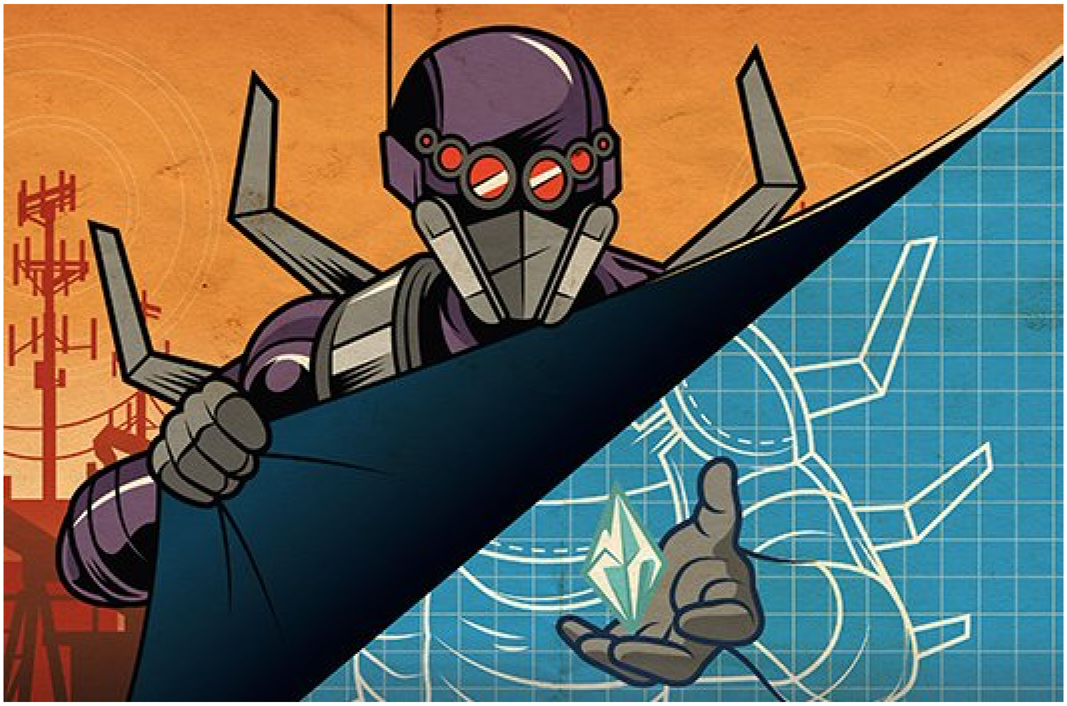
Arrests Put New Focus on CARBON SPIDER Adversary Group

crowdstrike.com/blog/arrests-put-new-focus-on-carbon-spider-adversary-group/

August 1, 2018

August 1, 2018

Paul Moon Research & Threat Intel



In an indictment unsealed by the U.S. Department of Justice (DoJ) on Aug. 1, 2018, three Ukrainian nationals have been charged with conspiracy, wire fraud, computer hacking, access device fraud and aggravated identity theft. Dmytro Fedorov, 44, Fedir Hladyr, 33, and Andrii Kopakov, 30, are suspected to be key members within CARBON SPIDER's point of sale (POS) subgroup.

The arrests took place between January and June 2018, and coincided with a slowdown in CARBON SPIDER activity. The DoJ announcement also details the group's use of a front company, named Combi Security, to recruit developers and intrusion specialists for its operations. Given that other members of this subgroup remain at large, it is likely that the tactics, techniques and procedures (TTPs) may change but activity will continue.

CARBON SPIDER, more widely known as the Carbanak group, is a long-standing criminal enterprise responsible for compromising banks to transfer funds to mule accounts, performing ATM jackpotting attacks, and conducting mass compromise of debit and credit cards from POS terminals in large enterprises. They have been active in some form since at least 2013. During that time, the group has focused on the banking, financial, media, technology, hospitality, and food and beverage verticals, using targeted campaigns to reach their objectives.

Untangling the CARBON SPIDER Web

The structure of CARBON SPIDER is very complex and was initially suspected to be a single group, based on their use of several custom tools and specific TTPs. However, further research into the structure indicates that there are several clusters of activity likely made up of subgroups serving different missions, potentially with access to a shared development environment and pool of resources. A complex structure such as this is difficult to manage and speaks to the sophistication of the actor.

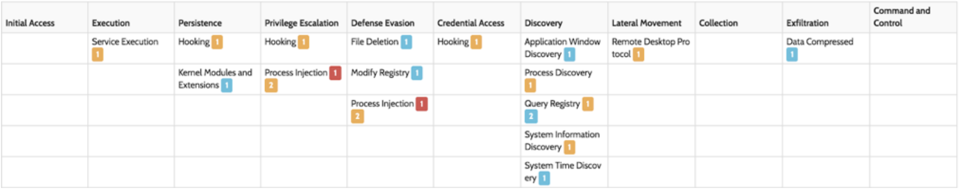
This blog aims to examine CARBON SPIDER over time and attempts to describe their changing relationship within the eCrime ecosystem.

Custom Tools

CARBON SPIDER has leveraged many custom tools since it began activity in 2013, including its primary implant *Sekur* (a.k.a. *Anunak*). These include the following:

Sekur

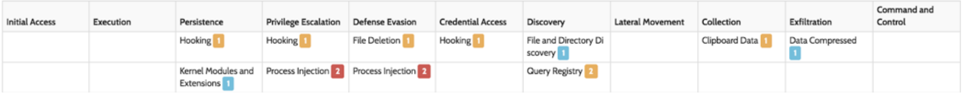
Name	Sekur
Aliases	Anunak and Carbanak RAT
First Seen	February 2014 (based on compile time)
Last Seen	November 2017 (based on compile time)
Purpose	Primary remote access toolkit (RAT) for monitoring victim systems of interest
Type	Microsoft Windows executable
Example Hash	f70cef297efe9ec0abea369b3c1235f14220a6165b48f6e8aa054296078122c8
Falcon EPP protection	Machine learning: Cloud-based, on-sensor indicators of attack(IOAs): Suspicious activity

MITRE ATT&CK™ technique analysis from Hybrid Analysis	

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
	Service Execution 1	Hooking 1	Hooking 1	File Deletion 1	Hooking 1	Application Window Discovery 1	Remote Desktop Pro tocol 1		Data Compressed 1	
		Kernel Modules and Extensions 1	Process Injection 1 2	Modify Registry 1		Process Discovery 1				
				Process Injection 1 2		Query Registry 1 2				
						System Information Discovery 1				
						System Time Discov ery 1				

Sekur has been CARBON SPIDER's primary tool for several years, although usage over the last year appears to have declined. It contains all the functionality you would expect from a RAT, allowing the adversary to execute commands, manage the file system, manage processes, and collect data. In addition, it can record videos of victim sessions, log keystrokes, enable remote desktop, or install Ammyy Admin or VNC modules. From July 2014 on, samples were compiled with the capability to target Epicor POS systems and to collect credit card data.

Agent ORM

Name	Agent ORM
Aliases	Toshliph and DRIFTPIN
First Seen	June 2015 (based on compile time)
Last Seen	May 2016 (based on compile time)
Purpose	First-stage information collection and downloading next-stage payloads
Type	Microsoft Windows executable
Example Hash	36937e5e744873b3646c9d345e8cf50fb969029dc77525acfe63d5a9d28b73f2
Falcon EPP protection	Machine learning: Cloud-based, on-sensor IOAs: Suspicious activity
MITRE ATT&CK™ technique analysis from Hybrid Analysis	

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
		Hooking 1	Hooking 1	File Deletion 1	Hooking 1	File and Directory Di scovery 1		Clipboard Data 1	Data Compressed 1	
		Kernel Modules and Extensions 1	Process Injection 2	Process Injection 2		Query Registry 2				

Agent ORM began circulating alongside Sekur in campaigns throughout the second half of 2015. The malware collects basic system information and is able to take screenshots of victim systems. It is used to download next-stage payloads when systems of interest are identified. It is strongly suspected that Agent ORM has been deprecated in favor of script-based first-stage implants (*VB Flash*, *JS Flash*, and *Bateleur*).

VB Flash

Name	VB Flash
Aliases	HALFBAKED
First Seen	September 2015 (based on observed distribution)
Last Seen	May 2017 (based on observed distribution)
Purpose	First-stage information collection and downloading next-stage payloads
Type	VBScript
Example Hash	a7a927bd44040817ae39e15aeb3f0b69ca943d4ce5b00d12eed6fae5b1c325d0
Falcon EPP protection	IOAs: Attacker methodology; Suspicious activity

VB Flash was first observed being deployed alongside Agent ORM in September 2015. It is likely that this was developed as a replacement to Agent ORM and contained similar capabilities. The first observed instance of VB Flash included comments and was easy to analyze—later versions soon began to integrate multiple layers of obfuscation. Several versions of VB Flash were developed including ones that utilized Google Forms, Google Macros, and Google Spreadsheets together to make a command-and-control (C2) channel. This variant would POST victim data to a specified Google form, then make a request to a Google macro script, receiving an address for a Google Spreadsheet from which to request commands.

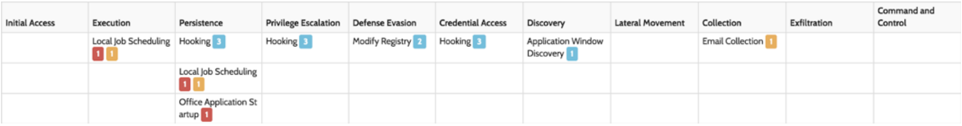
JS Flash

Name	JS Flash
Aliases	JavaScript variant of HALFBAKED
First Seen	May 2017 (based on observed distribution)
Last Seen	November 2017 (based on observed distribution)
Purpose	First-stage information collection and downloading next-stage payloads

Type	JavaScript
Example Hash	ffebcc4d2e851baecd89bf11103e3c9de86f428fdeaf0f8b33d9ea6f5ef56685
Falcon EPP protection	IOAs: Attacker methodology; Suspicious activity

JS Flash capabilities closely resemble those of VB Flash and leverage interesting techniques in deployment via batch scripts embedded as OLE objects in malicious documents. Many iterations of JS Flash were observed being tested before deployment, containing minor changes to obfuscation and more complex additions, such as the ability to download *TinyMet* (a cutdown of the *Metasploit Meterpreter* payload). PowerShell was also used heavily for the execution of commands and arbitrary script execution. No JS Flash samples were observed being deployed after November 2017.

Bateleur

Name	Bateleur
Aliases	N/A
First Seen	June 2017 (based on observed distribution)
Last Seen	April 2018 (based on observed distribution)
Purpose	First-stage information collection and downloading next-stage payloads
Type	JavaScript
Example Hash	da70df51aa80414fcba9bf7322e44e8ea5ed6a3725f342cd05c733376c6f2121
Falcon EPP protection	IOAs: Malicious document; Establishing persistence.
MITRE ATT&CK™ technique analysis from Hybrid Analysis	

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
	Local Job Scheduling 1 1	Hooking 3	Hooking 3	Modify Registry 2	Hooking 3	Application Window Discovery 1		Email Collection 1		
		Local Job Scheduling 1 1								
		Office Application Startup 1								

Bateleur deployments began not long after JS Flash and were also written in JavaScript. Deployments were more infrequent and testing was not observed. It is likely that Bateleur was run in parallel as an alternative tool and eventually replaced JS Flash as CARBON

SPIDER’s first stage tool of choice. Although much simpler in design than JS Flash, all executing out of a single script with more basic obfuscation, Bateleur has a wealth of capabilities—including the ability to download arbitrary scripts and executables, deploy TinyMet, execute commands via PowerShell, deploy a credential stealer, and collect victim system information such as screenshots.

Clusters of Activity

Based on the use of these tools, it is possible to group the CARBON SPIDER activity into several clusters. These clusters may represent different groups with a common tool supply chain, or isolated campaigns from the same group, using separate individuals to carry out attacks with a different focus.

Point of Sale (POS) Targeting

Target Region	Primarily U.S. and Western Europe
Target Sector	Enterprises that process many card transactions (in particular casinos, hotels, and restaurant chains)
Active From	At least mid 2015
Active To	Current

The POS cluster is the most prolific associated to the CARBON SPIDER actor and is also known as FIN7. This cluster has used all the custom tools described with VB Flash, JS Flash, and Bateleur that are unique to them. Over time, they have used targeted spear phishing emails to deploy malicious documents that initially used exploits; more recently, they have used macros and OLE embedded objects. The primary method of cash out for this group is the acquisition and sale of credit and debit card dumps from POS devices. Many of the stolen cards are sold as collectives on the eCrime marketplace, Joker’s Stash.

Targeting of Russian Financial Institutions

Target Region	Russia
Target Sector	Financial and banking
Active From	Late 2013
Active To	Early 2015

This cluster can also be described as the original Carbanak group. It is suspected that they stole large sums of money using several cash out methods against Russian banks, at which point the group may have diverged. It is likely that they developed the primary CARBON SPIDER implant Sekur and were, at the point of being operational, probably the only users of it.

Targeting of Middle Eastern Financial Institutions

Target Region	Middle East and South Asia
Target Sector	Financial and banking
Active From	October 2014
Active To	Activity reported up to at least early 2016

Although the targeting profile is the same as the Russian banking cluster, the TTPs are very different. In particular, the use of tooling stands out from other clusters of CARBON SPIDER activity. As with other clusters, the primary infection vector is targeted spear phishing emails that use exploits for a variety of vulnerabilities in Microsoft Office:

- CVE-2015-2545
- CVE-2014-4114
- CVE-2015-1770
- CVE-2015-1641

A custom `.NET` first stage payload is deployed that in some cases deploys Agent ORM or Sekur, but is also used to deploy *NetWire*. Instances of *DarkComet* and *Morphine RAT* use some custom `.NET` downloader servers as their C2. One possibility is that CARBON SPIDER outsourced deployment of their malware for this campaign. An alternative theory is that this is a seperate group also using CARBON SPIDER tools. Little is reported publicly about the successfulness of this cluster of activity, and no cash out methods are known.

Targeting of Eastern European Financial Institutions

Target Region	Ukraine and Eastern Europe
Target Sector	Likely financial and banking
Active From	Mid-2015
Active To	Last known activity in late 2015

The Eastern European banking cluster is based on a single campaign using a strategic web compromise of an Italian bank in Ukraine to deploy instances of Agent ORM to likely Ukrainian targets. It is likely that this cluster links to one of the other clusters of Sekur activity, possibly the unattributed activity discussed below. However, no follow-on actions have been observed past Agent ORM deployment.

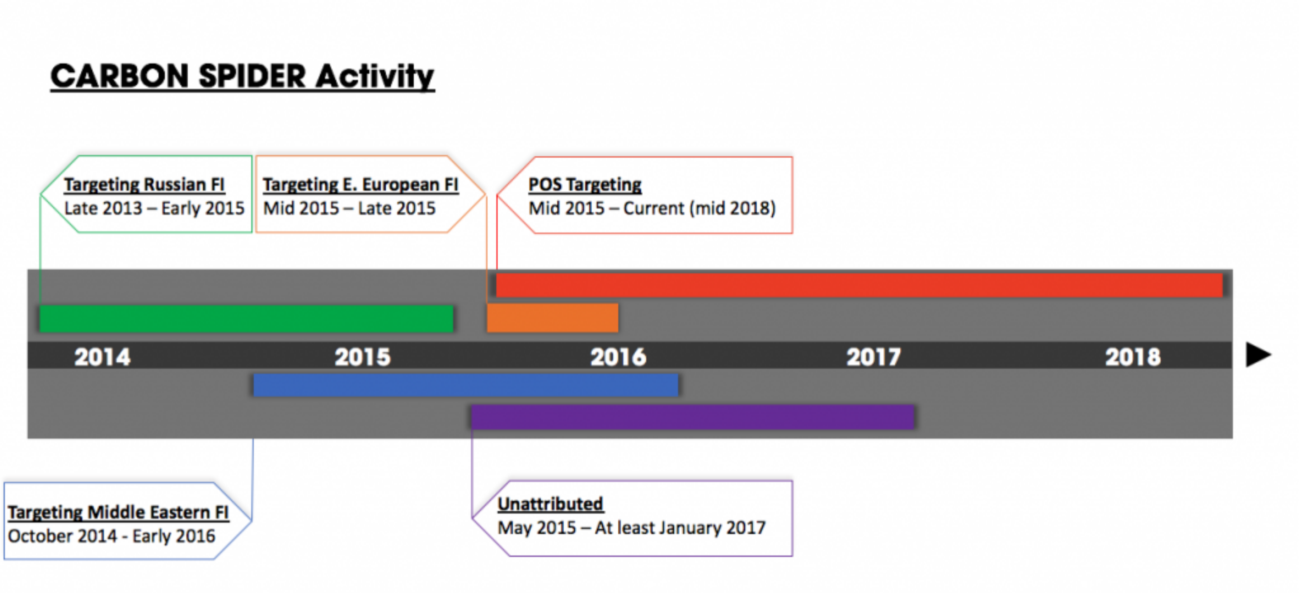
Unattributed

Target Region	Where known (appears to be Ukraine)
Target Sector	Not known in most cases (one case focused on news and media organizations)
Active From	May 2015
Active To	At least January 2017

The unattributed activity is based on a cluster of Sekur activity that runs in parallel with the POS cluster of activity, but does not exhibit the same TTPs (with differences in Sekur configuration, campaigns, and infrastructure selection). Many of these samples were submitted from Ukraine; additionally, one of them was deployed using a malicious document with a decoy that suggests Ukrainian news and media targeting. It is possible that this activity relates to the Eastern European bank cluster of Agent ORM activity; yet without further evidence of follow-on activity, it is not possible to determine this cluster's action on objectives.

Timeline

Below is a timeline showing the activity of each of the five clusters of CARBON SPIDER activity:



The timeline shows that several of these clusters of activity started just after public reporting of the group (around mid-2015) and that the divergence in activity may have been the result of this exposure. It also highlights that CARBON SPIDER now likely operates multiple parallel missions focusing on different regions and sectors.

Links to Other Targeted eCrime Groups

Beyond the described clusters of CARBON SPIDER activity based around their custom tools, their are also interesting links to other tracked, targeted eCrime activity. This includes the group dubbed RATPAK SPIDER (also known as Buhtrap) that targets Russian and Ukrainian financial institutions, a group dubbed Odinaff targeting SWIFT systems particularly in Eastern Europe, and the group COBALT SPIDER (also known as Cobalt) that, again, specializes in targeting Russian banks.

RATPAK SPIDER

Operation Buhtrap had a similar target scope (Russian financial) to the first cluster of CARBON SPIDER activity. Although these have always been tracked as seperate groups, there is a technical link between payload deployments. A custom macro dropper that would encode the payload using VB Script notation, and contained the strings “After OnTime” and “FUCK AV,” was observed in only 19 unique samples across Crowdstrike sample stores. One of the payloads was an instance of Agent ORM used to targeted casinos; a second payload also used by CARBON SPIDER was an instance of Sekur. The other six unique payloads observed being deployed using this custom macro dropper were instances of the Nullsoft Scriptable Install System (NSIS) downloader attributed to the Buhtrap group. Initially, this led to tracking both threats as CARBON SPIDER. Although it now appears that Buhtrap is likely a separate entity, the use of this shared deployment mechanism — unique to these two groups — suggests a common supply chain or developer and a closer working relationship, especially given some similarities in target scope.

Odinaff

A SWIFT compromise was observed in mid-2016, targeting a Ukrainian bank that at the time was unattributed. Based on similar TTPs, it was hypothesised that this could be CARBON SPIDER activity; however, although common off-the-shelf tools (such as Meterpreter and Cobalt Strike) were used, the custom CARBON SPIDER arsenal was not present. Later, this group was reported in open source as Odinaff. In addition to similar TTPs, there appeared to be some infrastructure overlap with two IP addresses. One Odinaff C2 was also reported to be in previous use as a Sekur plugin server. A second IP was also reported to be used by CARBON SPIDER in a previous campaign. Again, this may just be a shared hosting provider, but the TTP similarity makes this infrastructure overlap more noteworthy.

COBALT SPIDER

The Cobalt group, tracked by CrowdStrike intelligence as COBALT SPIDER, bears many similarities in the targeting of banks to the Russian cluster of CARBON SPIDER activity. Both groups also use Cobalt Strike and several other pen-testing tools in their operations; nevertheless, the two groups appear to be distinct outside of this.

On March 26, 2018, an announcement was made that a Russian citizen identified by authorities as “Denis K.” was arrested by the Spanish national police in Alicante, Spain. He was reportedly involved in early CARBON SPIDER targeting of Russian banks and is suspected of being one of the members of COBALT SPIDER. Although reports suggest that he may have been a leader of COBALT SPIDER, activity has continued from this group, suggesting his role was not a key one within this organization. This suggests a link between the two groups between 2013 and likely, 2015. This is around the time that the dominant focus for CARBON SPIDER became targeting the POS systems of Western enterprises. It is possible that at least one individual left CARBON SPIDER and either joined forces with or created COBALT SPIDER.

Summary

CARBON SPIDER is the pioneer of targeted eCrime activity with some of the largest publicly attributed success. Their level of sophistication across the clusters of activity makes them a key player in the eCrime ecosystem. Although there is not enough evidence to directly link CARBON SPIDER to other targeted criminal groups, it is assessed with high confidence (based on analysis of artifacts and infrastructure over time) that CARBON SPIDER shares resources with other notable criminal groups.

There are two possible hypotheses as to how the clusters of CARBON SPIDER activity are linked. One theory is that they were originally one group that splintered into several with different focuses. Several of the splinter groups may have maintained access to their custom tools (e.g., Sekur), while others moved on to work with other actors (e.g., COBALT SPIDER). A second theory is that CARBON SPIDER operates as distinct groups with different focuses, but they report to a single management structure. Resources may be shared between the groups, but each has its own members. At this stage, the first theory appears to be the most likely.

Based on recently observed tooling and operations, CARBON SPIDER appears to be focusing their efforts on the POS cluster of activity against the hospitality and restaurant sector, with no recently reported activity against banks. They also appear to be moving away from their custom tooling, with no Sekur samples compiled since November 2017 and fewer samples appearing in live operations.

Going forward, it is likely that CARBON SPIDER will continue operations to target sectors that give the best financial return for their efforts. For the short term, this will likely mean a continued focus on POS systems and large enterprises that process them. It is possible that they may return to target banks, but this would likely be on a small scale with very focused operations. CARBON SPIDER will likely move completely away from their old custom toolset, either developing new tools or using commodity off-the-shelf packages to achieve their objectives. This is even more assured given the arrests of three members of the most prolific CARBON SPIDER subgroup.

As CARBON SPIDER adversary groups retool and alter their TTPs CrowdStrike will continue to track this adversary leveraging FalconX capabilities to combine endpoint protection, automation and malware analysis to prevent CARBON SPIDER from breaching our customer networks.

To learn more about how to incorporate intelligence on threat actors like CARBON SPIDER into your security strategy, please visit the Falcon Intelligence product page.

Download the CrowdStrike 2020 Global Threat Report

Related Content

Who is EMBER BEAR?

A Tale of Two Cookies: How to Pwn2Own the Cisco RV340 Router

PROPHET SPIDER Exploits Citrix ShareFile Remote Code Execution Vulnerability CVE-2021-22941 to Deliver Webshell