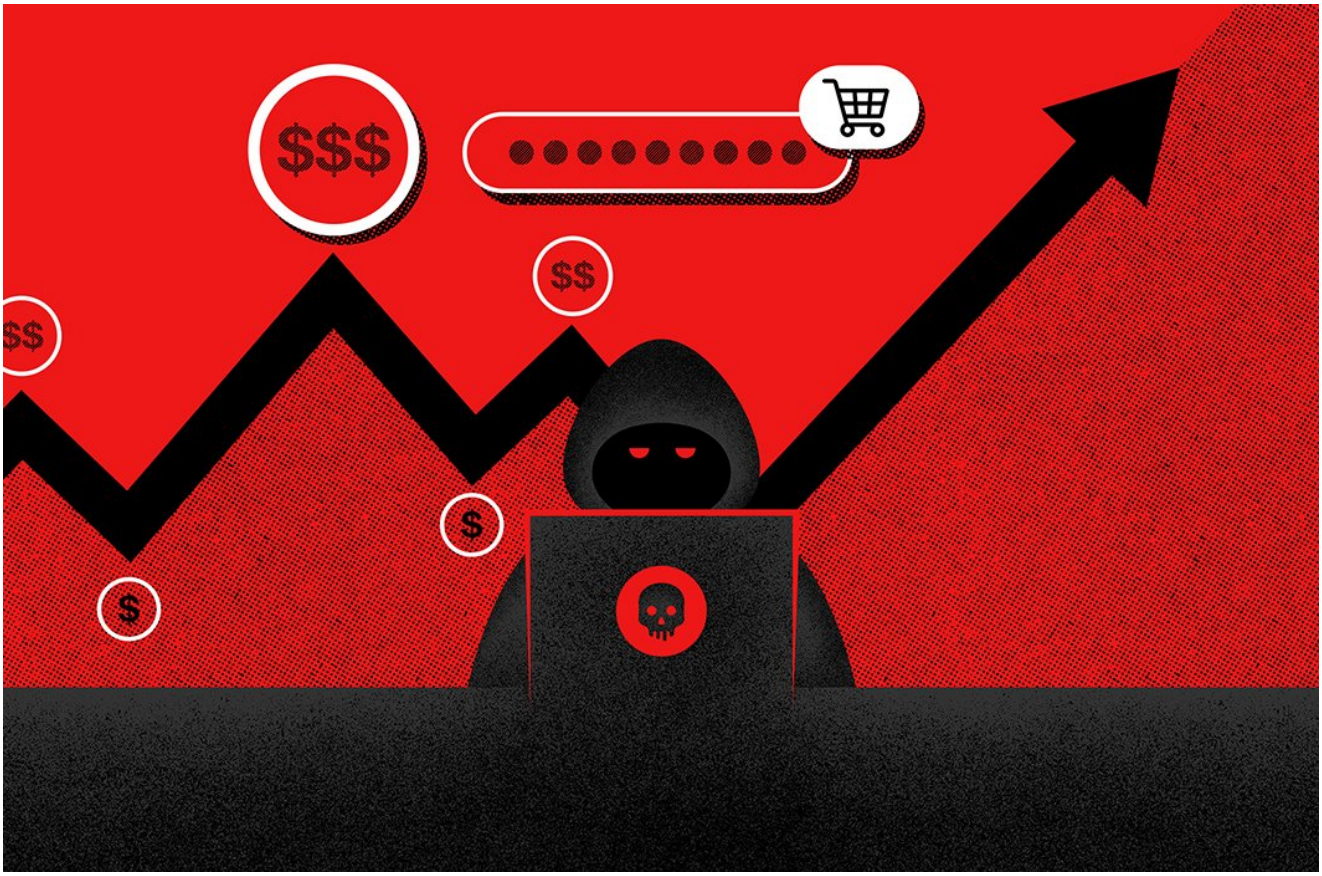
Big Game Hunting on the Rise Again According to eCrime Index

crowdstrike.com/blog/big-game-hunting-on-the-rise-again-according-to-ecrime-index/

CrowdStrike Intelligence Team October 12, 2021



This announcement is part of the Fal.Con 2021 CrowdStrike Cybersecurity Conference, Oct. 12-14. Register now for free to learn all about our exciting new products, partnerships and latest intel!

The eCrime ecosystem is an active and diverse economy of financially motivated threat actors engaging in a myriad of criminal activities to generate revenue. CrowdStrike Intelligence maintains the CrowdStrike eCrime Index (ECX) to provide a composite score for tracking 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.

Since a CARBON SPIDER *DarkSide* affiliate infected Colonial Pipeline in May 2021, CrowdStrike Intelligence observed big game hunting (BGH) adversaries slow or cease their activity and change their tactics, techniques and procedures (TTPs), resulting in a downward trend in the ECX. However, in recent weeks, the ECX has mirrored a resurgence in BGH ransomware data leaks and demonstrated an uptick in activity.

Surge in Data Leaks

In the week prior to the Colonial Pipeline incident, BGH ransomware incidents that resulted in data leaks had reached an all-time high of 92. Following the incident, many ransomware families significantly reduced their operational tempo or ceased operations, likely in an attempt to avoid the increased scrutiny that ransomware campaigns attracted. Figure 1 illustrates the ransomware data leak activity observed since the CARBON SPIDER affiliate Colonial Pipeline infection (highlighted in white).

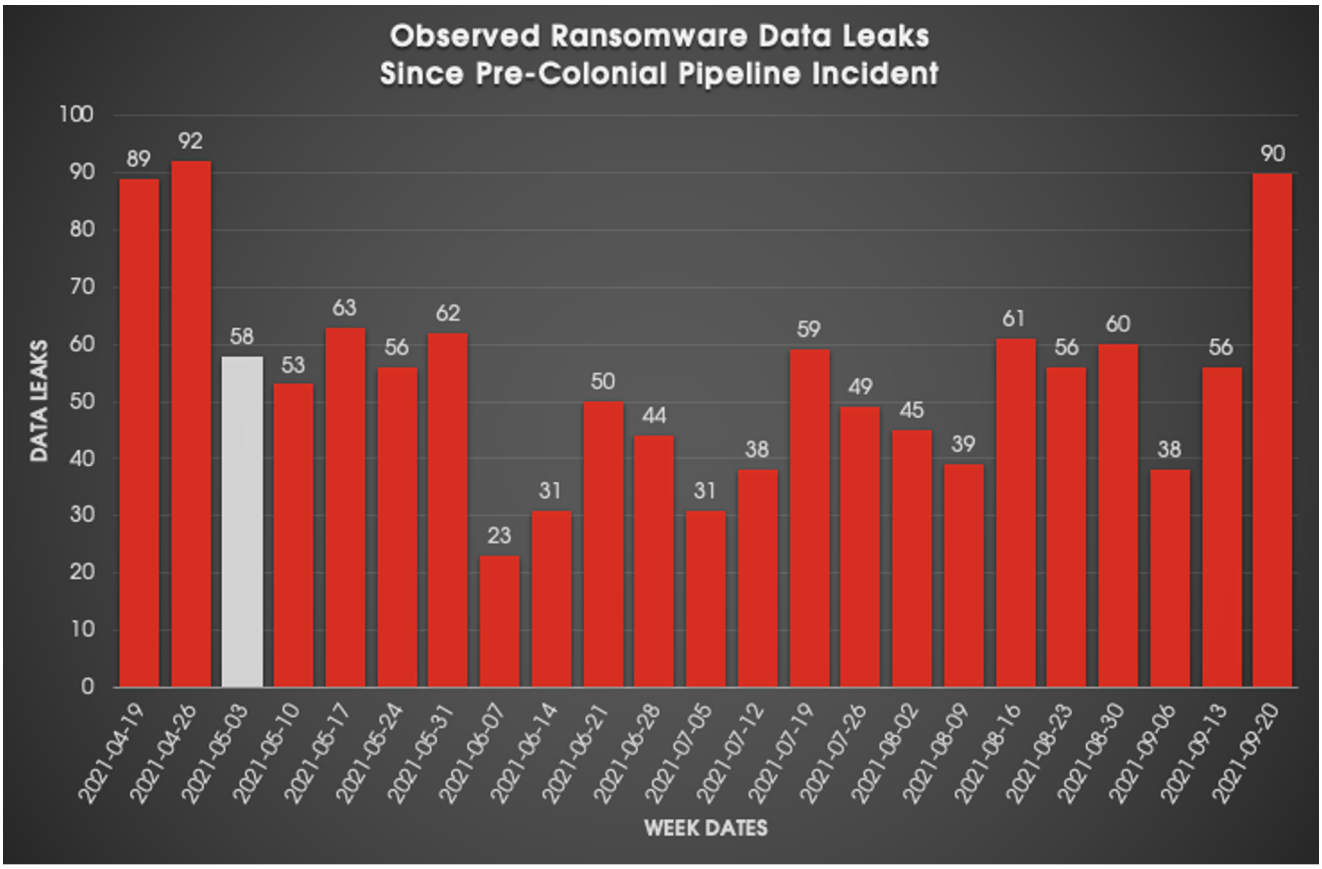


Figure 1. Number of BGH ransomware data leaks by week since the Colonial Pipeline incident

The reduction of incidents following the week beginning May 3, 2021, is likely attributed to a combination of factors:

- Increased scrutiny of ransomware threat actors
- Banning of forum activity related to ransomware operations
- The reported retirement of adversaries, such as CIRCUS SPIDER (*Netwalker*) and RIDDLE SPIDER (*Avaddon*)
- The disappearance of prolific threat actors, such as PINCHY SPIDER (*REvil*)
- Disruption within certain groups, such as the operators of *Babuk Locker*, who have split into multiple groups and diversified their respective offerings

However, in the past few weeks, CrowdStrike Intelligence has observed ransomware data leak incidents reach 90 — representing the highest peak since the dip. This surge in data leaks is very likely due to the return of PINCHY SPIDER's *REvil* ransomware as a service (RaaS), the increase in CARBON SPIDER's *BlackMatter* RaaS activity, and the prolific operational tempo of *LockBit* RaaS, which is responsible for 220 data leaks since it returned in July 2021; the *LockBit* data leaks account for more than 36% of the leaks since their huge resurgence.

CrowdStrike Intelligence has also observed forum activity from or associated with BGH actors continuing, despite restrictions put in place by admins in July 2021. Some notable topics observed include:

- RaaS projects and other posts related to ransomware partnerships continue to be posted and advertised in forums.
- Groups such as *LockBit* have recently advertised they were looking for penetration testers for "red team operations" in a style of language designed to mirror that found in legitimate cybersecurity job postings.
- Separately, other actors have resorted to advertising ransomware partnerships on RAMP — a forum purportedly established by *Babuk Locker* operators specifically for ransomware-related chatter.

ECX Reflections

While the ECX models a wide range of data points within the eCrime marketplace, it is clear that a recent surge in data leaks is reflected in the ECX. Also having a significant impact on the ECX is the number of high ransom demands. For example, PINCHY SPIDER *REvil* affiliates have been observed issuing a ransom demand of $80 million USD, and CARBON SPIDER's *BlackMatter* affiliates have been observed demanding as much as $60 million USD in the past weeks. The combination of these factors has resulted in a significant increase in the ECX (Figure 2).

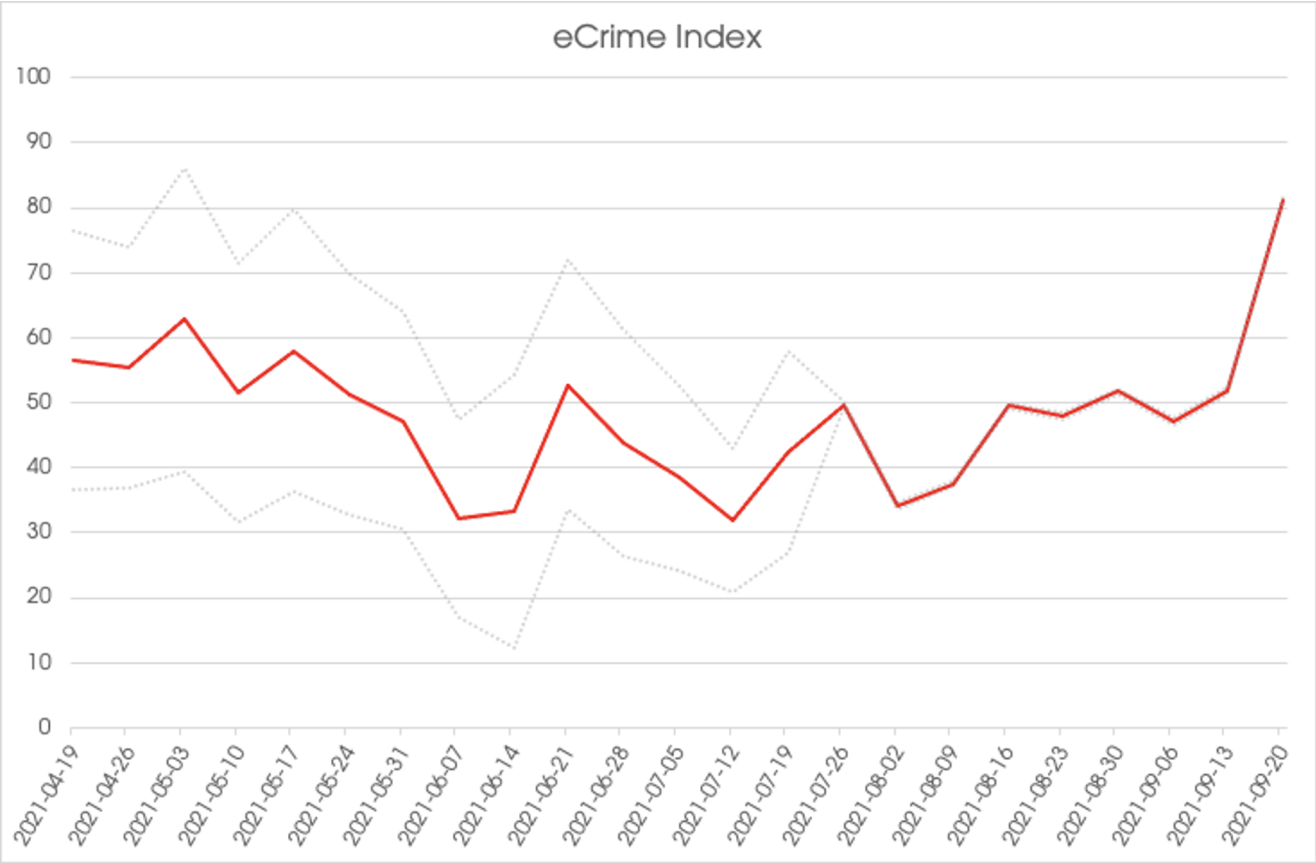


Figure 2. ECX values by week since the Colonial Pipeline incident

Outlook

Attempts by the Biden administration to put political pressure on the Russian government to assist in clamping down on BGH actors do not appear to have borne fruit. Although some groups have stated they will avoid targeting certain sectors, these pledges have proven to be rather limited.

Despite increased law enforcement attention following a *REvil* attack on the U.S.-based food processing company JBS in May 2021, some BGH actors remain willing to continue targeting major and possibly critical companies. For example, on Sept. 18, 2021, a *BlackMatter* operator attempted to ransom a North American agricultural cooperative for more than $11 million USD despite this business being clearly identified as critical infrastructure by the U.S. Department of Homeland Security.

The CrowdStrike Intelligence ECX is mathematically calculated using multiple tracked observables. Over the past few weeks, the increase of ransomware data leaks — and a consistent number of high ransom demands — has resulted in a substantial upward trend, which is likely to continue in the short term. This assessment is made with moderate confidence based on the continuation of BGH actors restoring to their prior operational tempo, as well as new and existing ransomware operators emerging and maturing.

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.

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.*