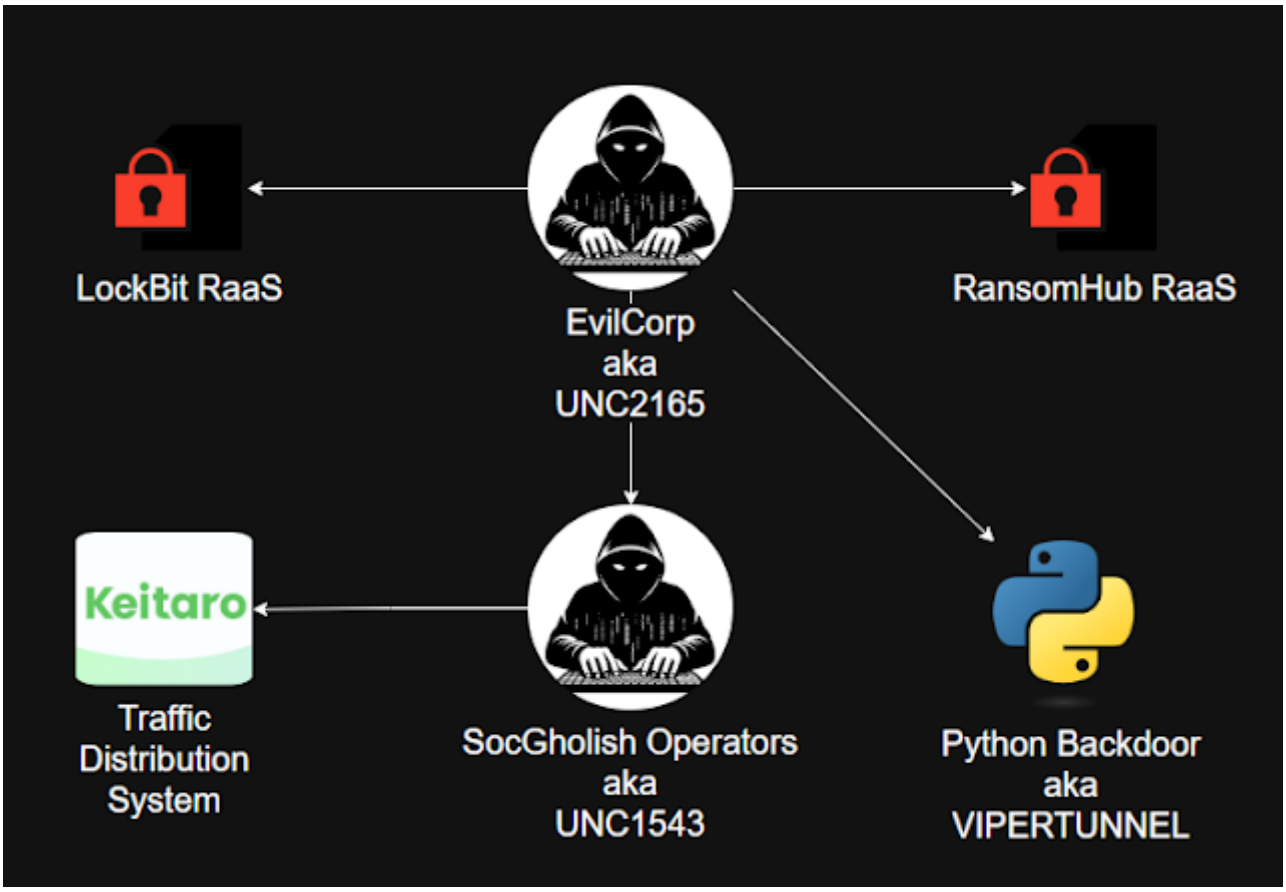
Tracking Adversaries: EvilCorp, the RansomHub affiliate

blog.bushidotoken.net/2025/04/tracking-adversaries-evilcorp-ransomhub.html



Introduction

This blog is part of a cyber threat intelligence (CTI) blog series called Tracking Adversaries that investigates prominent or new threat groups.

The focus of this blog is EvilCorp, a sanctioned Russia-based cybercriminal enterprise known for launching ransomware attacks, and RansomHub, a prominent ransomware as a service (RaaS) operation run by Russian-speaking cybercriminals.

These two threat groups have been linked together through cooperation on intrusions and IOCs and TTPs shared by multiple CTI sources. The implication of this link is critical due to RansomHub being the most active ransomware gang and is working with a well-known sanctioned affiliate.

Who is RansomHub?

Active since February 2024, RansomHub is a RaaS operation formerly known as Cyclops and Knight and is run by Russian-speaking adversaries. It is currently used by more and more cybercriminals that are ex-affiliates of other RaaS operations. This includes the ALPHV/BlackCat RaaS and the LockBit RaaS, which have since shutdown or disappeared. This has made the RansomHub RaaS one of the most widespread ransomware families as of early 2025.

Due to having a high number of affiliates, the tools and TTPs observed before the final RansomHub payload is deployed can vary significantly. Each affiliate may have their own set of tools and TTPs to achieve the final objectives of data exfiltration and ransomware deployment.

Who is EvilCorp?

Evil Corp is an international cybercrime network sanctioned for orchestrating large-scale financial cyberattacks led by Maksim Yakubets. EvilCorp's operations have evolved over time, expanding from Dridex banking trojan campaigns into developing ransomware like BitPaymer, WastedLocker, Hades, PhoenixLocker, and MacawLocker.

Notably, Aleksandr Ryzhenkov, was identified by the National Crime Agency (NCA) as a high-ranking member of EvilCorp and also LockBit affiliate. Ryzhenkov became a LockBit affiliate around 2022, contributing to over 60 LockBit ransomware builds and attempting to extort more than $100 million from victims. This discovery aligns with Mandiant's previous reporting on EvilCorp shifting to LockBit as well.

The NCA also found that EvilCorp maintains close ties with Russian intelligence agencies through Yakubets' father-in-law, Eduard Bendersky, a former FSB officer, who is suspected of using his influence to shield the group from prosecution in Russia.

One of the TTPs that makes EvilCorp standout from the rest of the RaaS affiliates is their own affiliation to the SocGholish JavaScript malware (aka FAKEUPDATES). If ransomware deployment takes place following a SocGholish infection, then the attackers responsible for the attack will be affiliated with EvilCorp.

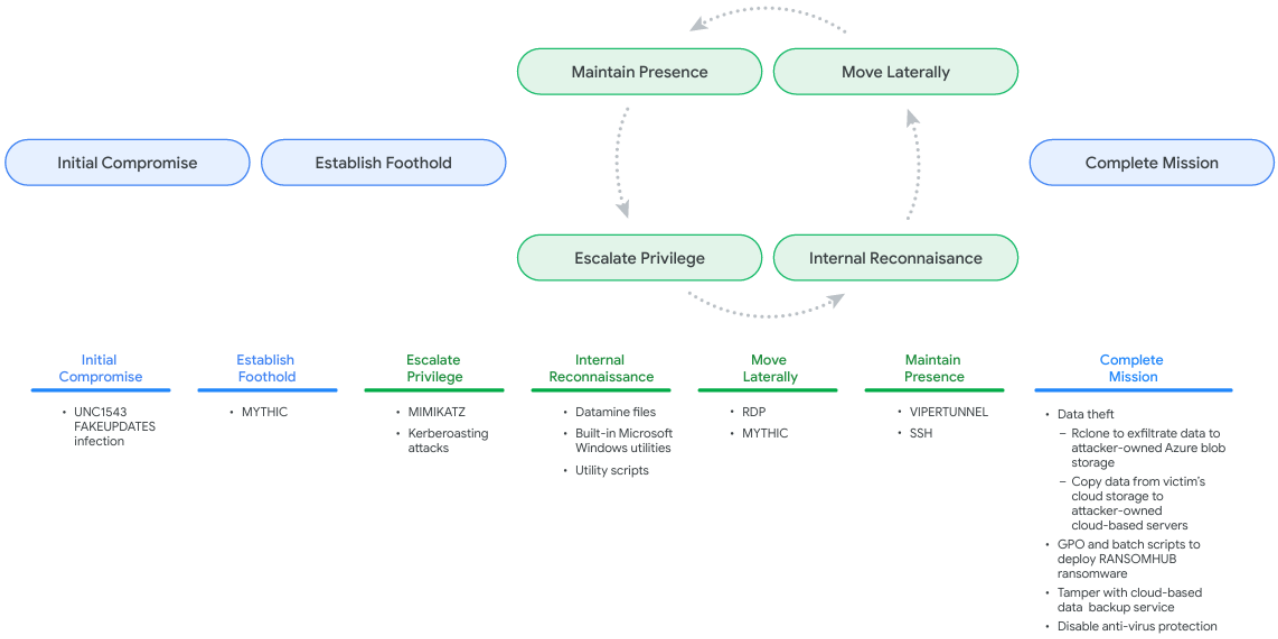
Reported Connections Between EvilCorp and RansomHub

On 15 July 2024, Microsoft shared a post on X stating that RansomHub was observed being deployed in post-compromise activity by Manatee Tempest (which is Microsoft's name for EvilCorp) following initial access via SocGholish (aka FakeUpdates) infections (which Microsoft tracks as Mustard Tempest).

On 15 January 2025, Guidepoint wrote a blog on a new Python backdoor used by an affiliate of RansomHub. Notably, the new Python backdoor was delivered by SocGholish. Therefore, this Python backdoor is another potential artifact worth monitoring for its connection to known EvilCorp-related malware.

The next day, on 16 January 2025, Google shared a report on EvilCorp (which Google tracks as UNC2165) that disclosed numerous tools and malware families they have been using to deliver RansomHub, including a Python backdoor dubbed VIPERTUNNEL (see the image below). The presence of a Python backdoor following a SocGholish infection is notable TTP that overlaps with the Guidepoint blog on RansomHub.

Figure 6: UNC2165 Attack Lifecycle in Observed Intrusions Leading to RANSOMHUB Deployment



On 14 March 2025, Trend Micro disclosed further details that also confirmed the SocGholish malware is leading to the deployment of RansomHub ransomware. The operators of SocGholish are tracked as Water Scylla by Trend Micro. The operators distribute SocGholish via the Keitaro Traffic Direction System (TDS), a legitimate service used for marketing campaigns. Trend Micro also observed SocGholish dropping the same custom Python backdoor (aka VIPERTUNNEL) as well.

So What?

EvilCorp has been under US sanctions since 2019, making it illegal for affected organisations to pay ransoms to them without facing potential fines from the US Treasury's Office of Foreign Assets Control (OFAC). Despite these sanctions, EvilCorp has continued its cybercriminal activities by adapting its tactics to include rebranding their ransomware and becoming an affiliate of RaaS operations, such as LockBit and RansomHub.

The key indicator of EvilCorp's involvement in ransomware attacks continues to be the use of the SocGholish malware, which employs drive-by downloads masquerading as web browser software updates to gain initial access to systems.

EvilCorp's affiliation with RansomHub raises the possibilities that RansomHub may soon face sanctions similar to those imposed on EvilCorp. Consequently, any victim that pays a ransom to RansomHub could become significantly riskier for cyber insurance organisations, incident responders, and ransomware negotiators, as they may inadvertently violate sanctions and face legal repercussions.

Given EvilCorp's prominence as a target for international law enforcement, its association with RansomHub is likely to draw increased scrutiny. This could result in RansomHub becoming the focus of future law enforcement actions, including potential takedowns and additional sanctions, further complicating the landscape for entities involved in ransomware response and mitigation.

There is also the increased likelihood that RansomHub will now rebrand. As we saw in the BlackBasta Leaks, ransomware groups pay close attention to the news, CTI reports, and even posts on X and even blogs by researchers. This association to EvilCorp and threat of sanctions is an issue for ransomware groups as it impacts their business model and makes earning harder. Therefore, by linking the two entities together CTI analysts can impose cost on these cybercriminals.

References:

Raspberry Robin: A global USB malware campaign providing access to ransomware operators

The Ransomware Tool Matrix

The Russian APT Tool Matrix