Zebrocy’s Multilanguage Malware Salad

By GReAT

Published: 2019-06-03 · Archived: 2026-04-05 21:57:12 UTC

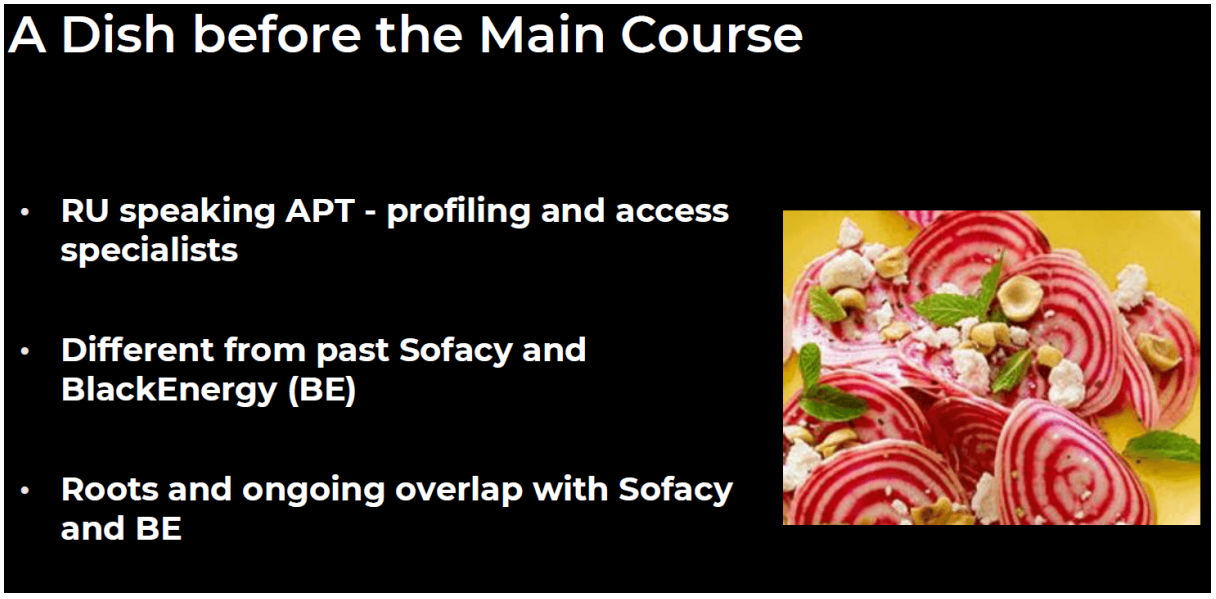
03 Jun 2019

6 minute read

- Expert GReAT

Zebrocy is Russian speaking APT that presents a strange set of stripes. To keep things simple, there are three things to know about Zebrocy

- Zebrocy is an active sub-group of victim profiling and access specialists
- Zebrocy maintains a lineage back through 2013, sharing malware artefacts and similarities with BlackEnergy
- The past five years of Zebrocy infrastructure, malware set, and targeting have similarities and overlaps with both the Sofacy and



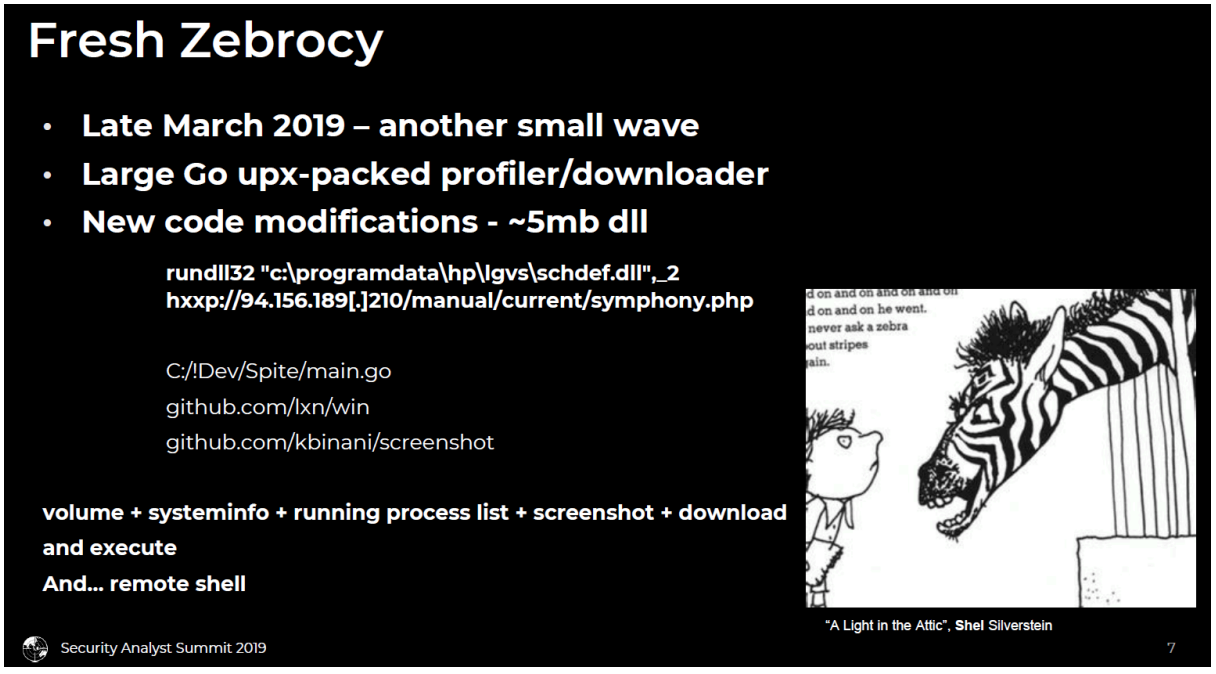
Zebrocy shares data points and crosses lines with other clusters of activity in unique and unexpected ways. Zebrocy initially shared limited infrastructure, targets, and interests with Sofacy. Zebrocy also shared malware code with past BlackEnergy/Sandworm; and targeting, and later very limited infrastructure with more recent BlackEnergy/GreyEnergy. Oddly, Turla deployed spearphish macros almost identical to previous, non-public Zebrocy code in 2018.

It’s fantastic to see some of these same points being repeated publicly by other research teams. A previous claim that Zebrocy distributed Sofacy’s XAgent as a second stage implant remains unsubstantiated but now is replaced with findings identical to these following the SAS2019 presentation, so it seems we are all slowly getting on the same page.

A first course with new additions

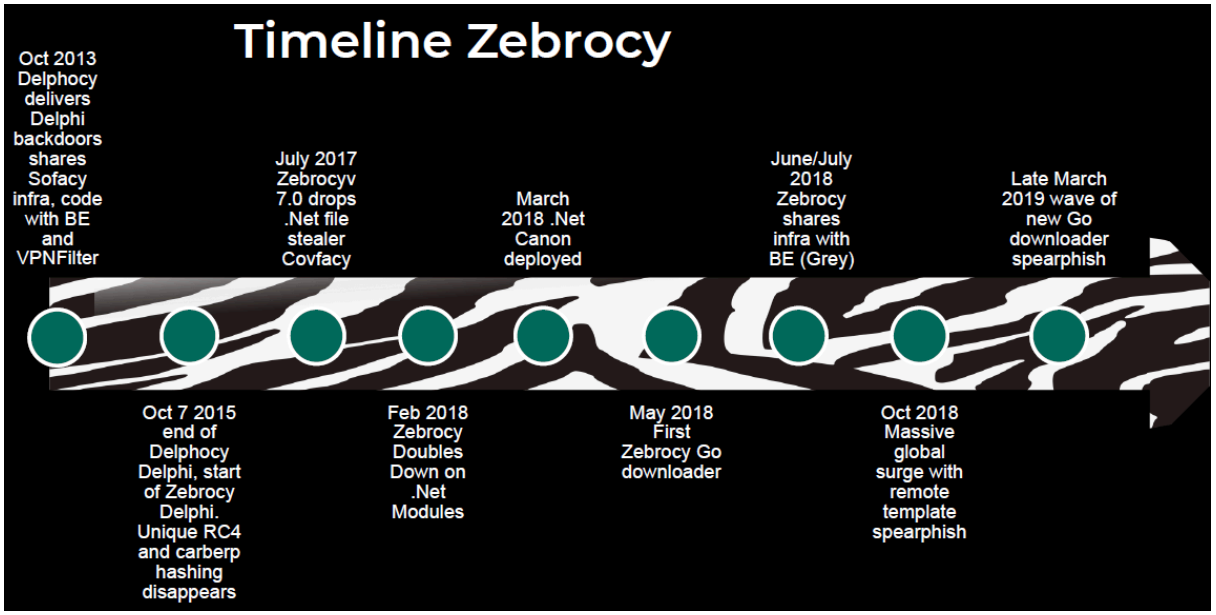
When we originally documented a Zebrocy malware incident in late 2015, we noted an Oct 2015 AutoIT downloader and a Delphi backdoor payload. Since then, we have noted a virtual salad of Zebrocy code tossed together, built with a handful of languages, often ripped from various code sharing sites. Zebrocy activity initiates with spearphishing operations delivering various target profilers and downloaders without the use of any 0day exploits. Browser credential theft, keylogging, and Windows credential theft, along with some incidents of file and communications theft, are all on the list of Zebrocy second stage implant specials.

This Zebrocy dish is served before the main course – gaining and maintaining access is not an easy job. And, because the group seems to maintain lineage in both the 0day capable and destructive BlackEnergy/Sandworm APT and the prolific and 0day capable Sofacy APT, this course is very interesting. Let’s take a more intelligent perspective on the Zebrocy malware set and activity and its lineage, based on reporting provided to our



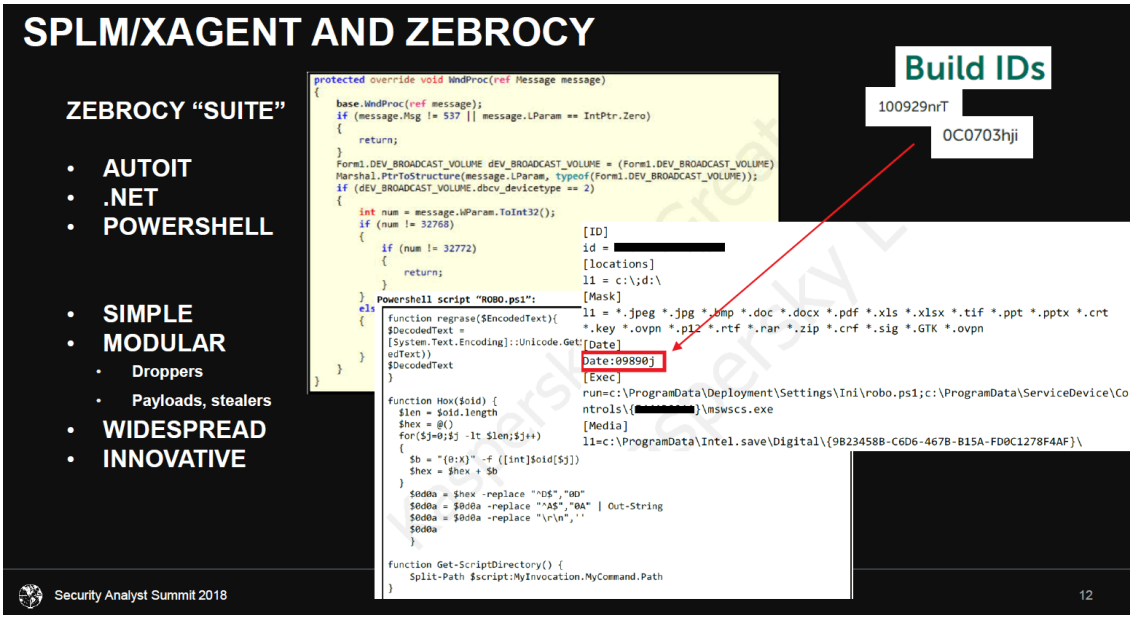
Since the SAS2019 presentation, we have identified a new Zebrocy backdoor family, deployed with a new downloader. So Zebrocy continues to expand its malware set. There appears to be both a return to C coding

for the group, and also an expansion with the

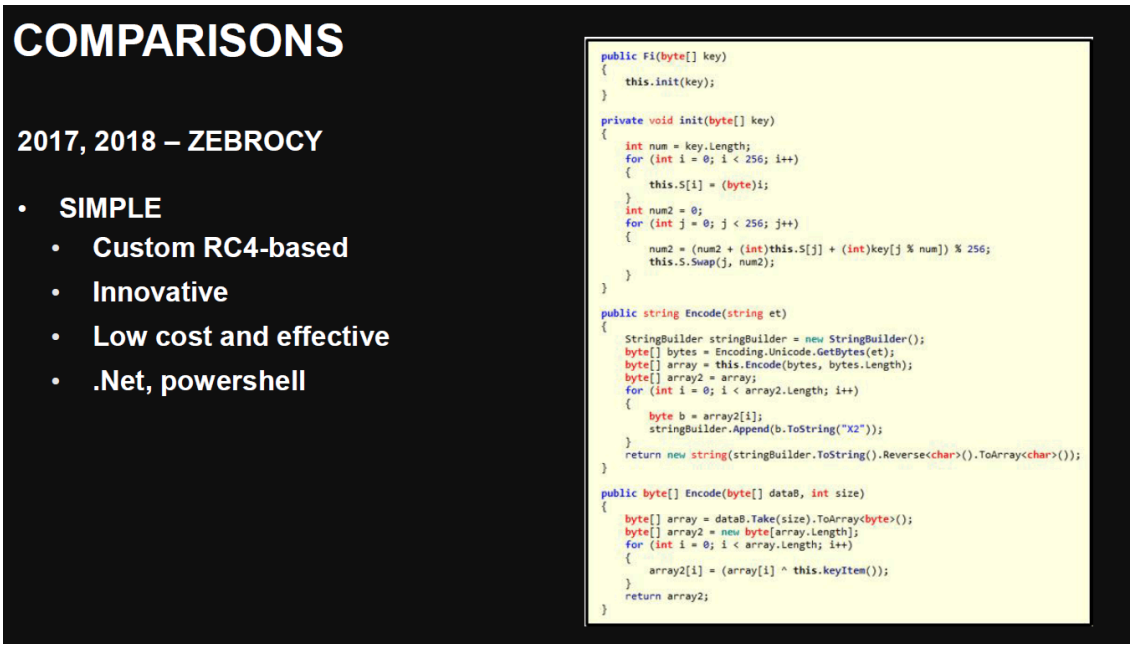


A set of Zebrocy related events best characterize years of the activity and help to carve out the group's own profile, its lineage, malware set, infrastructure, and modus operandi.

- Zebrocy lineage – early Sofacy infrastructure overlap (late 2015/early 2016) for the Zebrocy Delphi backdoor
- Zebrocy lineage – Delphocy Delphi deployment and abrupt conclusion (2013 – late 2015), and start of Zebrocy Delphi timeline (late 2015)
- Zebrocy lineage – shared, unique kernel code between BlackEnergy and Delphocy bootkit (2013 – 2015)
- Zebrocy unique malware set – vintage Delphi programming coupled with unusual and agile development capabilities with new managed languages like Python, C#, and Go all perform screengrab anchor, volume serial number id, systeminfo and process list collection
- Zebrocy ongoing targeting and infrastructure overlap – fairly recent



- The full 2018 decline of SPLM/XAgent for the more traditional “Sofacy” activity
- A coincidental new increase in Zebrocy activity
- Shared build-id format with BlackEnergy modules
- An expansion in Zebrocy spearphishing
- An expansion in the managed languages the Zebrocy malware set is built on



These predictions later turned into global events, as lighter targeting turned into a massive global surge of Zebrocy activity, sometimes sharing targets between both Sofacy and Zebrocy. Also later that year, the Zebrocy malware set expanded with C#, Python, and Go. This wouldn’t be the first or last time we reported on this group’s innovative malware set.

The limited set of 2013-2015 Delphocy intrusions in Ukraine and Poland deployed a Delphi backdoor both with and without a bootkit loader. This bootkit loader included a routine that shares the same compiled code with only the BlackEnergy kernel loaders, helping to tie Zebrocy malware to the BlackEnergy malware set.

This unique encryption implementation was shared between BlackEnergy’s kernel loader, and Delphocy’s bootkit kernel loader code. The appearance of this code overlap coincides with several project events:

- End of Delphocy/BlackEnergy overlapped code use, while BlackEnergy moved forward with other code
- End of Delphocy’s user-mode Delphi payload (October 2015)
- Start of Zebrocy’s Delphi payload (October 2015)

A particular chunk of kernel mode code for a custom encryption routine was shared across the older Delphocy bookit and the BlackEnergy malware platform in 2013. While Delphocy replaced this bootkit with a simplified user-mode persistence technique, BlackEnergy malware continued using this code until late 2015. Then, these APTs discontinued both the Delphi-based Delphocy project

and the use of this mysterious chunk of code within BlackEnergy malware. Almost immediately, Delphi-based Zebrocy backdoors began to be deployed. Several months later, a Zebrocy backdoor connected back to a domain that was registered by a particular email address. This address had been used to register another Sofacy domain hosted on a well-known Sofacy IP at the time (rammatica[.]com/raveston[.]com).

```
bVar1 = *(byte *)(param_1 + 0x100);
cVar2 = *(char *)((ulonglong)bVar1 + param_1);
bVar4 = *(char *)(param_1 + 0x101) + cVar2;
cVar3 = *(char *)((ulonglong)bVar4 + param_1);
*(char *)((ulonglong)bVar1 + param_1) = cVar3;
*(char *)((ulonglong)bVar4 + param_1) = cVar2;
*param_2 = *param_2 ^ *(byte *)((ulonglong)(byte)(cVar2 + cVar3) + param_1);
*(char *)(param_1 + 0x100) = bVar1 + 1;
*(byte *)(param_1 + 0x101) = bVar4;
return;
```

Note that both Delphocy's and BlackEnergy's kernel mode code appropriated unique content in 2013 from the Carberp codebase – hashing, injection, bootkit functionality. Surprisingly, this same unique encryption cipher was seen pasted again into 2018 VPNFilter code as well. Clearly it happens with other malware, but Zebrocy's consistent copy/paste tendency is something not frequently seen in other APT malware with a "best use" date spanning five years or more. Portions of its AutoIT code were copied from code sharing forums and pasted into their own code. This is different from Sofacy's disappeared and exhaustive SPLM/XAgent codebase. It was used for at least six years and was entirely custom-built.

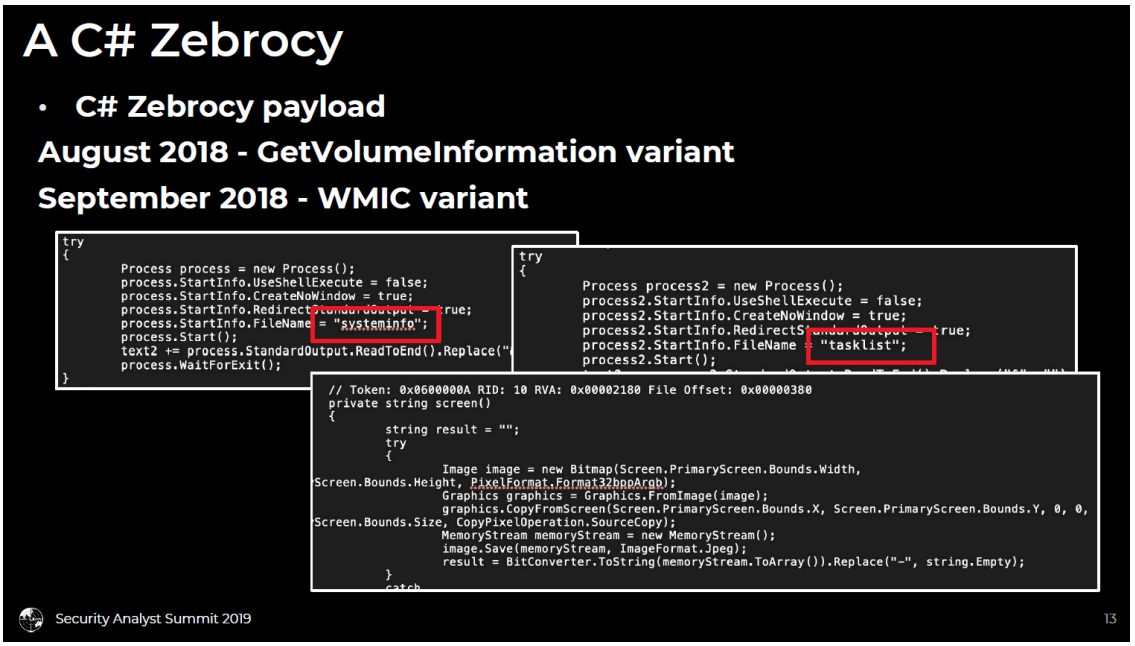
Zebrocy's mix

The Zebrocy malware set is tossed together from a wide set of languages and technologies, including both legitimate and malicious code shared on online forums and sites like Github and Pastebin. This repeated "copy/paste" practice is not frequently seen in Russian speaking APT malware sets, although

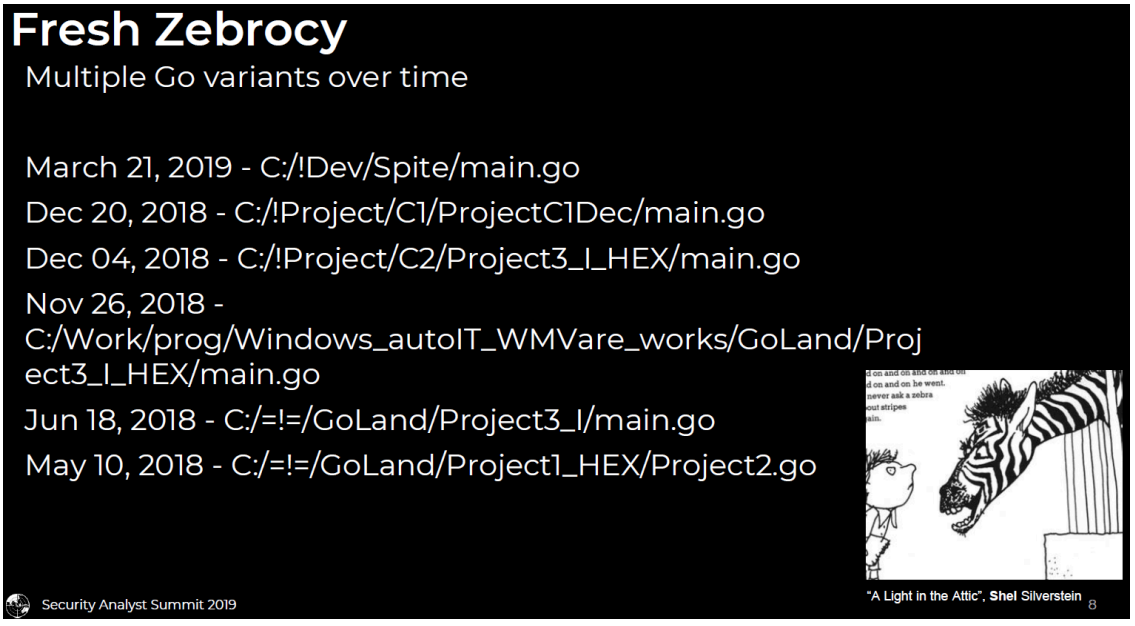
FUNC Name	Detail
SCREENCAPTURE	user32.getdesktopwindow -> capture screenshot
SCREENCAPTURE_SAVETOJPG	save screenshot to C:\Users\xxx\AppData\Roaming\Desktop.jpg
FILESEARCH	recursive and selective extension based file search
SCREEN_SI	generates base64 encoded string of screengrab desktop.jpg, systeminfo output, processlist output for POST
SI (SystemInfo)	cmd /c SYSTEMINFO & PROCESSLIST
CMD	cmd /c <anything>
POST	set up persistence with registry run key write, fetch volume serial number, build URL with serial number and SCREEN_SI output, POST to hardcoded server using winhttp.winhttprequest.5.1
UPLOAD	open file, read contents, POST binary string of file contents to hardcoded c2 as form data

C# Zebrocy backdoor

Zebrocy pushed a C# backdoor that maintains much the same functionality as its other assortment of backdoor implementations.



Most interesting in this implementation is its consistent collection of screengrab and system information, and a list of running processes. Again, with this first stage backdoor, it is profiling its targets and looking for unexpected sources of credential collection to develop bespoke second stage credential harvesters against. Additionally, Zebrocy wheeled out a

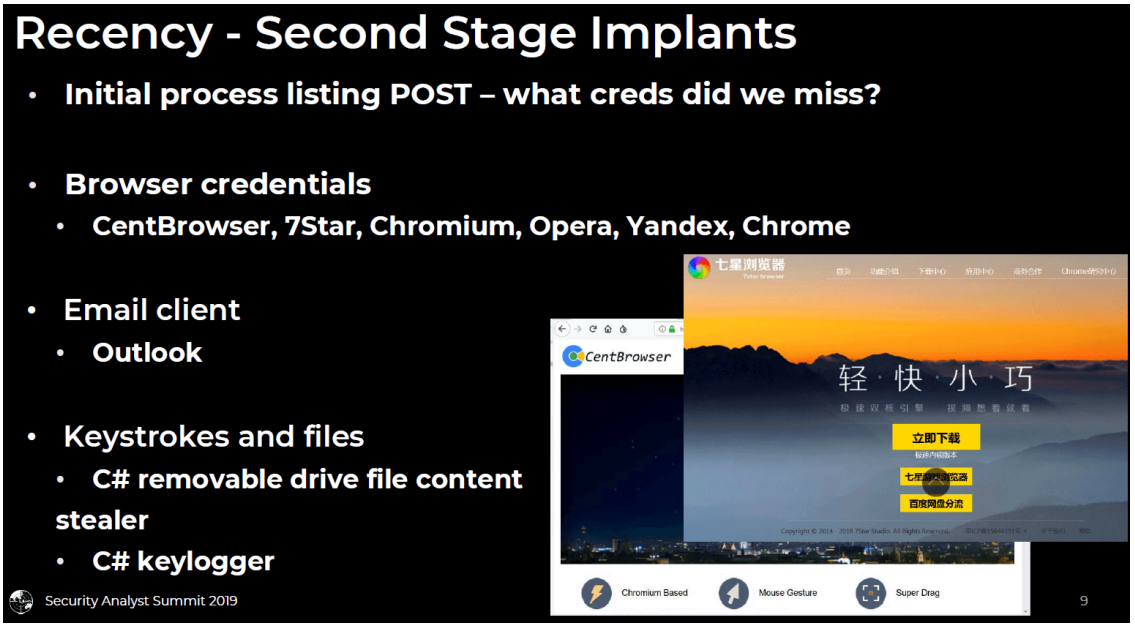


A second stage

These findings were particularly interesting in the light of past claims about SPLM/XAgent being the second stage of choice for Zebrocy, for which there was a lot of monitoring on our part, but

never any data support. Some guesses were made about why that was, perhaps Zebrocy downloaders were all mitigated prior to attempting to download further stages? But never any answers.

Instead, we arrived at the answers ourselves. In order to account for unexpected software installations at victim systems, no matter which language, each first stage backdoor implementation collects a “system information” listing, screengrab, and enumerates running processes. This malware behavior was included in Zebrocy backdoors from the very first backdoor that we reported on, and continued into 2019 with the latest rounds of Go backdoors. After collected information is POSTed to the C2, a long delay ensues. Eventually, target systems may receive a custom built second stage implant to retrieve credentials from those unexpected software sources. More unusual software packages included little-known customized Chromium builds like CentBrowser and 7Star from Asian studios. In some cases, malware password stealers are deployed to address more common software.



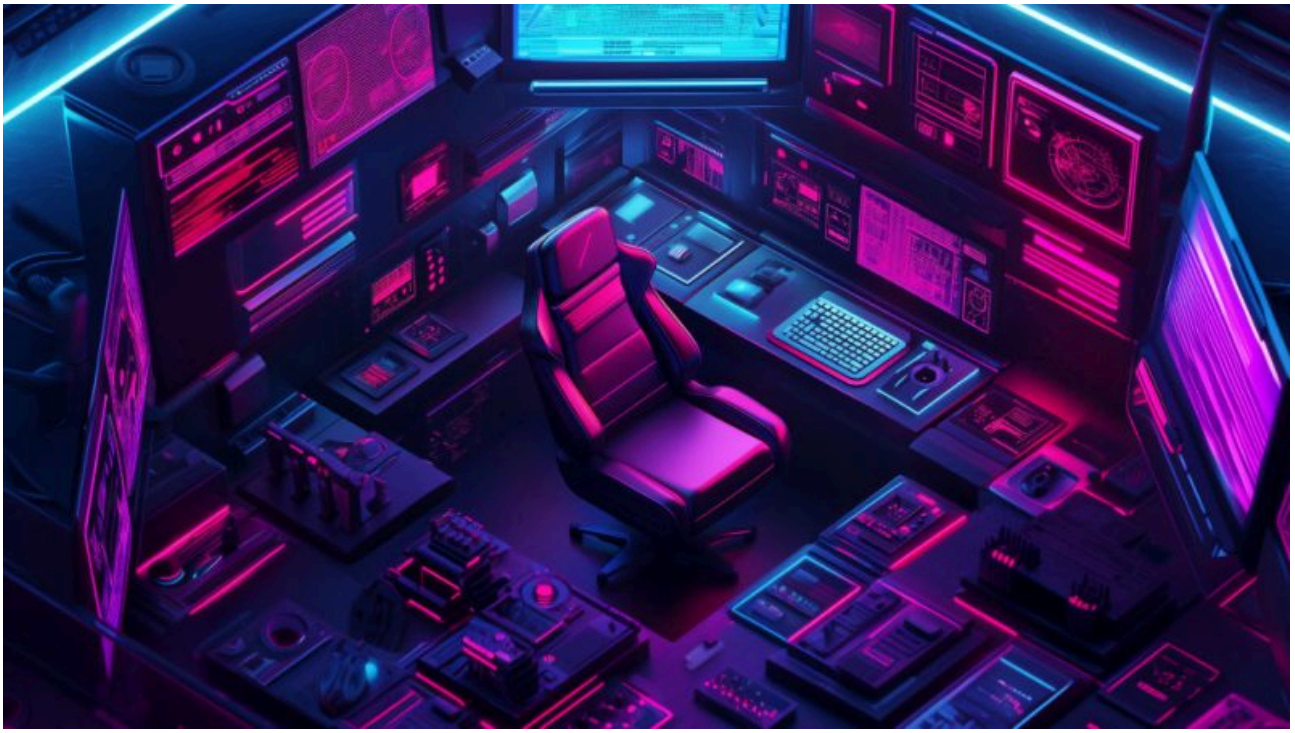
In addition, Zebrocy file content stealers and keyloggers coded in C# were detected at targets in 2017 and 2018. Some of this code and their build id value format was reviewed in the SAS2018 “Masha and these Bears” presentation.

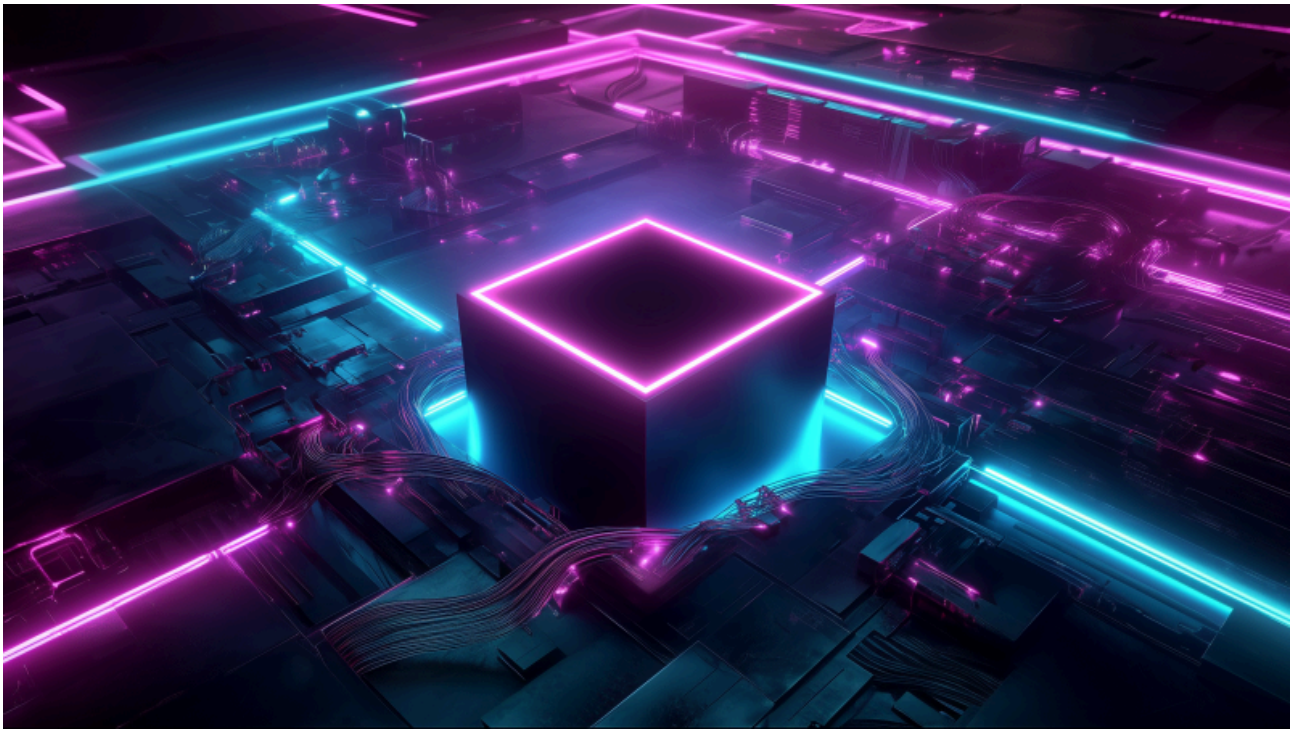
Served cold

Zebrocy version 2.2 called back to a domain sharing Whois and hosting resources with Sofacy in early 2016, and later versions used naming and URL constructs very similar to BlackEnergy resources. And since then, just like BlackEnergy, mostly all of the Zebrocy C2 used no domain registrations. Communications directly to the host over IPv4 with no domain resolution are common behavior for the group’s malware. However, every now and then, Zebrocy malware calls back to servers located by hardcoded domain names.

Its ongoing activity demonstrates a long game commitment to gaining access to targeted networks. And as we predicted at SAS2018 and SAS2019, this latest new Nim coding adds to the growing list of languages for this malware set. We will see more from Zebrocy into 2019 on government and military related organizations.

Latest Webinars





Reports

Kaspersky researchers analyze updated CoolClient backdoor and new tools and scripts used in HoneyMyte (aka Mustang Panda or Bronze President) APT campaigns, including three variants of a browser data stealer.

Kaspersky discloses a 2025 HoneyMyte (aka Mustang Panda or Bronze President) APT campaign, which uses a kernel-mode rootkit to deliver and protect a ToneShell backdoor.

Kaspersky GReAT experts analyze the Evasive Panda APT's infection chain, including shellcode encrypted with DPAPI and RC5, as well as the MgBot implant.

Kaspersky expert describes new malicious tools employed by the Cloud Atlas APT, including implants of their signature backdoors VBShower, VBCloud, PowerShower, and CloudAtlas.
