Response to CISA Advisory (AA23-320A): Scattered Spider

By Francis Guibernau

Published: 2023-11-21 · Archived: 2026-04-02 12:07:56 UTC

On November 16, 2023, the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) released a joint Cybersecurity Advisory (CSA) detailing the identification of Indicators of Compromise (IOCs), Tactics, Techniques, and Procedures (TTPs), and detection methods associated with Scattered Spider identified through FBI investigations as recent as November 2023.

Scattered Spider is an eCrime adversary that has been active since at least May 2022, known for conducting social engineering campaigns against Business-Process Outsourcing (BPO) organizations, as well as the Telecommunications and Technology sectors.

The adversary employs phishing websites, SMS phishing, and social engineering attacks to gather authentication credentials such as One-Time-Password (OTP) codes. To bypass Multi-Factor Authentication (MFA), Scattered Spider overwhelms targets by using MFA notification fatigue or resorts to SIM swapping attacks.

Once access has been achieved, Scattered Spider opts to use legitimate Remote Management tools instead of custom malware to ensure persistent access. Since April 2023, the adversary has been leading extortion campaigns during which they use BlackCat/ALPHV Ransomware-as-a-Service (RaaS) to encrypt the victim's data and demand the payment of a ransom to prevent the captured data from being resold or published.

AttackIQ has released a new assessment template that emulates the observed capabilities of Scattered Spider during a series of activities recorded as recently as November 2023 with the goal of helping customers validate their security controls and their ability to defend against this sophisticated threat.

Validating your security program performance against these behaviors is vital to reducing risk. By using this new assessment template in the AttackIQ Security Optimization Platform, security teams will be able to:

- Evaluate security control performance against a threat known for targeting commercial facilities sectors worldwide.
- Assess their security posture against activities primarily focused on encryption and exfiltration of proprietary information.
- Continuously validate detection and prevention pipelines against behaviors similar to that of many other adversaries focused on ransomware activities.

[CISA AA23-320A] Scattered Spider

This assessment template emulates the different Tactics, Techniques and Procedures (TTPs) employed by Scattered Spider within a Microsoft Windows environment. A combination of behaviors and malware samples are utilized to perform the exact same behaviors that the adversary has exhibited.

The template is divided by Tactics, and these group the Techniques and Implementations used by Scattered Spider at each stage of their attacks.

1. **Execution:** Consists of techniques that result in adversary-controlled code running on a local or remote system. Techniques that run malicious code are often paired with techniques from all other tactics to achieve broader goals, such as exploring a network or stealing data.

   Native API (T1106): Provides a controlled means of calling low-level OS services within the kernel, such as listing processes.

2. **Persistence:** Techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access.

   Scheduled Task/Job: Scheduled Task (T1053.005): This scenario creates a new scheduled task using the `schtasks` utility.

3. **Defense Evasion:** Techniques adversaries use to avoid detection throughout their compromise.

   Access Token Manipulation (T1134): This scenario lists active access tokens that could be impersonated by another process. This method is commonly used to escalate privileges.

   Subvert Trust Controls: Code Signing (T1553.002): This scenario executes a self-signed binary in order to bypass security policies that require signed code to execute on a system.

   Impair Defenses: Disable or Modify System Firewall (T1562.004): This scenario temporarily disables the Windows Firewall using the `netsh advfirewall` utility. By disabling the Firewall, the adversary can open up previously blocked incoming or outgoing network connections that could allow for remote access.

   Impair Defenses: Disable or Modify System Firewall (T1562.004): This scenario temporarily disables the Windows Firewall by modifying the EnableFirewall registry key to `0` for the `DomainProfile`, `StandardProfile` and `PublicProfile` keys within `HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Parameters\FirewallPolicy\` and `HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\`

4. **Credential Access:** Consists of techniques for stealing credentials like account names and passwords.

   OS Credential Dumping: LSASS Memory (T1003.001): LSASS memory is dumped to disk by creating a minidump of the `lsass.exe` process. This process is used for enforcing security policy on the system and contains many privileged tokens and accounts that are targeted by threat actors. `Mimikatz` is then used to dump the credentials from that minidump file.

5. **Discovery:** The adversary may use these techniques to gain knowledge about the initially infected system and internal network. These techniques help adversaries observe the environment and orient themselves before deciding how to act.

   File and Directory Discovery (T1083): A batch script is executed that lists all files and directories in `%ProgramFiles%` and the `%systemdrive%\Users` directory.

Account Discovery: Domain Account (T1087.002): The system command `net group` is used to list Domain and Enterprise Admins accounts.

Remote System Discovery (T1018): This scenario executes the `net view` command to gather additional hosts available to the infected asset.

Remote System Discovery (T1018): This scenario executes the `nltest` command to gather a list of domain controllers associated with a domain.

System Owner/User Discovery (T1033): The native `whoami` command is called to receive details of the running user account.

6. **Lateral Movement:** Consists of the techniques adversaries use to enter and control remote systems on a network. Following through on their primary objective often requires exploring the network to find their target and subsequently gaining access to it.

   Remote Services: Remote Desktop Protocol (T1021.001): Remote Desktop is the built-in remote access utility used by Windows. This scenario attempts to remotely connect to another accessible asset with stolen credentials.

7. **Collection:** The adversary may use these techniques to gather information and the sources information is collected from that are relevant to following through on the adversary's objectives.

   Clipboard Data (T1115): This scenario will use the native PowerShell `Get-Clipboard` cmdlet to retrieve data stored in the clipboard.

8. **Command and Control:** Techniques that adversaries may use to communicate with systems under their control within a victim network.

   Ingress Tool Transfer (T1105): This scenario downloads to memory and saves to disk in independent scenarios to test network and endpoint controls and their ability to prevent the delivery of known malicious BlackCat/ALPHV ransomware samples.

9. **Impact:** Techniques that adversaries use to disrupt availability or compromise integrity by manipulating business and operational processes.

   Data Encrypted for Impact (T1486): AttackIQ has replicated the functionality used by the BlackCat/ALPHV ransomware to encrypt files on the targeted hosts. This includes the common file extensions and encryption methods utilized by the actor.

Detection and Mitigation Opportunities

Given the number of different techniques being utilized by this threat, it can be difficult to know which to prioritize for prevention and detection opportunities. AttackIQ recommends first focusing on the following techniques emulated in our scenarios before moving on to the remaining techniques.

1. Review CISA's Patching and Detection Recommendations:

CISA has provided a significant number of recommendations for the best ways to defend yourself from these and similar attacks. AttackIQ strongly recommends reviewing the detection and mitigation recommendations with the goal of adapting them to your environment first to determine if you have any existing impact before reviewing the assessment results.

2. Scheduled Task/Job: Scheduled Task (T1053.005)

Adversaries may abuse the Windows Task Scheduler to perform task scheduling for initial or recurring execution of malicious code. There are multiple ways to access the Task Scheduler in Windows. The schtasks utility can be run directly from the command line, or the Task Scheduler can be opened through the GUI within the Administrator Tools section of the Control Panel.

2a. Detection

With an EDR or SIEM Platform, you can detect the following commands being issued to schedule a malicious task

```
Process Name = (“cmd.exe” OR “Powershell.exe”)
Command Line CONTAINS (“schtasks” AND “/CREATE” AND (“cmd” OR “powershell”)
```

2b. Mitigation

MITRE ATT&CK has the following mitigation recommendations for Scheduled Task

- M1047 – Audit
- M1028 – Operating System Configuration
- M1026 – Privileged Account Management
- M1018 – User Account Management

Wrap-up

In summary, this assessment template will evaluate security and incident response processes and support the improvement of your security control posture against the activities carried out by Scattered Spider. With data generated from continuous testing and use of this assessment template, you can focus your teams on achieving key security outcomes, adjust your security controls, and work to elevate your total security program effectiveness against a known and dangerous threat.

AttackIQ offers a comprehensive Breach and Attack Simulation Platform to assist security teams. This includes AttackIQ Flex, a tailored pay-as-you-go service; AttackIQ Ready!, a fully managed service for continuous security optimization; and AttackIQ Enterprise, a co-managed service offering enhanced support. These services ensure your team maintains a robust security posture.
