CARBON SPIDER Embraces Big Game Hunting, Part 2

crowdstrike.com/blog/carbon-spider-embraces-big-game-hunting-part-2/

Eric Loui - Josh Reynolds November 4, 2021

In 2020, CARBON SPIDER began conducting big game hunting (BGH) ransomware campaigns with PINCHY SPIDER's *REvil* before introducing *Darkside*. The adversary later opened up *Darkside* to affiliates through a ransomware-as-a-service (RaaS) program, allowing other actors to use the ransomware while paying CARBON SPIDER a portion of the received ransom.

The first part of this two-part blog series explored CARBON SPIDER's initial BGH campaigns in depth. This blog discusses the *Darkside* ransomware incident at U.S. oil pipeline system Colonial Pipeline in May 2021 and how CARBON SPIDER responded to fallout from this event. Despite the termination of the *Darkside* program, the adversary continued malware distribution campaigns and subsequently introduced the *BlackMatter* RaaS. Due to numerous technical overlaps with *Darkside*, *BlackMatter* is attributed to CARBON SPIDER.

Colonial Pipeline Incident

On May 8, 2021, Colonial Pipeline disclosed that it had been the victim of a ransomware incident the day before;[1] however, it would be several days until the FBI indicated that Colonial Pipeline fell victim to *Darkside* ransomware.[2] On May 9, 2021, a ransom payment of approximately $4.4 million USD (75 BTC) was made to a probable *Darkside* affiliate. The U.S. Department of Justice (DOJ) later announced the seizure of the affiliate's portion of this payment.[3]

On May 10, 2021, CARBON SPIDER posted a response to media attention to the Colonial Pipeline incident on the *Darkside* dedicated leak site (DLS) stating they are "apolitical," do not participate in "geopolitics," and that their "goal is to make money, and not creating problems for society." The post further mentioned a vetting process for all victims, providing further evidence that the Colonial Pipeline incident was conducted by an affiliate rather than the core CARBON SPIDER group. These statements were likely made in an attempt to correct certain public speculation that the attack was politically motivated.

A statement on May 13, 2021 — purportedly from CARBON SPIDER — claimed the adversary group lost access to the *Darkside* DLS, payment servers and content delivery network (CDN) servers. The statement also claimed CARBON SPIDER servers had been blocked "at the request of law enforcement agencies." Since then, CrowdStrike Intelligence has not observed any new valid *Darkside* samples, indicating this date marked the end of the *Darkside* RaaS. Separately on May 13, 2021, several forum administrators banned posts relating to ransomware, likely to avoid media attention.

Subsequent CARBON SPIDER Operations

Despite *Darkside*'s termination, CARBON SPIDER did not cease their operations or entirely abandon prior tooling. On May 25, 2021, CrowdStrike Falcon Complete and Falcon OverWatch detected a SQL injection incident that delivered a PowerShell (PS) stager tracked by CrowdStrike Intelligence as *Demux*.

From May 31 through June 29, 2021, CARBON SPIDER used malicious Microsoft Excel and Word documents as well as *Leo VBS* to distribute an updated version of *JSS Loader*. This version of *JSS Loader* — written in C++, compared to its .NET progenitor — introduced a new packer.

On July 9 and 12, 2021, CARBON SPIDER used malicious Microsoft Word documents to distribute the *Harpy* backdoor. These documents used Windows 11 Alpha-themed content identical to lure content used in a *JSS Loader* campaign (Figure 1).

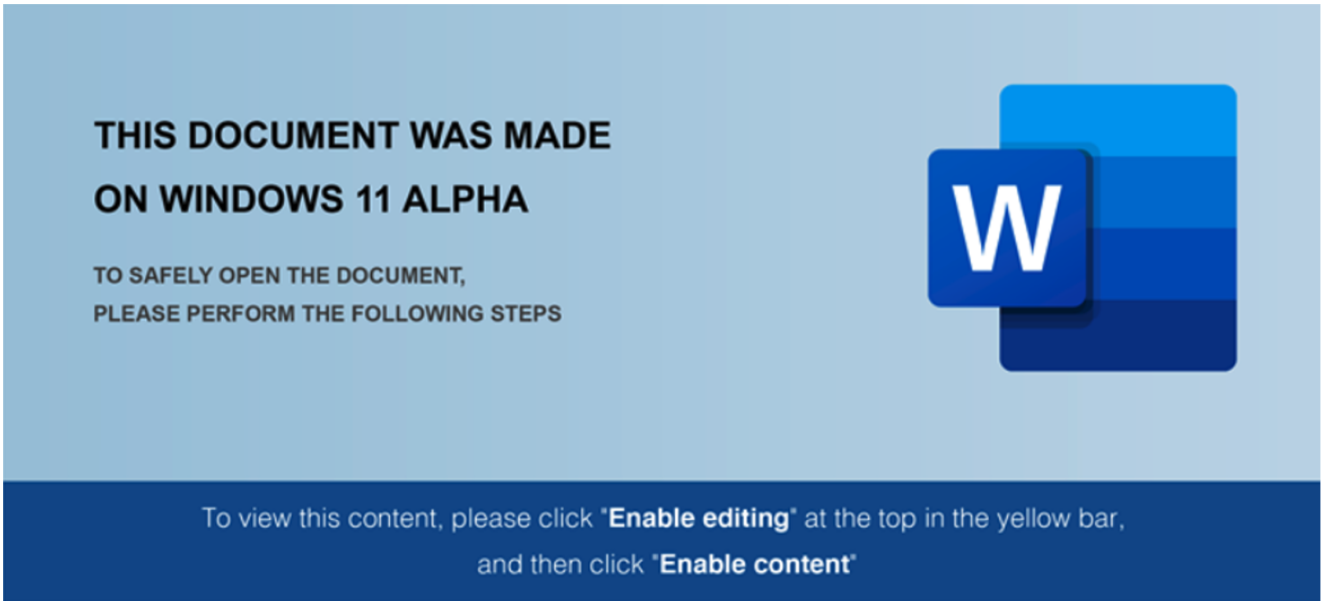

Figure 1. JSS Loader/Harpy document content

In this campaign, after *Harpy* successfully contacted its command-and-control (C2) server, a JavaScript system enumeration module was delivered and executed by *Harpy*. This enumeration module strongly resembles a PS system enumeration module written for the *Domenus* suite, providing evidence that both tools share a common developer.

In June 2021, a probable CARBON SPIDER actor deployed the open-source *Hidden Tear* ransomware during a ransomware operation. This incident was attributed to CARBON SPIDER based on prior use of the *Demux* stager and the *Sekur* Remote Access Tool (RAT) to establish persistent access, in addition to *Cobalt Strike*. This incident marks the first known CARBON SPIDER ransomware campaign following the Colonial Pipeline incident; CARBON SPIDER likely chose to use *Hidden Tear* to avoid attracting additional attention.

BlackMatter

On 21 July 2021, a Russian-language forum member named *BlackMatter* sought to purchase access to a variety of corporate networks. The actor specifically expressed interest in the U.S., Canada, Australia and the UK, and expressed disinterest in targeting medical or government institutions. Subsequent CrowdStrike Intelligence analysis confirmed that *BlackMatter* is provided to affiliates via a RaaS program, similar to *Darkside*.

Windows PE and Linux ELF versions of *BlackMatter* were subsequently obtained and analyzed. Extensive coding similarities indicate *BlackMatter* is highly likely the successor to *Darkside*. Windows version overlaps include:

- Building an import address table at runtime using dynamic function resolution
- Using aPLib to decompress the embedded ransomware configuration
- Overlaps in configuration formats and multiple configuration items

- Using the same file encryption system, including using Salsa20 to encrypt files through a randomly generated state matrix and protecting the state matrix with an embedded RSA-1024 key
- Using two HTTP C2 requests before and after file encryption containing system information and encryption statistics
- Using Windows Management Instrumentation (WMI) for shadow copy deletion

Linux version overlaps include:

- A Red Hat Linux build environment
- Being written in C++ and compiled using GCC with statically linked libcurl, Boost and CryptoPP libraries
- Using the CryptoPP `RandomPool` random number generator to produce symmetric keys
- Using an embedded RSA-4096 public key to protect generated symmetric keys
- Using an embedded configuration that specifies an RSA-4096 public key, an allowlist of file extensions to encrypt, a thread count to use during encryption, a debug log file path and C2 domains
- All *BlackMatter* extension allowlist values exist within *Darkside*'s configuration
- Performing a C2 request via cURL containing embedded system information
- Placing a hard-coded URL containing a unique URL string within the ransom note to the victim payment portal
- The ability to stop ESXi virtual machines using `esxcli`
- The ability to enumerate ESXi volumes for encryption using `esxcli`

BlackMatter ransom notes direct victims to communicate via a portal hosted on Tor. If victims do not pay ransom demands, stolen files are typically posted on a DLS that is also hosted on Tor. CrowdStrike Intelligence has identified *BlackMatter* victims spanning numerous sectors across North and South America, Asia and Europe.

Conclusion and Outlook

CrowdStrike Intelligence assesses CARBON SPIDER is highly likely behind the development of *BlackMatter* and operating the *BlackMatter* RaaS. This assessment carries high confidence based on the extensive amount of technical overlaps between *Darkside* and *BlackMatter*. CARBON SPIDER's resilience and launch of *BlackMatter* shortly following the termination of *Darkside* demonstrates how difficult it is to disrupt cybercrime adversaries and their operations. The potential profits from ransomware are evidently worth risking potential law enforcement actions. Without fundamental changes in the economics of cybercrime, CARBON SPIDER and other actors will likely continue to provide RaaS programs to affiliates.

Indicators of Compromise

Type	SHA256 Hash
JSS Loader C++ version	`1414704797a7ecbbd0fb0ae48207bdef367697eafddd70fd646e4662a77a30d6`
BlackMatter Windows	`22d7d67c3af10b1a37f277ebabe2d1eb4fd25afbd6437d4377400e148bcc08d6`
BlackMatter Linux	`6a7b7147fea63d77368c73cef205eb75d16ef209a246b05698358a28fd16e502`

Table 1. Exemplar SHA256 Hashes of CARBON SPIDER Malware

CrowdStrike Confidence Assessment Definitions

- **High Confidence**: Judgments are based on high-quality information from multiple sources. High confidence in the quality and quantity of source information supporting a judgment does not imply that that assessment is an absolute certainty or fact. The judgment still has a marginal probability of being inaccurate.
- **Moderate Confidence**: Judgments are based on information that is credibly sourced and plausible, but not of sufficient quantity or corroborated sufficiently to warrant a higher level of confidence. This level of confidence is used to express that judgments carry an increased probability of being incorrect until more information is available or corroborated.
- **Low Confidence**: Judgments are made where the credibility of the source is uncertain, the information is too fragmented or poorly corroborated enough to make solid analytic inferences, or the reliability of the source is untested. Further information is needed for corroboration of the information or to fill known intelligence gaps.

Endnotes

1. https[:]//www.colpipe[.]com/news/press-releases/media-statement-colonial-pipeline-system-disruption
2. https[:]//www.fbi[.]gov/news/pressrel/press-releases/fbi-statement-on-compromise-of-colonial-pipeline-networks
3. https[:]//www.justice[.]gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside

Additional Resources

- *For more intel about CARBON SPIDER, visit the CrowdStrike Adversary Universe.*
- *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™ to see for yourself how true next-gen AV performs against today's most sophisticated threats.*