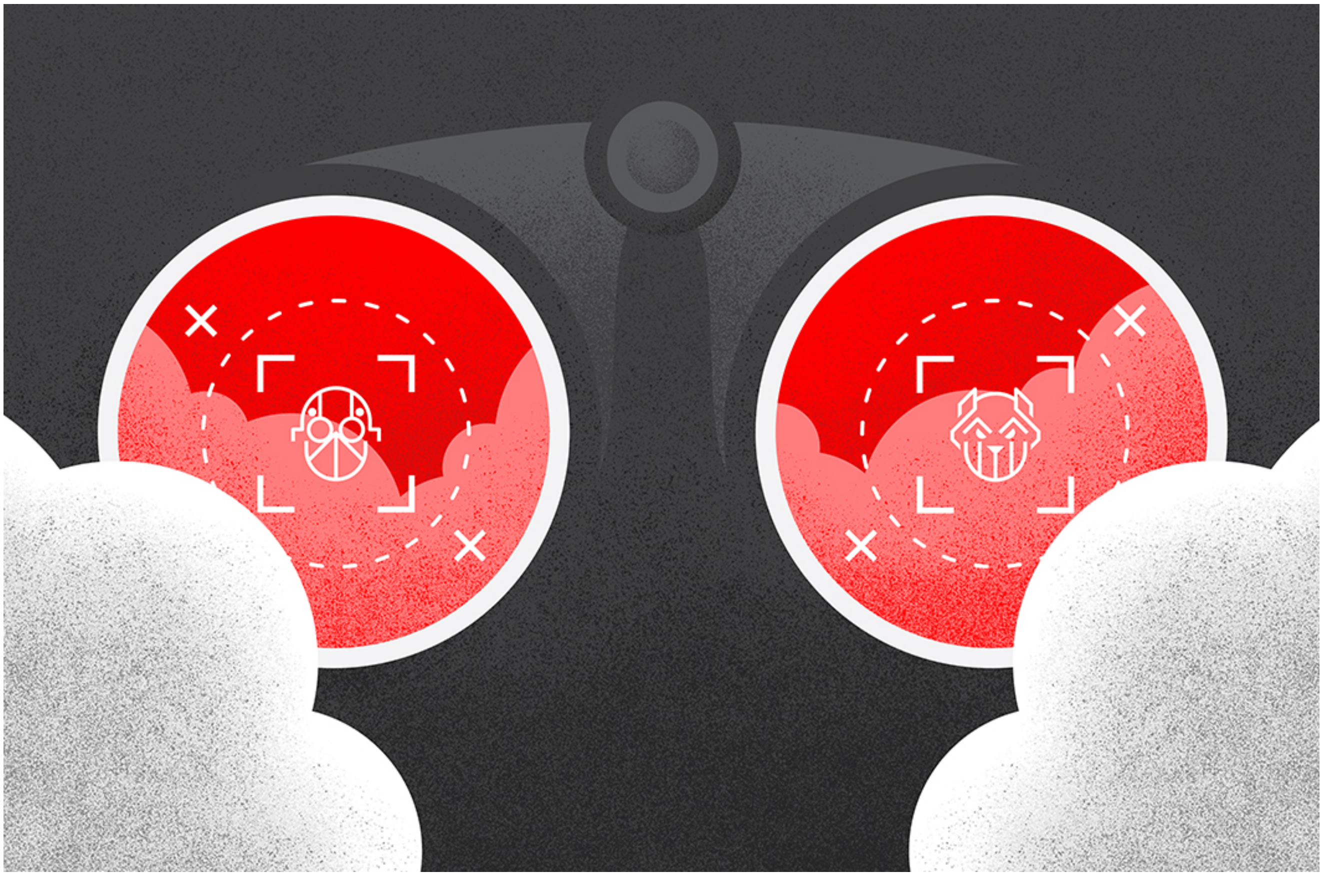
Big Game Hunting TTPs Continue to Shift After DarkSide Pipeline Attack

crowdstrike.com/blog/how-big-game-hunting-ttps-shifted-after-darkside-pipeline-attack/

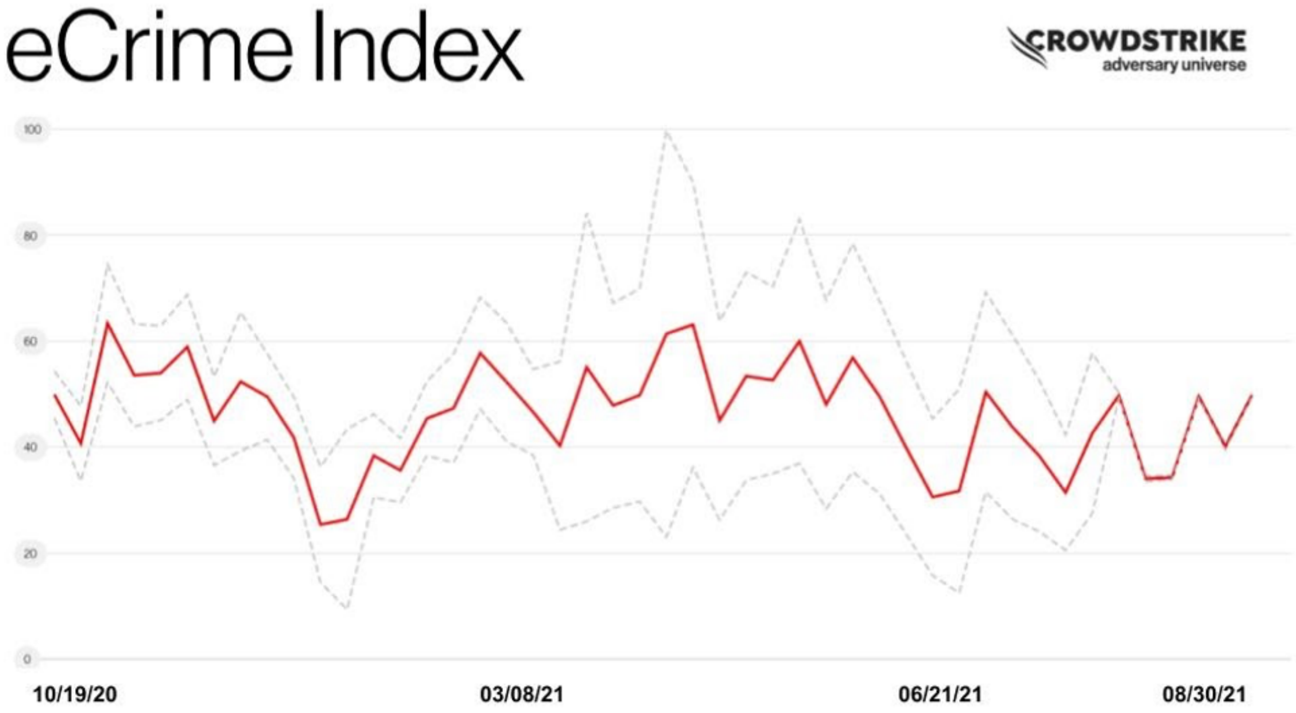
CrowdStrike Intelligence Team September 14, 2021



The eCrime ecosystem is an active and diverse economy of financially motivated threat actors engaging in a myriad of criminal activities to generate revenue. With the CrowdStrike eCrime Index (ECX), CrowdStrike's Intelligence team maintains a composite score to track changes to this ecosystem. The ECX is composed of several key observables covering different aspects of criminal activity that are combined using a mathematical model. In recent weeks, the Intelligence team observed a notable shift in big game hunting (BGH) activity and tactics, techniques and procedures (TTPs) that resulted in a downward trend of the ECX. As noted in a previous CrowdStrike Intelligence blog, the intense attention surrounding the Colonial Pipeline and JBS incidents had a significant impact on the criminal marketplace and the political landscape. Get more Intel updates on the latest eCrime activity and TTPs at Fal.Con, our annual cybersecurity conference, Oct. 12-14 — register for free today.

ECX Suggests Downward Trend in Ransomware Operations Following Colonial Pipeline Attack

By the time of the Colonial Pipeline attack on May 7, 2021, observed BGH ransomware incidents had reached a yearly high. However, publicly observable BGH activity declined throughout early June 2021, immediately after the incident, amid reports of mounting U.S. pressure to pursue BGH actors. A similar decline was also observed in the number of specific leaks posted to adversaries' dedicated leak sites (DLS). Despite the decline in the ECX, there has been sustained ransomware activity, likely indicating that a number of adversaries are remaining active despite the dismantling of other groups.



BGH Actor Developments

BGH adversaries responded to the Colonial Pipeline ransomware incident and the resulting widespread media coverage in many ways. Some named actors shuttered ransomware-as-a-service (RaaS) affiliate programs — at least publicly — while others have continued deploying ransomware.

CARBON SPIDER (operators of *DarkSide* ransomware) continues to create active command-and-control (C2) servers to deploy their *Domenus PS* backdoor and *Cobalt Strike* post-exploitation framework. The activation of new C2 servers demonstrates that CARBON SPIDER has not halted activities despite allegedly losing control of *DarkSide*-related infrastructure and having their ransomware funds seized by the U.S. government.[1] However, in late July 2021, CrowdStrike Intelligence observed a new ransomware called *BlackMatter* being distributed. Code overlaps indicate that *BlackMatter* is highly likely the successor of CARBON SPIDER's *DarkSide* ransomware. CARBON SPIDER has also created a Linux version of *BlackMatter* that resembles the Linux version of *DarkSide* in multiple ways. After taking a short break, CARBON SPIDER reinstated their BGH operations involving this RaaS and have stated that they have an interest in purchasing and executing unauthorized access to corporate networks.

RIDDLE SPIDER (operators of *Avaddon* ransomware) closed down their operations in late June. Earlier in June 2021, media sources allegedly received emails containing a password and links to 7zip files containing *Avaddon* ransomware decryption keys.[2] RIDDLE SPIDER's DLS also went offline in June. While CrowdStrike Intelligence cannot confirm RIDDLE SPIDER's motivations for closing down the *Avaddon* RaaS, the decision was likely influenced by the Colonial Pipeline incident and its resulting effects throughout the ransomware industry.

GRACEFUL SPIDER had several members of their group arrested on June 16, 2021, by a joint international law enforcement operation.[3] These members were involved in laundering cryptocurrency funds acquired through the use of GRACEFUL SPIDER's *Clop* ransomware. The immediate impact to GRACEFUL SPIDER operations resulting from these arrests is currently unclear. GRACEFUL SPIDER's DLS site remains active after the arrests, with two new listings in June, indicating they have not ceased their activity.

PINCHY SPIDER (developers and operators of the popular *REvil* RaaS) continued operating at a high pace throughout June and early July 2021, and the group introduced a new ransomware named *REvix,* which is used to target ESXi and Linux environments. However, on the morning of July 13, 2021, PINCHY SPIDER's *REvil* infrastructure supporting their DLS and payment portal went offline. On the same day, the forum administrator of the Russian-language criminal forum XSS banned the actor *Unknown* (aka *UNKN*), who has acted as the public spokesperson for PINCHY SPIDER since 2019. PINCHY SPIDER had released *REvil* version 2.08 a few days prior, confirming the ransomware was under active development, and version 1.2 of *REvix* was observed on July 23.

On Sept. 7, after an approximately three month hiatus, CrowdStrike Intelligence observed PINCHY SPIDER's *REvil* infrastructure come back online. Financial activity in terms of BTC transactions from previously identified *REvil* addresses was also detected on Sept. 5.

On June 4, a sample of INDRIK SPIDER's *Hades* ransomware was identified using the name *PAYLOADBIN*, similar to *Babuk Locker*'s DLS site Payload.bin. INDRIK SPIDER likely switched the names in an effort to avoid attribution by law enforcement and therefore avoid Office of Foreign Assets Control (OFAC) sanctions. Prior to this recent name change, INDRIK SPIDER attempted to change the names of *Hades* and their *Phoenix CryptoLocker* ransomware at least one other time to avoid OFAC sanctions. The changes made to avoid these sanctions indicates that INDRIK SPIDER desires to continue their deployment of ransomware.

In July 2021, CrowdStrike Intelligence determined that *Grief* ransomware is developed by DOPPEL SPIDER, likely as an intended successor to *DoppelPaymer* ransomware. The cessation in *DoppelPaymer* activity coincided with the emergence of the *Grief* DLS that was first observed in May. Analysis of recently identified *Grief* samples indicates a number of technical overlaps with DOPPEL SPIDER's wider toolset that provides a definitive link to the adversary.

WIZARD SPIDER continues to actively deploy *Conti* ransomware and update the *Conti* DLS. In June 2021, WIZARD SPIDER continued to target large entities in Europe and the United States, including organizations in real estate, education and local government. Recent developments related to the Colonial Pipeline and JBS incidents have not slowed down WIZARD SPIDER's ransomware operations. This indicates WIZARD SPIDER remains largely unaffected by external pressure, similar to their response to the September 2020 takedown efforts targeting *TrickBot* infrastructure.

Outlook

The confluence of U.S. and international law enforcement pressure and forum bans on ransomware activity has led to a highly fluid and chaotic situation in the eCrime ecosystem. The ECX has indicated a change in BGH activity May through June 2021 as well as the persistence of ongoing BGH incidents at a level observed in the first quarter of 2021. However, the downward trend in BGH victims posted to DLSs in June likely indicates that some BGH actors have shifted TTPs to make tracking their activity more difficult.

Numerous adversaries have shown themselves keen to take advantage of the situation and to attract new affiliates. These adversaries have explicitly expressed their intent to continue ransomware operations despite reports of possible U.S.-Russian collaboration — or more aggressive unilateral enforcement actions by the U.S. — in response to incidents, suggesting that a complete drop in BGH activity is highly unlikely to occur in the near future.

The ECX remains a valuable tool used to identify significant events affecting the eCrime ecosystem. The ECX provides an easily referenced index to mark areas of disruption or change in the eCrime ecosystem in real time.

Monitor the ECX regularly in the CrowdStrike Adversary Universe to make sure you stay up-to-date on eCrime trends.

Endnotes

1. https[:]//www.justice[.]gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside
2. https[:]//www.bleepingcomputer.com/news/security/avaddon-ransomware-shuts-down-and-releases-decryption-keys/

3. https[:]//www.npu.gov[.]ua/news/kiberzlochini/kiberpolicziya-vikrila-xakerske-ugrupovannya-u-rozpovsyudzhenni-virusu-shifruvalnika-ta-nanesenni-inozemnim-kompaniyam-piv-milyarda-dolariv-zbitkiv/

Additional Resources

- *Learn how Falcon X Recon™ mitigates digital risk from the deep, dark web and beyond.*
- *Read about BGH adversaries tracked by CrowdStrike Intelligence in 2020 in the CrowdStrike 2021 Global Threat Report.*
- *To find out how to incorporate intelligence on threat actors into your security strategy, visit the Falcon X™ Threat Intelligence page.*
- *Learn about the powerful, cloud-native CrowdStrike Falcon® platform by visiting the product webpage.*
- *Get a full-featured free trial of CrowdStrike Falcon Prevent™ and learn how true next-gen AV performs against today's most sophisticated threats.*