,” or “Sysnetsf” to masquerade as legitimate-appearing processes. These point to various copies of TrickBot installed in the system, usually within the user profile under `%USER_DIR%\AppData\Roaming\` or a subdirectory. The subdirectories also use similarly misleading names like “WinDefrag” or “NetSocket” to appear innocuous. TrickBot may also be installed as a service with names like “ControlServiceA” that points to a copy in the system drive root. WIZARD SPIDER uses a module named NewBCtestnDll64 as a reverse SOCKS proxy that allows for the download and installation of the open source

PowerShell Empire post-exploitation framework. These services launch a Base64-encoded PowerShell script that will fetch the full PowerShell Empire code from a remote IP. Each instance of the Updater service connects to a single IP address, and multiple versions may be added at the same time, pointing to different IPs and requesting a `.php` resource.

Credential Access

The TrickBot module used for credential harvesting is `pwgrab64`. As with all modules launched by the TrickBot core, `pwgrab64` is installed into a subfolder, usually named either “modules” or “data,” and modified the following registry value: `Registry Key: HKLM\System\CurrentControlSet\Control\SecurityProviders\WDigest` `Value: UseLogonCredential` `Data: 1` Setting the “UseLogonCredential” value to “1” configures the Windows operating system to store credentials as cleartext in memory, where they can then be retrieved via the use of credential dumping tools. Older versions of the pwgrab module has a limited scope that targets mail clients, web browsers, FileZilla and WinSCP. Newer versions also dump passwords for applications such as PuTTY, VNC and RDP. In the investigations reviewed by CrowdStrike Services, the `UseLogonCredential` registry value was observed having been set to “1” on systems throughout the infrastructure, often in conjunction with TrickBot’s first deployment to the host.

Discovery

The TrickBot modules used for discovery include `networkdll` and `psfin`. TrickBot downloads modules for collecting local system information and scouting the network, primarily part of the `networkdll` module. This module has a battery of command line, WMI and LDAP queries to gather information, and then exfiltrate the data to GRIM SPIDER for review. The `psfin` module has a similar purpose but specifically searches for financial and point-of-sales indicators.

Lateral Movement

Following initial access, GRIM SPIDER focuses on collecting credentials from the compromised hosts and uses existing RDP in an attempt to get a domain administrator account and access to the Windows Domain Controller. This process can take several iterations of harvesting credentials, connecting to new systems and establishing persistence. For the incidents observed, this stage of the attack can last from a few days to a few months. GRIM SPIDER also has been observed selecting a server to be the primary staging point. Subsequently, the adversary copies the Microsoft SysInternals PSTools archive to this system, and executes `PsExec.exe`, a utility that allows them to move laterally and execute commands on other Windows systems within the infrastructure. Using this common administrator tool, GRIM SPIDER can traverse the network, remotely installing TrickBot and adding

persistence to new targets. TrickBot also has the `shareDll` module for propagating to other hosts using the current, active user credentials.

Deploying Ransomware

Once GRIM SPIDER has gained access to credentials and a Domain Controller, or other host management server, they would then stage the Ryuk ransomware on that system and deploy to targets via PsExec. Being the “noisiest” part of the operation, it is usually accomplished as quickly as possible to minimize chances of detection, as all of the necessary preliminary work has already been completed. In observed instances, the deployment and execution of Ryuk occurred in one session, typically lasting 3 to 8 hours.

Summary

Putting the pieces together gives a view into WIZARD SPIDER'S and GRIM SPIDER’s methodology, but it also provides some useful detection points that can give defenders advanced notice by setting up monitoring and configurations to thwart the goals of these eCrime actors. With this knowledge, we aim to equip you to stop the WIZARD SPIDER and GRIM SPIDER threat actors well before they have an opportunity to encrypt your data or cause serious harm to your business.

Additional Resources

Table 1 below contains a mapping of WIZARD SPIDER and GRIM SPIDER tactics to the MITRE ATT&CK™ Framework.

Tactic	Technique	Observable
Initial Access	Spear-Phishing Attachment	Not observed, due to time frame and data decay
Execution	Command Line Interface, PowerShell, Scheduled Task, Service Execution, Windows Remote Management	Execution of TrickBot via PsExec or PSEXESVC and scheduled tasks. Services and powershell used for PowerShell Empire
Persistence	New Service, Scheduled Task, Valid Accounts	PowerShell Empire service, Trickbot Scheduled Task, recording passwords of valid uses for remote authentication
Privilege Escalation	Valid Accounts	TrickBot pwgrab modules to get privileged accounts
Defense Evasion	Obfuscated Files or Information, File Deletion	PowerShell Empire service is Base64-encoded, services and files are generated with innocuous names. Some modules and configurations are removed after use.
Credential Access	Credential Dumping	Indications of TrickBot pwgrab64 module having been executed

Discovery	Remote System Discovery	Use of TrickBot modules for network discover
Lateral Movement	Windows Admin Shares, Remote File Copy and Remote Desktop Protocol (RDP)	Use of PsExec to deploy Trickbot/PowerShell Empire, copy credentials, other information from compromised infrastructure, RDP for exploring, copy tools to compromised infrastructure
Collection	Data Staged	Credential/network enumeration information
Exfiltration	Exfiltration via Command and Control Channel	Domain credentials, network enumeration information is sent back to GRIM SPIDER via http
Command and Control	Custom Command and Control Protocol	PowerShell Empire, TrickBot modules communicate over http
Impact	Data Encrypted for Impact	Ryuk ransomware

Table 1: MITRE ATT&CK Mapping Indicators of compromise (IOCs) associated with WIZARD SPIDER investigations are available in Table 2.

Indicator	Purpose
UseLogonCredential = 1	Registry value set for storing passwords (plaintext) in memory, used to harvest credentials
“Updater”, “Technoservice”	Service file name contains encoded PowerShell commands, service pointing to TrickBot
%COMSPEC% /C start /b C:\Windows\System32\WindowsPowershell\v1.0\powershell -noP -sta -w 1 -enc <*BASE64*>	Service File Name content for PowerShell Empire loader
C:\Windows\tetup.exe , C:\mswvc.exe	Trickbot binary paths in C:\ or C:\Windows\, observed as a 5-character alphabetical name, or a long alphanumeric string with underscores
C:\Users\Default\AppData\Roaming\mssert\mtwvc.exe	Trickbot binary paths in home directories, observed as a 5-character alphabetical name under an alphabetical folder in AppData\Roaming\ , or a long alphanumeric string with underscores

Table 2: IOCs Associated with GRIM SPIDER

Learn More

- *Learn how CrowdStrike can help your organization answer its most important security questions: Visit the CrowdStrike Services web page.*
- *Download the 2020 CrowdStrike Global Threat Report.*
- *Download the 2018 CrowdStrike Services Cyber Intrusion Casebook and read up on real-world IR investigations, with details on attacks and preventative recommendations.*
- *Learn more about CrowdStrike's next-gen endpoint protection by visiting the Falcon platform product page.*
- *Test CrowdStrike next-gen AV for yourself: Start your free trial of Falcon Prevent™ today.*
