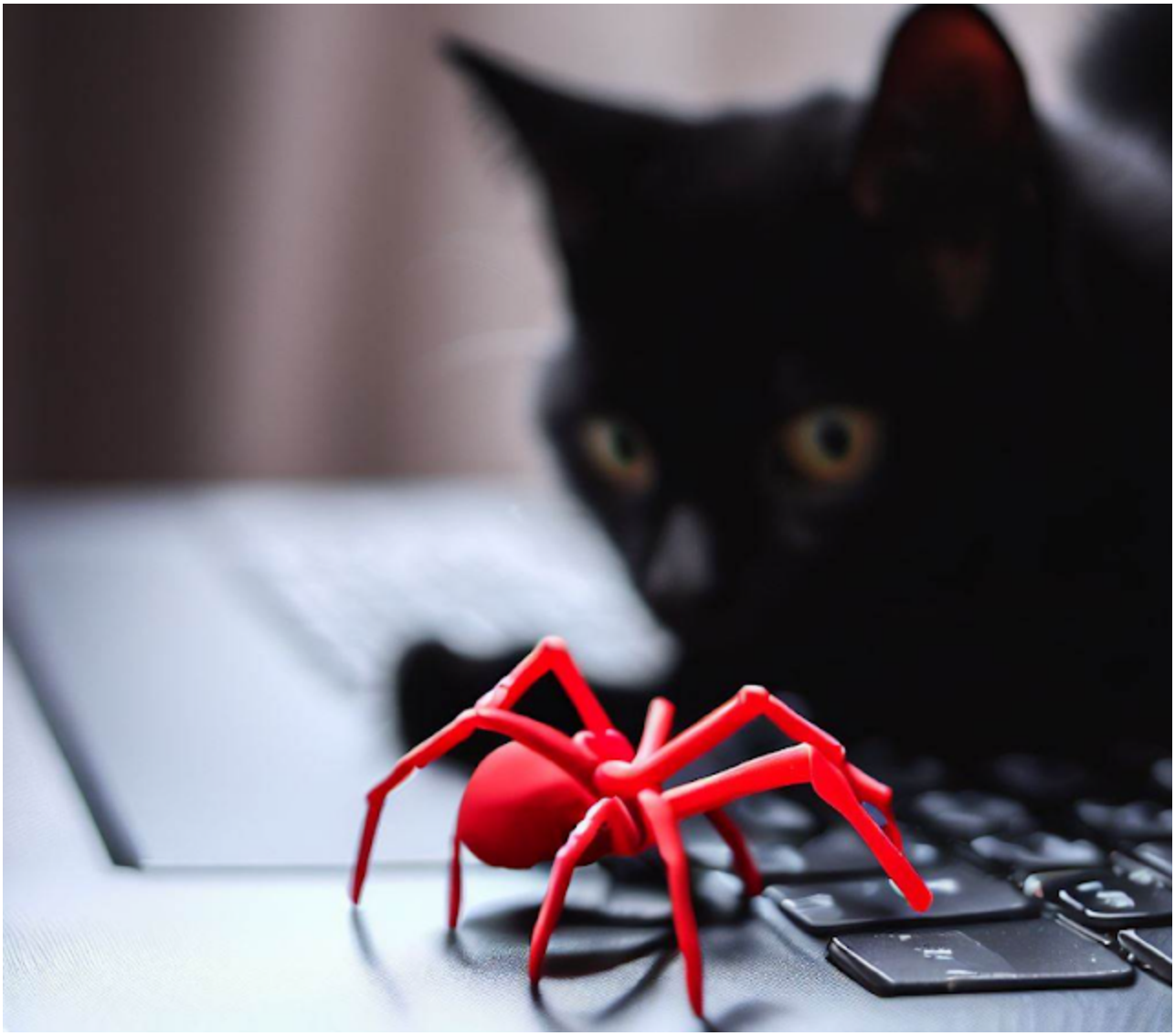
Tracking Adversaries: Scattered Spider, the BlackCat affiliate


blog.bushidotoken.net/2023/08/tracking-adversaries-scattered-spider.html

BushidoToken



After tracking the cybercrime threat landscape on a day-to-day basis for over four years now, it's not that often anymore that something surprises me. But the latest trend of a suspected English-speaking big game hunting cybercriminal group, tracked under the moniker as Scattered Spider by CrowdStrike or 0ktapus by Group-IB, teaming up with a Russian-speaking ransomware group known as BlackCat (or ALPHV) has caught my attention.

Background on Scattered Spider

CrowdStrike introduced Scattered Spider in December 2022 and shared an update in January 2023. These financially motivated English-speaking threat actors are known for their unique style of attacks, which usually all begin the same way, either via an SMS phishing message to harvest credentials or via an old school (yet still very effective) social engineering vishing call to get credentials or get the target to download malicious software and provide access.

Other tricks Scattered Spider is known for includes multi-factor authentication (MFA) fatigue attacks, which involve spamming the authentication request notification to the target's device until the accept (either by accident or out of annoyance), as well as SIM swapping, which includes tricking the mobile carrier of the target to provide SIM card access to the threat actor.

Scattered Spider's tricks don't end there though. They also use a variety of defense evasion techniques to bypass enterprise-level security, such as the bring-your-own-vulnerable-driver (BYOVD) exploit and Microsoft-signed malicious drivers, as well as the use of a UEFI Bootkit called BlackLotus that's sold as off-the-shelf malware on the cybercriminal underground. Plus, for command-and-control (C2) the group uses a whole host of legitimate commercial remote monitoring and management (RMM) tools to manipulate target systems, often through free trials too.

For more background information on Scattered Spider, you can watch my BSides Cheltenham talk from June 2023. The slides are also available on my GitHub too.

Scattered Spider shifts to BlackCat ransomware attacks

Scattered Spider is tracked under several cryptonyms by different cybersecurity vendors Group-IB calls them 0ktapus, Mandiant tracks them as UNC3944, and Microsoft calls them Storm-0875. Until recently, has been known primarily for data theft extortion without ransomware deployment.

The two best examples we have of a Scattered Spider archetypal intrusion has been against Riot Games in January 2023 and Reddit in February 2023. The threat actors used their tricks described above, got into the networks of these companies, and stole whatever they could in hopes to ransom it back to them. It doesn't seem though that these were very successful intrusions as neither Reddit nor Riot Games seemed to have paid any amount of ransom (as far as we know, that's just what these companies stated themselves).

We now have several reasons to believe that Scattered Spider have gone for the BlackCat (ALPHV) ransomware-as-a-service (RaaS) group. This includes temporal, technical, and behavioural analysis.

Links available in public sources (OSINT) between Scattered Spider and BlackCat are as follows:

- Following the February 2023 Reddit breach, that has several signs Scattered Spider was responsible for, the BlackCat data leak site posted Reddit as a victim in June 2023. The threat actor who wrote the leak post on the BlackCat blog also stated that "Operators broke into Reddit on February 5, 2023, and took 80 gigabytes (zipped) of data."
- In May 2023, Trend Micro researchers revealed that a certain BlackCat affiliate used an identical Microsoft-signed driver for defense evasion with the same file-hash (MD5: 909f3fc221acbe999483c87d9ead024a) that Mandiant has called POORTRY and has linked to UNC3944 (Scattered Spider), among other threat actors.
- In July 2023, the Canadian Center for Cyber Security (CCCS) shared a comprehensive Ransomware Alert on BlackCat (ALPHV) attacks against Canadian organisations. In this alert, the CCCS described some very familiar Scattered Spider tradecraft. This includes the use of SMS phishing for credential harvesting, single sign-on (SSO) themed domains, social engineering phone calls, MFA fatigue attacks, the delivery of commercial RMM tools, the use of cloud file-sharing sites, and even the continued use of ExpressVPN for C2.
- IOCs from CrowdStrike's blog in December 2022 also align with the CCCS's alert as well. This includes the appearance of the Fleetdeck[.]io and Level[.]io RMM tools in both.
- Further, many of the same TTPs laid out in the Coinbase blog in February 2023 are also present in the CCCS advisory on BlackCat. This includes the use of SMS phishing, social engineering over the phone, an SSO-themed domain, and the use of RMM tools.

In summary, the technical, behavioural, and temporal overlaps between Scattered Spider and this latest BlackCat affiliate campaign are abundant. I suspect that due to the hit and miss nature of Scattered Spider's campaigns up to early 2023 the group has decided to change tactics and join the Russian-speaking cybercriminal community of ransomware operators.

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

Tips for Investigating Cybercrime Infrastructure