Ransomware Actors Evolved Operations in 2020

crowdstrike.com/blog/ransomware-actors-evolved-operations-in-2020/

Josh Dalman - Heather Smith

June 18, 2021

In 2020, CrowdStrike Services observed the continued evolution and proliferation of eCrime adversaries engaging in big game hunting (BGH) ransomware techniques. This trend is continuing into 2021 — a recent high-profile example is the CARBON SPIDER/DarkSide attack on a U.S. fuel pipeline.

BGH was first observed by CrowdStrike in 2016 with the introduction of BOSS SPIDER’s Samas (aka SamSam) ransomware. Since then, BGH ransomware variants have multiplied, evolved and become more sophisticated, with their proliferation going virtually unimpeded by legacy endpoint security tools.

The year 2020 was marked by the trend continuing at an accelerated rate. The advancements by eCrime actors include refinement and application of high-pressure extortion tactics on victim organizations and the sharing or copying of new techniques among different ransomware groups, in addition to a marked increase in the number of ransomware variants. These advancements all but ensure that ransomware will remain a popular method for eCrime actors to monetize breaches in the foreseeable future.

Ransomware Actors Increase Pressure

CrowdStrike Services observed eCrime adversaries utilizing various techniques to increase pressure on victim organizations to pay their extortion. While in previous years ransomware eCrime adversaries were rarely observed exfiltrating data, 2020 witnessed a widespread adoption of ransomware with data-leak extortion tactics among multiple eCrime groups. This method involves both encrypting a victim organization's environment and also exfiltrating data with the threat to leak it if the extortion demand is not paid. This tactic was initially observed by CrowdStrike Intelligence with OUTLAW SPIDER in May 2019. However, it was not until November 2019, when TWISTED SPIDER adopted this technique, that it became a catalyst for multiple other eCrime actors, many of which have created dedicated leak sites to threaten exfiltration and distribute data. CrowdStrike Intelligence performed research on known dedicated leak sites for 2020. The results of this analysis depict growth throughout the year in terms of the number of leak sites and the number of victim entities with data published on the leak sites.

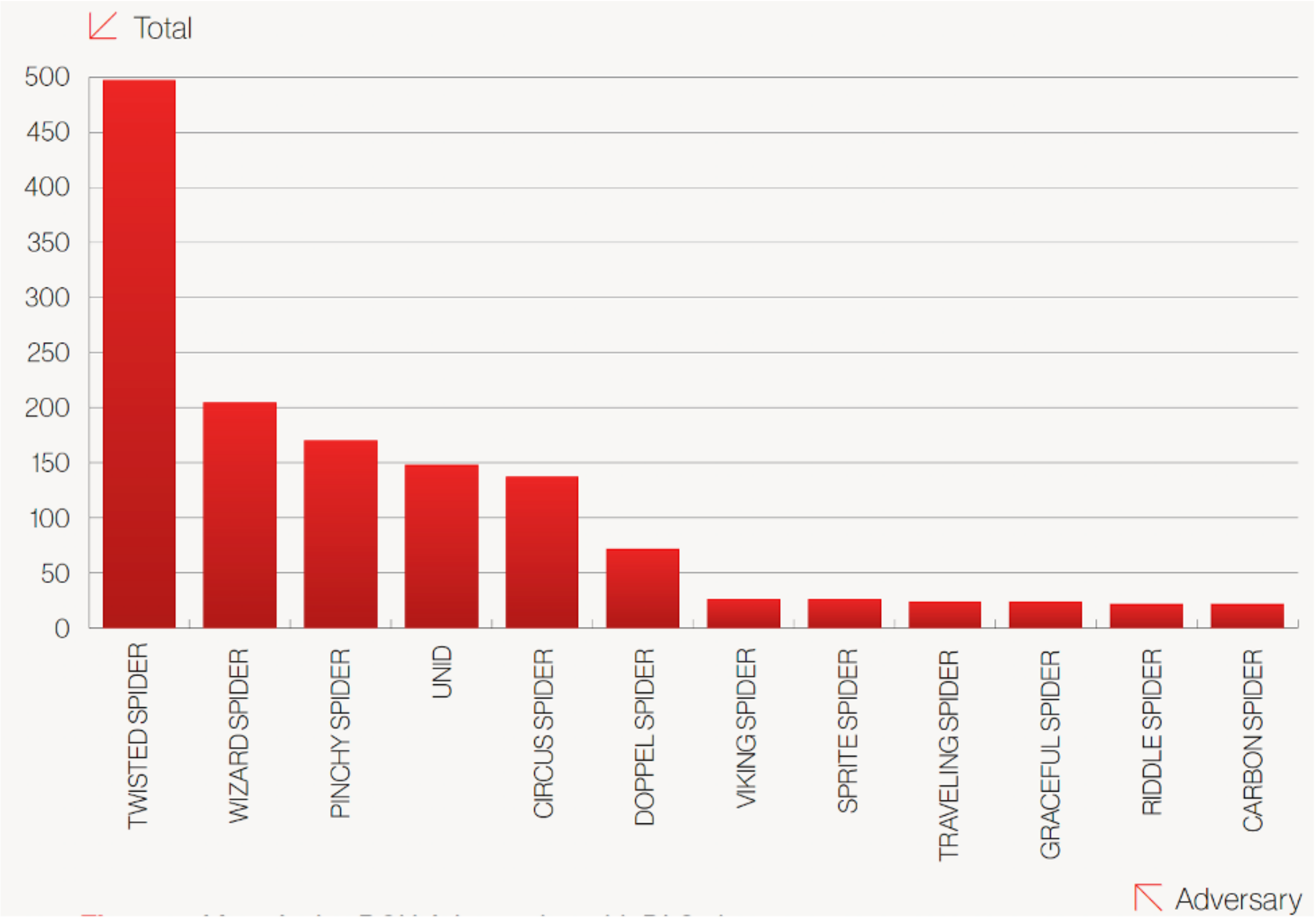

Figure 1. Most Active BGH Adversaries with DLSs in 2020

In engagements involving eCrime adversaries that use ransomware with data-leak extortion, CrowdStrike Services is regularly asked to perform incident response investigations to assist stakeholders by identifying data that was accessed and exfiltrated by threat actors.

Frequently, CrowdStrike Services is able to identify the data exfiltrated prior to publication by the eCrime adversary, thereby giving stakeholders an opportunity to prepare.

Not only has the number of eCrime dedicated leak sites grown, threat actors have also become more sophisticated in their methods of leaking the data. In general, eCrime adversaries will leak exfiltrated data slowly, saving what they perceive to be the most sensitive data for last in an effort to increase pressure on the victim organization to pay the extortion, rather than posting all of the exfiltrated data at once. PINCHY SPIDER's dedicated leak site frequently holds auctions to sell exfiltrated data. Others, such as DOPPEL SPIDER's leak site, utilize a countdown timer that triggers an increase in the ransom demand upon each expiration. CARBON SPIDER's leak site automatically releases data on a pre-set timer, with the least sensitive data leaked first and the most sensitive leaked last. There are also significant differences in the amount of data exfiltrated by threat actors. CrowdStrike Services has observed DOPPEL SPIDER frequently exfiltrating only tens of gigabytes, while others — such as TRAVELING SPIDER and affiliates associated with Nemty X ransomware — exfiltrate hundreds of gigabytes of data or more from victim organizations.

In addition to ransomware with data-leak extortion, CrowdStrike Services has identified additional tactics by eCrime adversaries to increase pressure on the victim to pay the ransom. During several recent incidents, the eCrime adversaries, after deploying ransomware to the victim organization's environment, have utilized stolen credentials to gain access to the victim organization's email instance to send extortion-related emails to users demanding payment to prevent exfiltrated data from being leaked. In other instances, the eCrime adversaries have called and harassed employees of a victim organization following ransomware deployment. Finally, CrowdStrike also observed threat actors increase pressure for payment with credible threats of distributed denial-of-service (DDoS) attacks if ransom payment is not received.

Ecrime Adversaries Collaborate

CrowdStrike has observed formal collaboration among eCrime adversaries as well as shared tactics. In June 2020, the self-named "Maze Cartel" was created when TWISTED SPIDER, VIKING SPIDER and the operators of LockBit ransomware entered into an apparent collaborative business arrangement. After this occurred, leaks associated with VIKING SPIDER's Ragnar Locker began appearing on TWISTED SPIDER's dedicated leak site and Maze ransomware began deploying ransomware using common virtualization software, a tactic originally pioneered by VIKING SPIDER.

In addition to formal collaboration, CrowdStrike Services has observed new tactics used and spread among eCrime actors. One such tactic is the development and deployment of an ELF ransomware binary that can be deployed to ESXi hosts for the purpose of encrypting virtual systems. This tactic was initially observed being used by SPRITE SPIDER's Defray777 ransomware in August 2020 and was quickly adopted by CARBON SPIDER, which utilized a similar tactic weeks later. In addition, multiple eCrime adversaries share common exfiltration techniques. CrowdStrike has observed multiple eCrime adversaries exfiltrating data through MegaSync as well as Rclone, an open-source computer program.

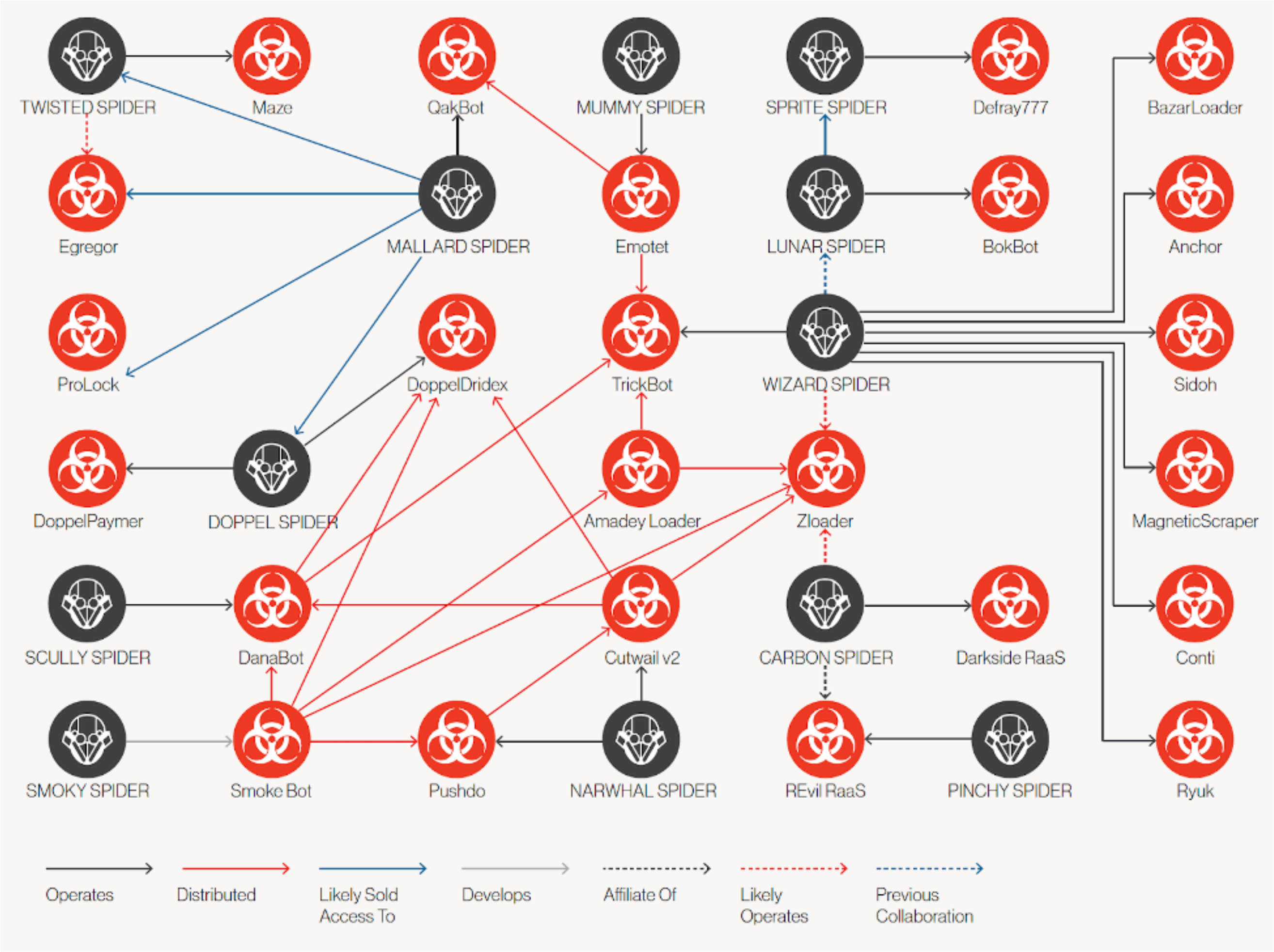

Figure 2. Mapping of observed relationships between eCrime adversaries by CrowdStrike Intelligence

What To Expect Next

Over the last several years, eCrime adversaries that engage in BGH ransomware have advanced rapidly in terms of their capabilities and sophistication. It is reasonable to expect that this trend will continue at an accelerated rate with the same goal in mind — to apply as much pressure as possible to organizations to pay ever-larger extortion demands. CrowdStrike expects that eCrime adversaries will continue to refine their data-leak extortion ransomware tactics, develop increasingly sophisticated exfiltration tooling that can be deployed widely, and automate data exfiltration by searching for, identifying and exfiltrating sensitive data by keyword.

Lastly, CrowdStrike expects eCrime adversaries to continue pursuing targets of opportunity. Frequently, these are SMBs that rely heavily on legacy antivirus to protect them, but many large organizations are being hit frequently, as threat actors see a higher return on investment when targeting an organization that may have stronger defenses but is also likely to pay a higher ransom demand.

What Can Be Done?

Why is ransomware so prevalent? In short, ransomware with data extortion remains a lucrative tactic for eCrime adversaries to monetize their presence in a victim organization’s network. Fueled by increasingly larger ransom demands, eCrime adversaries continue to develop tactics and tools that allow them to slip past legacy antivirus virtually unnoticed. Following a ransomware incident, many organizations may find that they do not have adequate backups, or that their backups became encrypted, and they have few options but to pay the ransom. In addition, some cyber insurance companies, during cost-benefit analysis, may find that paying the ransom is a less costly option than rebuilding systems and incurring credit monitoring and legal fees due to the disclosure of regulated data by an eCrime adversary.

CrowdStrike recommends the following practices:

- **Build a bulletproof backup strategy.** When it comes to ransomware, how you’ve configured your backups is critical. Attackers often delete backups before deploying ransomware so you are more inclined to pay. Some steps to consider include purchasing an immutable backup solution, using separate non-domain accounts with multi-factor authentication to administer your backup solution, retaining multiple copies of data on different media with one of them being off-site, keeping at least one copy of your backups offline or on an otherwise air-gapped network, and closely monitoring your backup solution for evidence of data exfiltration, whether it’s on-premises or in the cloud. eCrime adversaries have publicly boasted about utilizing cloud backups for data exfiltration, and CrowdStrike recommends taking steps to prevent threat actors from accessing cloud backup infrastructure in the event of a compromise. This can involve using non-domain accounts for cloud management and multi-factor authentication.
- **Use multi-factor authentication.** Organizations can improve their security posture by enabling multi-factor authentication on all public-facing employee services and portals as well as restricting internet-facing protocols such as RDP and Server Message Block. This will inhibit unauthorized access to the organization’s environment.
- **Implement next-generation endpoint protection.** Organizations can improve their security posture by utilizing advanced endpoint protection across their environment. The agent should leverage machine learning to identify anomalies and perform heuristic analysis, in addition to conducting antivirus and anti-malware activities in real time. The agent should be capable of detection and prevention, allow for remote network containment of assets pending investigation and/or remediation, and detect unmanaged assets within the corporate environment.

- **Know when to ask for help.** In some instances, organizations become aware of threat actor activity within their environment but may lack the visibility to address the problem or the right intelligence to understand the nature of the threat. Getting educated about the latest threats and knowing when to ask for help by activating an incident response team or retainer, such as those offered by CrowdStrike Services, may allow for detection and remediation before the threat actor is able to deploy ransomware or exfiltrate data from the environment.

Additional Resources

- *Download CrowdStrike Services Cyber Front Lines Report: Observations From the Front Lines of Incident Response and Proactive Services in 2020 and Insights That Matter for 2021.*
- *Watch the on-demand webcast: CrowdStrike Services Cyber Front Lines Report.*
- *Find out how CrowdStrike Services can help your organization answer its most important security questions: Visit the CrowdStrike Services webpage.*
- *Learn about CrowdStrike's comprehensive next-gen endpoint protection platform by visiting the Falcon products webpage.*
- *Visit the CrowdStrike Resource Center for Securing Your Remote Workforce.*
- *Test CrowdStrike next-gen AV for yourself: Start your free trial of Falcon Prevent™.*