SCATTERED SPIDER Attempts to Avoid Detection with Bring-Your-Own-Driver Tactic

By CrowdStrike Intelligence Team

Archived: 2026-04-05 18:49:06 UTC

- In December 2022, CrowdStrike reported on a campaign by SCATTERED SPIDER, targeting organizations within the telecom and business process outsourcing (BPO) sectors with an end objective of gaining access to mobile carrier networks.
- In the weeks since that post, the CrowdStrike Falcon® platform prevented a novel attempt by SCATTERED SPIDER to deploy a malicious kernel driver through a vulnerability (CVE-2015-2291) in the Intel Ethernet diagnostics driver.
- The activity exploits a well known and pervasive deficiency in Windows security that enables adversaries to bypass Windows kernel protections with the Bring-Your-Own-Vulnerable-Driver tactic.
- CrowdStrike Services has observed the actor attempting to bypass other endpoint tools including Microsoft Defender for Endpoint, Palo Alto Networks Cortex XDR and SentinelOne using more traditional defense evasion techniques targeting Windows registry hives.

Introduction

In December, CrowdStrike reported that beginning in June 2022, the CrowdStrike Services, CrowdStrike® Falcon OverWatch™ and CrowdStrike Intelligence teams observed an increase in the targeting of telco and BPO industries. CrowdStrike Intelligence attributed this campaign with low confidence to the SCATTERED SPIDER eCrime adversary.

SCATTERED SPIDER (aka Roasted 0ktapus, UNC3944) leverages a combination of credential phishing and social engineering to capture one-time-password (OTP) codes or overwhelms targets using multifactor authentication (MFA) notification fatigue tactics. Having obtained access, the adversary avoids using unique malware, instead favoring a wide range of legitimate remote management tools to maintain persistent access.

In the weeks since that blog post, the Falcon platform detected a novel attempt by this adversary to deploy a malicious kernel driver through a vulnerability (CVE-2015-2291) in the Intel Ethernet diagnostics driver for Windows (`iqvw64.sys`).

Microsoft Windows Security Deficiencies Leave Devices Vulnerable

This vulnerability has been used by adversaries for several years to deploy malicious drivers into the Windows kernel. This technique is known as “Bring Your Own Vulnerable Driver” (BYOVD) and is a tactic that has persisted due to a gap in Windows security.

In an attempt to limit the amount of capabilities that malware can gain access to on a Windows system, starting with 64-bit Windows Vista, Windows does not allow unsigned kernel-mode drivers to run by default. BYOVD "makes it easy for an attacker with administrative control to bypass Windows kernel protections," allowing an adversary to install a legitimately signed but malicious driver to execute an attack. Publicly available tools, such as KDMapper, allow adversaries to easily take advantage of BYOVD to map non-signed drivers into memory.

In 2021, Microsoft stated that "Increasingly, adversaries are leveraging legitimate drivers in the ecosystem and their security vulnerabilities to run malware," and that "drivers with confirmed security vulnerabilities will be blocked on Windows 10 devices in the ecosystem using Microsoft Defender for Endpoint attack surface reduction (ASR) and Microsoft Windows Defender Application Control (WDAC) technologies to protect devices against exploits involving vulnerable drivers to gain access to the kernel."

However, as noted by multiple security researchers (e.g., here, here and here) over the past two years, the issue continues to persist as Microsoft fails to block vulnerable drivers by default.

In this instance, the adversary attempted to load a malicious driver that was prevented from running and quarantined by CrowdStrike Falcon® Prevent machine learning (ML) and identified by Falcon OverWatch. This driver is designed to use the privileged driver space provided by the vulnerable Intel driver to overwrite specific routines in the CrowdStrike Falcon sensor driver with adversary-created trampoline code. While this was prevented by the Falcon sensor and immediately escalated to the customer with human analysis, a series of recommendations to protect Microsoft kernel memory can be found in the "Recommendations" section below.

In the past months, CrowdStrike Services has observed the actor attempting to bypass other endpoint tools including Microsoft Defender for Endpoint, Palo Alto Networks Cortex XDR and SentinelOne.

Technical Analysis

CrowdStrike has identified various versions of a malicious driver that are signed by different certificates and authorities — including stolen certificates originally issued to NVIDIA and Global Software LLC, as well as a self-signed test certificate. The intent of the adversary is to disable the endpoint security products visibility and prevention capabilities so the actor can further their actions on objectives.

Versions of the sample are small, 64-bit Windows kernel drivers with less than 35 relatively simple functions.

An example driver with SHA256 hash

`b6e82a4e6d8b715588bf4252f896e40b766ef981d941d0968f29a3a444f68fef` has its build time set to `1970-01-01 00:01:35 UTC`. It contains various status messages and calls to `DbgPrintEx()`, as a means to provide status messages to the threat actor. The file is signed using a certificate with the following parameters:

serial: `31 11 00 fb 8d ee 5e 09 37 6b 69 a8 f6 23 e0 ee`

issued to: `Global Software, LLC`

valid from: `2018-05-14` valid to: `2021-06-18`

The same certificate has been observed signing other malicious files dating back to at least 2018, suggesting that other threat actors have copies of it.

The driver walks the list of loaded kernel modules, searching for `csagent.sys` (the CrowdStrike Falcon kernel component), and scans the identified module for a hard-coded pattern of 64 bytes. In addition to the search pattern, the scanning function retrieves the mask string " `xxxxxxxxxxxxxxxxxx??xxxxxxxxxxxxxxxxxxxxxxxxxxxx??xx` " as an argument that masks out bytes corresponding to absolute memory addresses. These change when the driver code is mapped to a different base address, and should therefore be excluded. The mask string is only 61 bytes long, 3 bytes shorter than the code pattern, possibly due to incomplete adjustments.

A second sample with SHA256 hash `e23283e75ed2bdabf6c703236f5518b4ca37d32f78d3d65b073496c12c643cfe` has a PE build timestamp of `2022-12-23 15:11:27 UTC` that matches the signing date. This file is digitally signed with what appears to be a test certificate with the following parameters:

serial: `23 43 9d 9d d3 2a a7 b2 4b bb 6e 31 64 fb 47 53`

issued to: `WDKTestCert guid0,133162475712847553`

valid from: `2022-12-23`

valid to: `2032-12-23`

This sample is intended to be loaded using BYOVD techniques and hence does not require a verifiable digital signature. No other files signed with this test certificate were available at the time of analysis.

Upon startup, the driver decrypts a hard-coded string of targeted security products using a basic XOR loop:

```
for i in len(name): name ^= i % 56 + 49
```

The malicious driver then finds the target driver using the same method and patches it, in memory, at hard-coded offsets. The patching routine operates on a list where each element represents a hook structure that contains a pointer to the target function, a pointer to the malware routine and trampoline code to invoke that routine. The installed malware routines signal success to the Falcon sensor in every case even though the routines perform no operation.

While the outlined activity appears to target specific industries, organizations of all types should apply the lessons learned to harden defenses against such threats. CrowdStrike recommends that organizations employ a rigorous, defense-in-depth approach that monitors endpoints, cloud workloads, identities and networks to defend against advanced, persistent adversaries. The holistic deployment of security tooling paired with a high operational tempo in responding to alerts and incidents are critical to success.

Recommendations

The described activity will be prevented and quarantined by the Falcon platform if configured as outlined in our prevention policy best practices recommendations.

Prevention Policy Settings

With regard to the malicious activity detailed here, in particular confirm the Windows prevention policy settings listed are set as follows:

- Sensor Tampering Protection enabled
- Cloud Anti-malware Prevention slider at Moderate or higher
- Sensor Anti-malware Prevention slider at Moderate or higher
- Suspicious Processes enabled
- Suspicious Kernel Drivers enabled

The complete list of our best practices recommendations for prevention policies may be found in the support portal here: Prevention Policy Best Practice Guidelines

Mitigate CVE-2015-2291

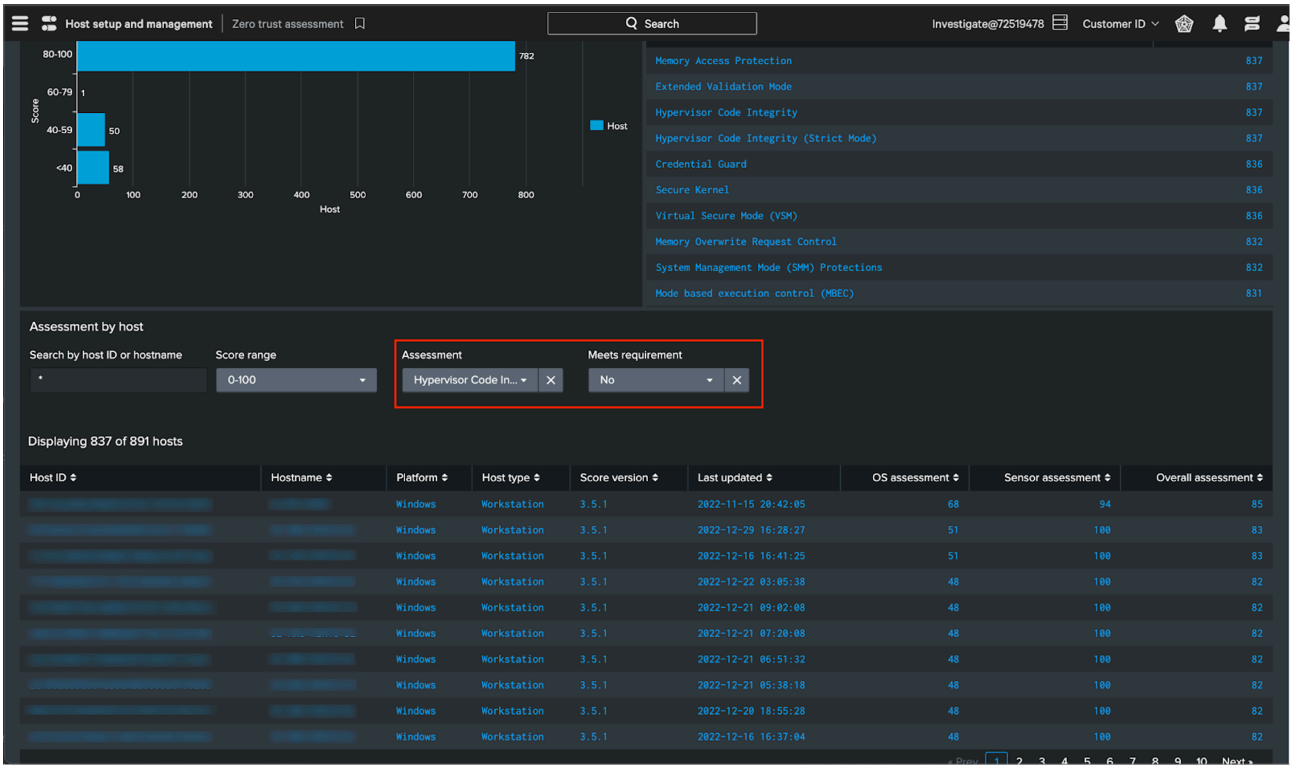
CrowdStrike customers should ensure they have the ability to locate and patch the vulnerable Intel Ethernet Driver specified in CVE-2015-2291. Prioritizing the patching of vulnerable drivers can help mitigate this and similar attack vectors involving signed driver abuse.

CrowdStrike Falcon® Spotlight customers can search for the presence of this driver by navigating to: Spotlight > Vulnerabilities. US-1 | US-2 | EU | Gov

Evaluate Enabling Microsoft Memory Integrity Capabilities

Due to the inherent flaws in Microsoft protection of kernel memory permitting these types of BYOVD attacks, additional functionality has been incorporated into modern Windows Operating Systems. Hypervisor-Protected Code Integrity (HVCI), a component of Virtualization-Based Security (VBS) is designed to prevent users with elevated privilege from being able to read and write to kernel memory. The protections were implemented in order to address the security flaw of not enforcing kernel memory protections.

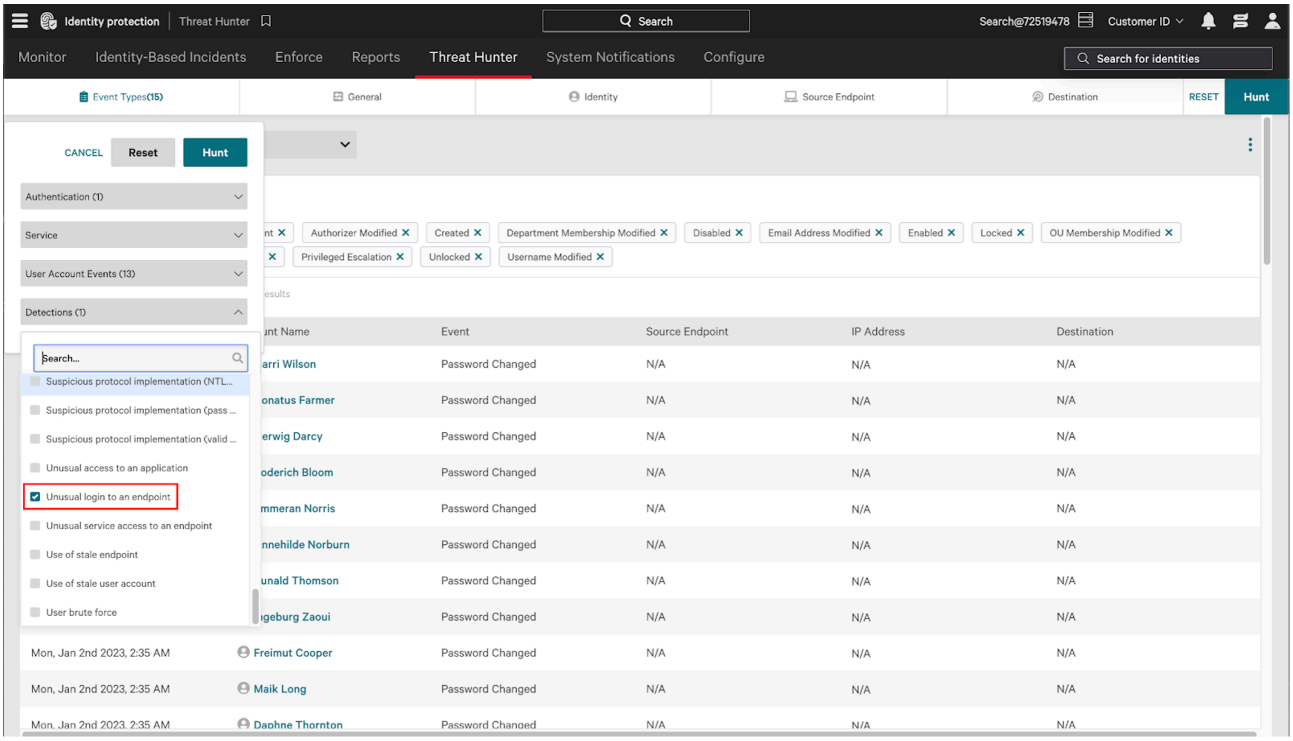
While CrowdStrike has not identified any issues with the Falcon platform running in environments with these features enabled, there have been intermittent reports of performance issues in various other environments tied to specific applications and some processors. CrowdStrike Falcon® Insight XDR customers can view the status of HVCI by navigating to: Host setup and management > Zero Trust Assessment.



(Click to enlarge)

Enable Traffic Inspection for CrowdStrike Falcon Identity Threat Protection

As the adversary is largely leveraging valid accounts as the initial access vector, additional scrutiny of legitimate login activity and two-factor authentication approvals from unexpected assets, accounts or locations are highly recommended.



(Click to enlarge)

Additional Resources

- *Request a free trial of the industry-leading CrowdStrike Falcon platform.*
- *Read about adversaries tracked by CrowdStrike in 2022 in the 2023 CrowdStrike Global Threat Report and in the 2023 Threat Hunting Report.*
- *Request a free CrowdStrike Intelligence threat briefing and learn how to stop adversaries targeting your organization.*
- *Learn how CrowdStrike Services can help your organization prepare to defend against sophisticated threats, respond and recover from incidents with speed and precision, and fortify your cybersecurity practices.*
- *Watch an introductory video on the CrowdStrike Falcon console and register for an on-demand demo of the market-leading CrowdStrike Falcon platform in action.*
