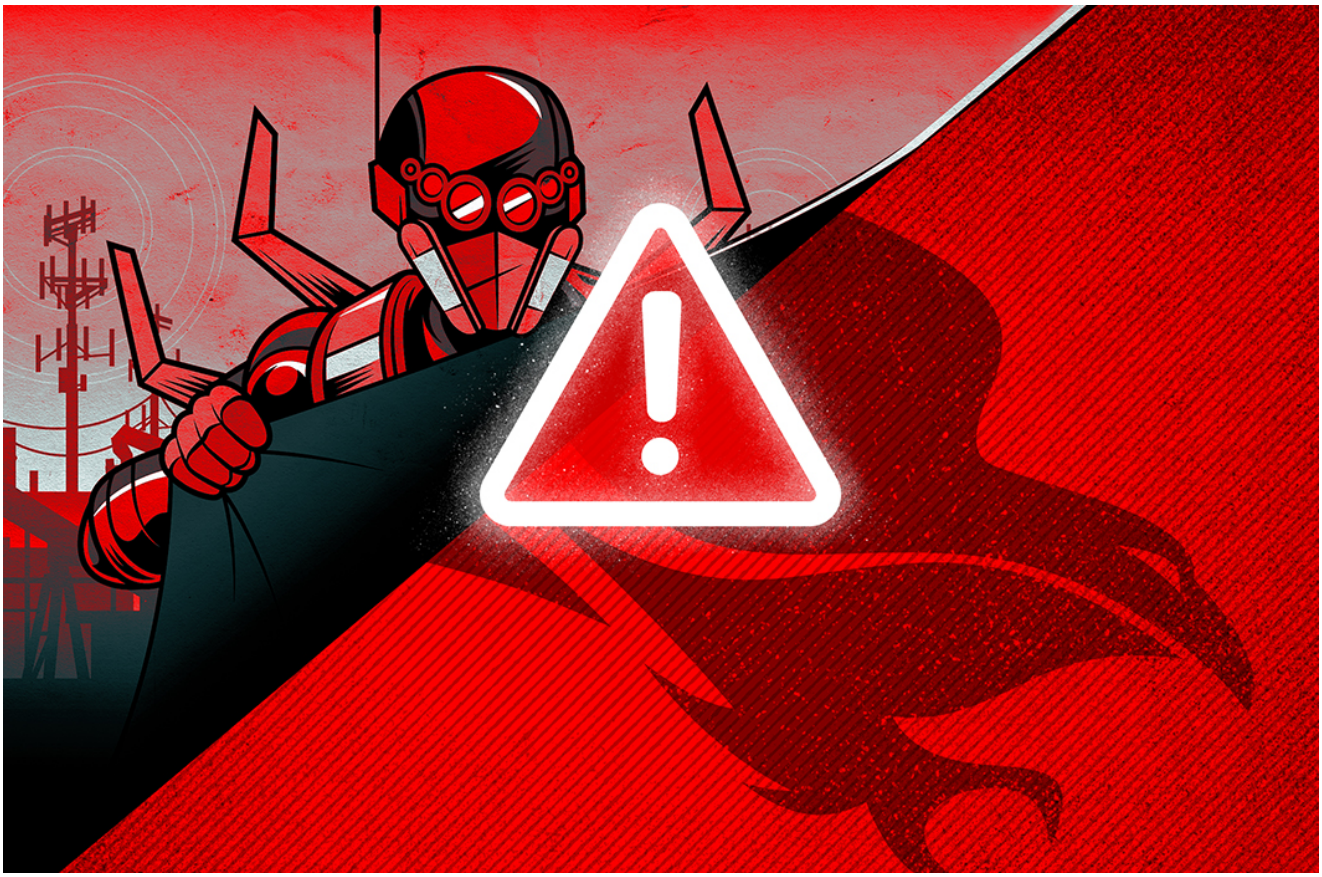
CARBON SPIDER Embraces Big Game Hunting, Part 1

crowdstrike.com/blog/carbon-spider-embraces-big-game-hunting-part-1/

Eric Loui - Josh Reynolds August 30, 2021



Throughout 2020, CARBON SPIDER dramatically overhauled their operations. In April 2020, the adversary abruptly shifted from narrow campaigns focused entirely on companies operating point-of-sale (POS) devices to broad, indiscriminate operations that attempted to infect very many victims across all sectors. The goal of these campaigns was to conduct big game hunting (BGH) operations using PINCHY SPIDER's *REvil* ransomware.

CARBON SPIDER deepened their commitment to BGH in August 2020 by using their own ransomware, *Darkside*. In November 2020, the adversary took another step into the world of BGH by establishing a ransomware-as-a-service (RaaS) affiliate program for *Darkside*, allowing other actors to use the ransomware while paying CARBON SPIDER a portion of the ransom received.

Part One of this two-part blog series details how CrowdStrike Intelligence attributed *Darkside* to CARBON SPIDER. Part Two will look at CARBON SPIDER's re-emergence after the Colonial Pipeline attack, which led to the shutdown of *Darkside* RaaS and the creation of *BlackMatter* RaaS.

Background

CARBON SPIDER, commonly referred to as FIN7 and active since 2013, is one of the oldest continuously operating eCrime groups. Between 2015 and 2020, the adversary conducted low-volume campaigns targeting company POS devices, primarily in the hospitality sector. These campaigns featured a variety of malware, including the *Sekur* (*Carbanak*) RAT, *VB Flash*, *Bateleur* and *Harpy* (*GRIFFON*). Using POS malware, including *PILLOWMINT*, the adversary harvested credit card track data and sold this data on criminal forums such as Joker's Stash.

April 2020: Target Scope Widens

In April 2020, CARBON SPIDER abruptly shifted from narrow campaigns focused entirely on companies operating POS devices to broad, indiscriminate operations that attempted to infect large numbers of victims across all sectors. The first of these occurred on April 14, 2020, when the adversary likely compromised a legitimate email distribution service to conduct a broad spam campaign targeting thousands of recipients across numerous verticals.

This campaign used malicious links that led to a ZIP archive hosted on `https[:]//colahasch[.]com/portal/app/CommerceNetwork/view/9b25068f2941618fb9b08d6d089a47faae552c93f` The ZIP archive contained a *Leo VBS*, which refers to a family of obfuscated scripts that download and execute a remote payload.

The *Leo VBS* performs an HTTP GET request to `https[:]//alphalanding[.]com/successfully/warranty.eml?uid=` and writes a *JSS Loader* binary to `%TEMP%\PaintHelper.exe`. *JSS Loader*, which has both .NET and C++ versions, has multiple capabilities, including the ability to load additional executables, PowerShell (PS) and JavaScript (JS) files.

The observed JSS Loader infection led to the download and execution of a setup VBScript from `https[:]//petshopbook[.]com`. This script installs a custom *Sekur* PS stager to `%LOCALAPPDATA%\Microsoft\WindowsDefender\ClearTemp.ps1` and establishes persistence for this stager with a second VBS that is launched by a scheduled task.

Since this campaign, CARBON SPIDER has maintained an opportunistic target scope, using phishing attachments and links to deliver *Harpy, Leo VBS, JSS Loader, Domenus VBS* and *Domenus JS*. *Domenus VBS* and *JS* are backdoors (written in VBS and JS, respectively) that enumerate a variety of system information, capture screenshots and browser history, and can download secondary payloads from a command-and-control (C2) server. Secondary payloads can include JS, Portable Executables (PEs), DLLs and PS scripts.

CrowdStrike Intelligence observed numerous *Domenus VBS/JS* phishing campaigns that made use of compromised and legitimate services to host *Domenus* toolchain payloads, including compromised WordPress installations, compromised SharePoint services, compromised web servers and Google Docs.

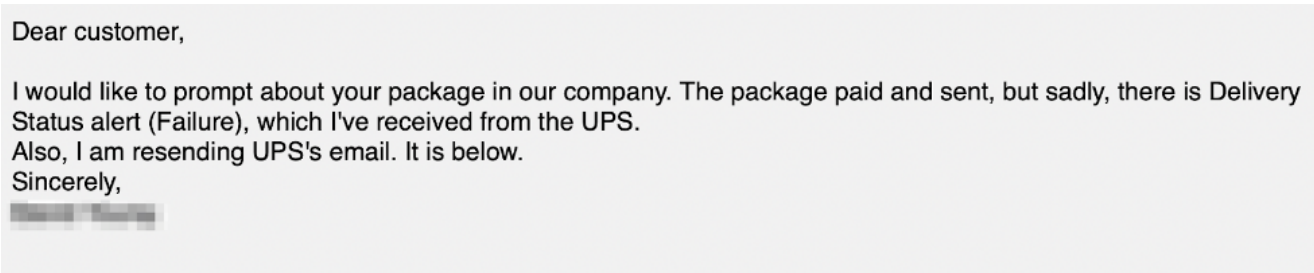
REvil Ransomware Campaigns

On April 28, 2020, CrowdStrike Intelligence observed a *Domenus VBS* distribution campaign that used a spear-phishing email containing a Google Docs link. The resulting Google Docs page contained a second link that, when clicked, directed the user to `https[:]//chauvinistable[.]com/perfsecure`, ultimately redirecting to a compromised SharePoint site. Here, the victim encountered a ZIP file containing a *Domenus VBS* file that, once opened, downloaded and executed *Harpy* from `https[:]//electroncador[.]com/info`.

The redirect URL provided from the Google Docs page `https[:]//chauvinistable[.]com/perfsecure` was hosted on the same IP address (`185.163.45[.]249`) resolving to a domain used by multiple *Cobalt Strike* samples sharing key configuration metadata with *Cobalt Strike* samples used in several *REvil* incidents. These *Cobalt Strike* samples were also observed in tandem with the custom PowerShell stager for *Sekur*. Separate reporting by Symantec further indicated that similar *Cobalt Strike* samples were used in campaigns delivering *REvil*. Based on these multiple overlaps, CrowdStrike Intelligence assesses with moderate confidence that CARBON SPIDER was responsible for certain *REvil* campaigns, likely stemming from *JSS Loader* or *Domenus VBS/JS* infections.

Darkside Ransomware Campaigns + RaaS

On July 1, 2020, CARBON SPIDER sent a phishing email with the subject “Notification: Package Status Fail.” The email purports to be from a customer who received an email from the U.S.-based delivery company UPS (Figures 1 and 2). The message body attempts to impersonate a UPS notification, but contains several grammar errors and non-idiomatic terms (e.g., “waybill”).


Dear customer,

I would like to prompt about your package in our company. The package paid and sent, but sadly, there is Delivery Status alert (Failure), which I've received from the UPS.
Also, I am resending UPS's email. It is below.
Sincerely,

Figure 1. CARBON SPIDER phishing email

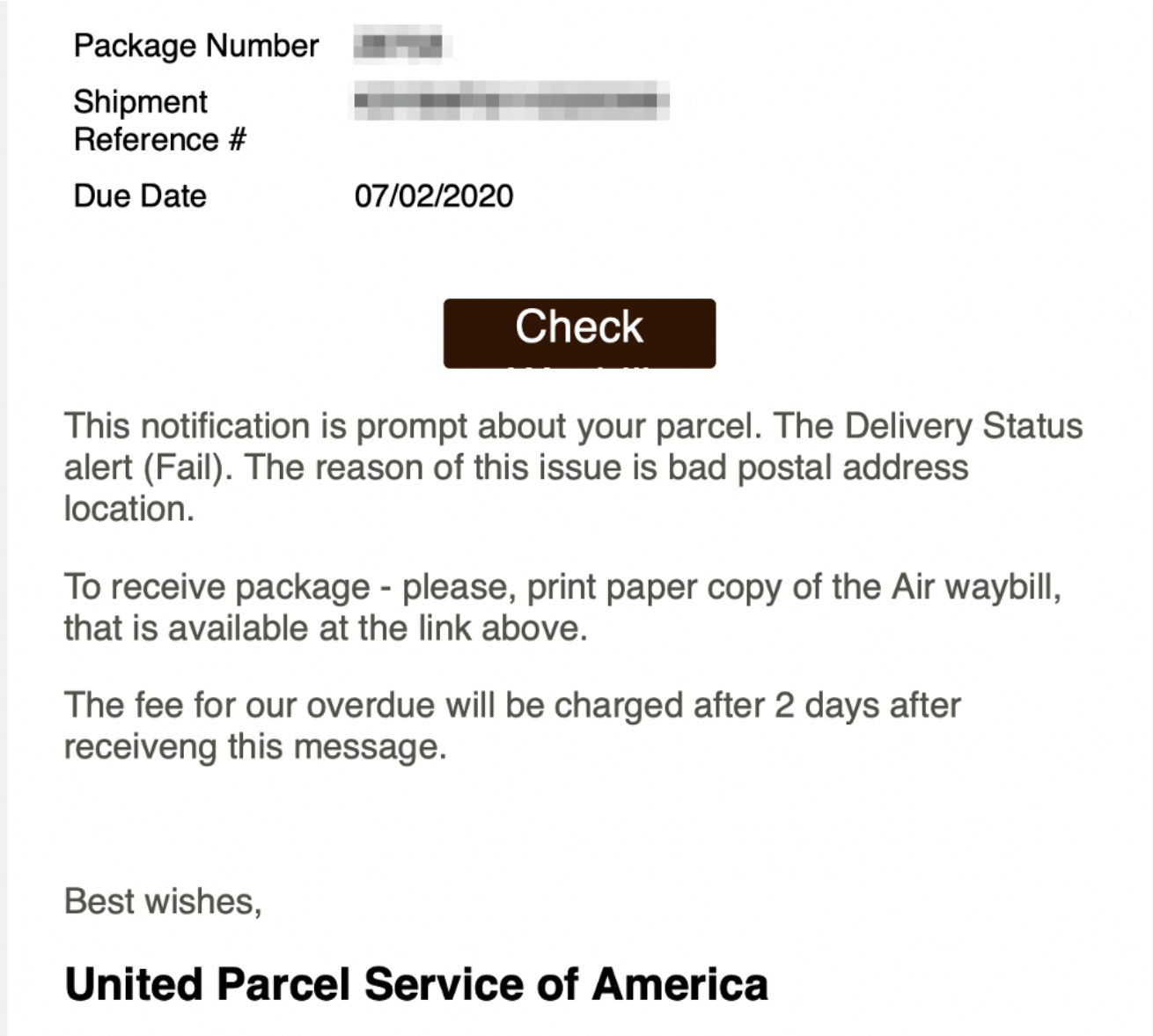


Figure 2. CARBON SPIDER phishing email (continued)

The link “Check” led to a Google Docs page, which contained a link that redirected to a ZIP file. The ZIP file was hosted on a likely compromised SharePoint account and contained *Domenus VBS*, which downloads *Harpy* from `https[:]//fashionableeder[.]com/info`. At one victim, CARBON SPIDER subsequently deployed the aforementioned custom PS *Sekur* stager and profiled the Active Directory environment using the utility *ADFind*.

In this incident, CARBON SPIDER also used the *KillACK* PS backdoor, executing the malware using both PowerShell and PowerShell ISE. *KillACK* sends host information to a C2 server (in this case, `againcome[.]com` or `besaintegration[.]com`) and executes provided PS script blocks. Multiple *KillACK* modules have been observed by CrowdStrike Intelligence, including modules for conducting self-propagation and AMSI hot-patching, as well as for executing *Cobalt Strike* stagers and enumerating network information.

On Aug. 9, 2020, CARBON SPIDER attempted to run the *Darkside* ransomware with the filename `sleep.exe`. This filename may reflect an attempt to masquerade as the legitimate Windows executable with the same name.

Following this incident, CrowdStrike Intelligence identified numerous similar *Darkside* campaigns featuring distinctive CARBON SPIDER tooling, including *Harpy, Domenus VBS/JS, KillACK* and *Sekur*. The adversary also used the commodity *Cobalt Strike* framework and *Plink* tunneling tool in many of these campaigns. After achieving initial access, the adversary consistently seeks to harvest valid administrative credentials to enable lateral movement and uses a variety of tools and techniques for this purpose, including CrackMapExec, Kerberoasting, Mimikatz, PowerSploit and SessionGopher. In one incident, the adversary likely exploited the ZeroLogon vulnerability (CVE-2020-1472) against a domain controller.

Using valid credentials, CARBON SPIDER moves laterally through victim environments using RDP and occasionally SSH. The adversary typically uses PS to run *Cobalt Strike* but occasionally writes *Cobalt Strike* stagers or *KillACK* backdoors to disk. Occasionally, CARBON SPIDER has deployed the legitimate *GoToAssist* or *TightVNC* tools to provide redundant control of hosts.

Similar to many other ransomware operators, CARBON SPIDER not only encrypted victim files using *Darkside*, but also exfiltrated data for publication on a dedicated leak site (DLS) hosted on Tor. For exfiltration, CARBON SPIDER primarily leveraged the *MEGASync* client for hosting provider MEGA but also employed *GoToAssist*. Further, CARBON SPIDER frequently conducted *hypervisor jackpotting* by encrypting ESXi servers using a version of *Darkside* specifically designed for ESXi.

On Nov. 10, 2020, CARBON SPIDER announced the establishment of the *Darkside* RaaS affiliate program. The announcement, posted on two major Russian-language forums, states that the operators of *Darkside* are looking for Russian-speaking affiliates who understand how to recognize and delete backups. On Nov. 11, 2020, CARBON SPIDER added a new message to their DLS concerning the new affiliate program. This announcement claims “we created the perfect product for ourselves,” indicating that *Darkside* was originally exclusive to one group and not shared.

CrowdStrike Intelligence assesses that *Darkside* ransomware campaigns prior to this announcement were likely conducted by CARBON SPIDER, and that CARBON SPIDER was responsible for creating *Darkside* and introducing the RaaS affiliate program. This assessment carries moderate confidence, based on:

- Multiple separate *Darkside* incidents attributable to CARBON SPIDER
- Low overall volume of *Darkside* campaigns
- The Nov. 11, 2020 announcement described above indicating *Darkside* was initially exclusive to one group

- The Oct. 10, 2020 press release indicating *Darkside* is operated by a single group

Subsequent to the creation of the *Darkside* RaaS program, CrowdStrike Intelligence continued to observe some *Darkside* campaigns almost certainly conducted by CARBON SPIDER — in addition to other campaigns operated by affiliates — featuring divergent tooling and TTPs. CARBON SPIDER's campaigns featured the malware discussed above, in addition to heavy use of the *Cobalt Strike* post-exploitation framework.

Conclusion

CARBON SPIDER's shift from POS malware to BGH ransomware attacks exemplifies a broader trend in the eCrime landscape. Numerous adversaries that previously relied on banking trojans (e.g., INDRIK SPIDER) or POS compromises (e.g., GRACEFUL SPIDER) have almost entirely reinvented themselves to focus on ransomware, reflecting how lucrative BGH campaigns are. Until the economics of cybercrime fundamentally change, it is unlikely these adversaries will alter their behavior.

Indicators of Compromise

Type	Value
Leo VBS	`8279ce0eb52a9f5b5ab02322d1bb7cc9cb5b242b7359c3d4d754687069fcb7b8`
JSS Loader	`98fe1d06e4c67a5a5666dd01d11e7342afc6f1c7b007c2ddbfc13779bcc51317`
Sekur stager	`bbd1c244c0861c0048d5eccecbb6dee1a6f57764c7d0028a7cbfd87c93d3166b`
Domenus VBS	`00fb044af4c92bd06699aaf1d83c4e6805e96f501f84ad1d2ff0885384aa3ea1`
Domenus JS	`5b7115ab612dcff8e84b2258082a6e7c71b5d52237a4ae8a6642baeb36c2aa48`
KillACK	`4f5eefe93ac2fa5f92c6bd245fff1400f6a61aeee07076c92c66d82f94dc45c3`

Table 1. Exemplar SHA256 hashes of CARBON SPIDER malware

Explanation of Confidence Rating

- **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.

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.*