FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

16 Sept 2020

Alert Number

AC-000133-TT

The following information is being provided by the FBI in collaboration with the Cybersecurity and Infrastructure Security Agency (CISA), with no guarantees or warranties, for potential use at the sole discretion of recipients in order to protect against cyber threats. This data is provided to help cyber security professionals and system administrators guard against the persistent malicious actions of cyber actors.

This FLASH has been released **TLP:WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction.

Indictment of China-Based Cyber Actors Associated with APT 41 for Intrusion Activities

Summary

The US Department of Justice (DOJ) indicted five cyber actors based in the People's Republic of China (PRC) for computer intrusions affecting more than 100 victim companies and organizations in the United States and abroad, as well as multiple foreign governments. The actors, Zhang Haoran and Tan Dailin, collaborated with Chengdu 404 Network Technology company employees Qian Chuan, Fu Qiang, and Jiang Lizhi to conduct computer network exploitation (CNE) operations originating from China.

These China-based cyber actors targeted victims in the following industries:

- education;
- computer hardware;
- software, including video gaming ;
- government ;
- healthcare;
- hospitality;
- social networking;
- non-governmental organizations;
- telecommunications.

FBI FLASH

FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Threat

This sophisticated hacking group located in Chengdu, Sichuan Province, PRC, has been active since at least 2011. The group conducted numerous computer intrusions as well as criminal for-profit computer fraud on a global scale. The group used sophisticated tradecraft against a variety of targets, such as compromising legitimate software for supply chain intrusions, using custom malware, deploying ransomware, and engaging in crypto-jacking attacks. Observed tactics, techniques, and procedures (TTPs) associated with the group can be mapped to the MITRE[1] Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK[2]) for Enterprise framework, Version 7.0.

Technical Details

Capabilities:

The group uses a wide range of tactics in order to gain *Initial Access* [TA0001]. Spearphishing emails with malicious files [T1566.001] is a common tactic for the actors. Spearphishing themes frequently target HR departments with malicious archive files masqueraded [T1036.002] as applicant resumes. The group historically used Microsoft Compiled HTML Help (CHM) [T1218.001] files within their spearphishing messages. In addition, the group conducted supply chain compromises resulting in the victimization of third-party customers throughout the world [T1195.002].

These actors typically obtain means of identification, such as login credentials belonging to individuals with administrative access to victim computer networks, to expand their unauthorized access. Additionally, the actors may deploy legitimate third-party VPN software such as SoftEther on victim networks to facilitate follow-on access to the victim network. The group has also deployed “Skeleton Key” malware to create a master password that will work for any account in the domain.

During early 2020, the group conducted a massive campaign to rapidly exploit publicly identified security vulnerabilities. This technique allowed the group to gain access into victim accounts using publicly available exploit code against VPN services [T1133] or public facing applications [T1190] – without using their own distinctive or identifying malware – so long as the group acted before victim companies updated their systems. This campaign targeted organizations that did not yet patch against security vulnerabilities such as CVE-2019-19781, CVE-2019-11510, CVE-2019-16920, CVE-2019-16278, CVE-2019-1652/CVE-2019-1653, and CVE-2020-10189. These compromises typically resulted in the installation of widely available remote access tools like Cobalt Strike. In all cases in this campaign, the exploit code used by the group was typically several months old.

[1] MITRE is a registered trademark of The Mitre Corporation. Information about Mitre can be found at https://mitre[.]org.

[2] ATT&CK is a registered trademark of The Mitre Corporation. Information about ATT&CK can be found at https://attack.mitre[.]org.

The group has used the following malware: gh0st, 9002, Zxshell, HK Door, XSLCMD, PlugX/Sogu, Derusbi, HiKit, Crosswalk/ProxIP, Winnti/Pasteboy/Stone/Treadstone, Azazel, PoisonPlug/Barlaiy/ShadowPad, metasploit-meterpreter, and Cobalt Strike. The group also uses numerous webshells including China Chopper.

One common persistence technique the group has used is DLL side-loading [T1574.002]. The group frequently implanted malware in “%WINDIR%\Windows\System32\wbem\loadperf.dll” to side-jack of the proper "loadperf.dll" file located in the "%WINDIR%\Windows\System32\" directory. This abuse of the loadperf DLL used the “WMI Performance Adapter Service” (wmiAPSrv). A similar technique is used with the “winmm.dll” file when it is not in “%WINDIR%\System32\winmm.dll”. This technique has been used to launch HK Door, Crosswalk, and other malware.

Infrastructure:

The cyber actors typically conducted their intrusions by accessing compromised servers called hop points from numerous China-based IP addresses resolving to different Chinese internet service providers (ISPs). These cyber actors used US-based and foreign-based email, social media, and other online accounts to develop online personas in order to interact with the group, other conspirators, ISPs, web hosting providers, and victim companies.

The actors obtained the use of servers, typically by leasing remote access to them, directly or indirectly from hosting providers. They used these servers to register and access operational email accounts, host command and control (C2) domains, and interact with victim networks. The actors used these hop points as an obfuscation technique when interacting with victim networks.

The actors registered and used malicious domains that mimic prominent companies in order to deceive targeted victims, cybersecurity professionals, and cybersecurity systems into identifying Internet traffic associated with those domains as legitimate or benign. These socially engineered domain were usually used as C2 domains.

These actors also created “C2 dead drops” (C2DD) [T1102.001], whereby they programmed their malware to contact these C2DD accounts on publicly available web pages. The C2DD pages were encoded with the IP addresses of C2 servers. Specifically, C2DD pages included what might appear to be random strings of text, with the relevant malware programmed to recognize the text strings—which typically started and/or ended with a pre-programmed “anchor text”—converting them into actor-controlled IP addresses or C2 domains. For example, PlugX/Sogu/Fast malware used by the group used encoded text sandwiched between “DZKS” and “DZJS”. The malware would then cause the victim computers to communicate with the servers hosting those IP addresses or C2 domains.

Indicators of Compromise:

Active Hop Point Servers:	
45.32.68[.]14 (started on/about 04/09/2020)	216.24.180[.]216 (used on 12/4/2019)
45.77.28[.]164 (started on/about 05/11/2020)	67.230.163[.]214 (used on 08/15/2020)
45.32.93[.]169 (started on/about 06/01/2020)	216.24.182[.]48 (used on 05/13/2020)
207.246.16[.]107 (started on/about 06/01/2020)	64.64.236[.]27 (used on 01/20/2020)
104.243.19[.]49 (used until 9/9/2020)	104.243.23[.]73 (used until 9/9/2020)
104.36.69[.]105 (used until 9/9/2020)	107.182.18[.]149 (used until 9/9/2020)
107.182.24[.]70 (used until 9/9/2020)	107.182.26[.]43 (used until 9/9/2020)
172.96.204[.]252 (used until 9/9/2020)	173.242.122[.]198 (used until 9/9/2020)
176.122.162[.]149 (used until 9/9/2020)	176.122.163[.]125 (used until 9/9/2020)
176.122.188[.]254 (used until 9/9/2020)	149.154.157[.]48 (used on 08/20/2020)
216.24.179[.]23 (used until 9/9/2020)	64.64.251[.]135 (used until 9/9/2020)
65.49.192[.]74 (used until 9/9/2020)	74.120.175[.]144 (used until 9/9/2020)
74.82.201[.]8 (used until 9/9/2020)	80.251.220[.]225 (used until 9/9/2020)
80.251.222[.]7 (used until 9/9/2020)	80.251.222[.]80 (used until 9/9/2020)
140.82.23[.]214 (started on/about 06/01/2020)	173.242.117[.]47 (used on 01/21/2020)
149.248.16[.]107 (started on/about 06/01/2020)	192.69.89[.]157 (used on 08/05/2020)
149.28.88[.]49 (started on/about 06/01/2020)	64.64.234[.]24 (used on 05/04/2020)
45.86.163[.]136 (used on 08/20/2020)	104.194.85[.]41 (used on 03/27/2020)
51.68.28[.]242 (used on 08/20/2020)	104.225.159[.]134 (used on 12/07/2018)
207.246.108[.]247 (used on 08/20/2020)	104.224.185[.]36 (used on 09/02/2020)
138.68.78.69 (started on 09/03/2020)	

Historic Hop Point Servers	
149.28.75[.]81 (ended on 3/26/2020)	45.76.6[.]149 (started on/about 05/14/2020 - ended on 6/01/2020)
66.42.96[.]115 (ended on 04/08/2020)	8.9.11[.]130 (started on/about 05/14/2020 - ended on 06/01/2020)
66.42.98[.]220 (ended on 04/09/2020)	149.248.8[.]134 (started on/about 03/01/2020 - ended on 08/06/2020)
149.28.69[.]116 (ended on 04/21/2020)	67.229.97[.]224/29 (October 2017 – October 2019)
45.76.174[.]221 (ended on 04/21/2020)	67.198.161[.]240/28 (July 2012 – October 2017)
140.82.23[.]214 (ended on 04/21/2020)	174.139.62[.]56/29 (July 2012 – October 2017)
149.28.75[.]141 (ended on 05/07/2020)	174.139.203[.]0/27 (June 2016)
66.42.96[.]115 (ended on 05/14/2020)	

Command and Control Domains

ad.lflink[.]com	id.serveuser[.]com	sexyjapan.ddns[.]info
biller.zzux[.]com	image.x24hr[.]com	splash.dns04[.]com
bschery.zzux[.]com	images.h1x[.]com	sport.wikaba[.]com
bsnl1.dynamic-dns[.]net	images.ikwb[.]com	spyd123.dynamic-dns[.]net
bswan.authorizeddns[.]org	item.itemdb[.]com	testtest.x24hr[.]com
cat.moneyhome[.]biz	l1nkedin.ns01[.]biz	token.dns04[.]com
cipp.dns04[.]com	linkedin.2waky[.]com	udm.dns05[.]com
clients.cleansite[.]info	money.moneyhome[.]biz	udomain.mrbonus[.]com
cronous.wikaba[.]com	mtnl1.dynamic-dns[.]net	udomaincom.dynamic-dns[.]net
ddns.4pu[.]com	mxmail.esmtp[.]biz	users.fartit[.]com
ddxsn.ddns[.]info	netsysdom.dynamic-dns[.]net	vada.my03[.]com
dr0pb0x.zyns[.]com	newnw.4pu[.]com	vb.xxuz[.]com
dropbox.dns2[.]us	newpic.sexxxy[.]biz	voda.dns04[.]com
excharge.sexxxy[.]biz	news.mrbonus[.]com	wind.ikwb[.]com
faceb00k.ns01[.]info	nxead.itemdb[.]com	winner.ikwb[.]com
faceb0ok.2waky[.]com	pachost.dynamic-dns[.]net	winner.serveuser[.]com
firejun.freeddns[.]com	pachost.wikaba[.]com	wordpr.dynamic-dns[.]net
firejun.freetcp[.]com	patch.itsaol[.]com	wordpressb.justdied[.]com
firejun.myddns[.]com	pd.zzux[.]com	wpblog.dynamic-dns[.]net
foods.x24hr[.]com	pd1.dynamic-dns[.]net	wwwss.mrbasic[.]com
forum1.zzux[.]com	pdbana.dynamic-dns[.]net	wxxxs.mefound[.]com
foryou.x24hr[.]com	pic.4pu[.]com	xnews.ikwb[.]com
free.itsaol[.]com	pic.x24hr[.]com	xnews.mypicture[.]info
gold.bigmoney[.]biz	purdue.dynamic-dns[.]net	xvideo.mrslove[.]com
gold.mrbonus[.]com	readme.myddns[.]com	xx0ssd.isasecret[.]com
happysky.edns[.]biz	rem0te.edns[.]biz	xx0xx.dnset[.]com
help.wikaba[.]com	remoteset.zyns[.]com	xznews.zzux[.]com
hike.dns04[.]com	remotetest.dynamic-dns[.]net	zxerbqr.zyns[.]com
hirez.ddns[.]info		

Spearphishing E-mail Accounts

0x41ex@gmail[.]com	hee_chow_ming@yahoo.com[.]hk	nslookup168@gmail[.]com
0x5h31l@gmail[.]com	hiliana550jonson@gmail[.]com	nuyuchen1983@hotmail[.]com
3g.xiao.i@gmail[.]com	himyjb@gmail[.]com	parameters4512@outlook[.]com
a210f1@gmail[.]com	holleword@hotmail[.]com	paulmckee518@gmail[.]com
aaronjayjack@outlook[.]com	hostay88@gmail[.]com	peterlovell29@gmail[.]com

- agsyhfyrdetyhfdgsh@gmail[.]com
- andreatilley178@gmail[.]com
- andr-lang@outlook[.]com
- angela.kuolt90@gmail[.]com
- angelatyrrell844@gmail[.]com
- anssi.kanninen@outlook[.]com
- anvisoftceo@gmail[.]com
- anydkim9@gmail[.]com
- artomikkola@outlook[.]com
- ashiksaha73@gmail[.]com
- b1ackn1ve@gmail[.]com
- bajsingh63@gmail[.]com
- baptistevillanyi@gmail[.]com
- bhssasqza54251@gmail[.]com
- blackwolf915@gmail[.]com
- blackwolf915@outlook[.]com
- bogart.mig@gmail[.]com
- bossjiang2016@outlook[.]com
- carlietoole56@gmail[.]com
- cary.emily90@gmail[.]com
- cheng.cheng.cheng3@gmail[.]com
- chris.weaver049@gmail[.]com
- ckevin324@gmail[.]com
- code.sec01@gmail[.]com
- danieldociu81@gmail[.]com
- dilo220sayontony@gmail[.]com
- epovkhan@gmail[.]com
- ervartiainen@gmail[.]com
- georgecraven379@gmail[.]com
- gogoiobit@gmail[.]com
- greatyeon3@gmail[.]com
- greatyeon7@gmail[.]com
- gsecdump@gmail[.]com
- gtagqwrxjhec@gmail[.]com
- gwanling1456@yahoo[.]com
- hangobangeros526c@gmail[.]com
- haueh410gakiam@gmail[.]com
- hrprter777@gmail[.]com
- hrsimon59@gmail[.]com
- ikoumoutzelis@gmail[.]com
- inministryofhealth@gmail[.]com
- ishiicaron@gmail[.]com
- jacktake@outlook[.]com
- jennyradford45@gmail[.]com
- jimgrem@msn[.]com
- jimgrou@msn[.]com
- jinnyit987@gmail[.]com
- johnx19@hotmail[.]com
- jonreal27@gmail[.]com
- josephbrier300@gmail[.]com
- josuepined@outlook[.]com
- justbyebye@hotmail[.]com
- justinbethune@hotmail[.]com
- karolinebartush67@gmail[.]com
- lauramuollo@yahoo[.]com
- lauren19111@hotmail[.]com
- lhm_cn@msn[.]com
- lhmjustfun@gmail[.]com
- liveupdate@outlook[.]com
- maddulasavitri@gmail[.]com
- mark_hedin@yahoo[.]com
- michaelbrown2151@gmail[.]com
- mikecoo2020@yahoo[.]com
- mm4rbury@outlook[.]com
- morissafetzko4@gmail[.]com
- mralphmielke@gmail[.]com
- ms.alienware@gmail[.]com
- mstsc@live[.]com
- myjobs.kr.hr@gmail[.]com
- nanettehoagland676@gmail[.]com
- nesakjsfdkl8754@gmail[.]com
- niying322@gmail[.]com
- nodarie89@yahoo[.]com
- nohavesky@hotmail[.]com
- petervc1983@gmail[.]com
- petter.mark@mail[.]com
- puttyoffice@gmail[.]com
- qiongzhi777@live[.]com
- qungtlak@gmail[.]com
- richardreed647@gmail[.]com
- robertaponte331@gmail[.]com
- robertblanchard511@gmail[.]com
- ryandaws@outlook[.]com
- shavonyasbjqoj@gmail[.]com
- skydrive1951@hotmail[.]com
- skydrivewinsborn@hotmail[.]com
- sotadoanfybs@hotmail[.]com
- stevenwhipple48@gmail[.]com
- summery679@gmail[.]com
- susanne.sawer@gmail[.]com
- sworgan88@gmail[.]com
- symanteclabs@outlook[.]com
- takeown2009@outlook[.]com
- terrenceruddell59@gmail[.]com
- thplldeepak@gmail[.]com
- tony.john90@outlook[.]com
- tw.slax@gmail[.]com
- ualmansife523f@gmail[.]com
- unameid@gmail[.]com
- us.webgame@gmail[.]com
- vaniadower5641c@gmail[.]com
- violetteclaveau54c@gmail[.]com
- willardstone92@gmail[.]com
- wljsdd@gmail[.]com
- wrennieeller564c@gmail[.]com
- ysummer56@gmail[.]com
- zeplin.law@gmail[.]com
- zeplincopyright@gmail[.]com
- zeplinlegal@gmail[.]com
- znetdevil@msn[.]com

Recommended Mitigations

Patch and Vulnerability Management:

- Install vendor-provided and verified patches to all systems for critical vulnerabilities, prioritizing timely patching of Internet-connected servers for known vulnerabilities and software processing Internet data, such as web browsers, browser plugins, and document readers.
- Ensure proper migrating steps or compensating controls are implemented for vulnerabilities that cannot be patched in a timely manner.
- Maintain up-to-date antivirus signatures and engines.
- Recommend that organizations routinely audit their configuration and patch management programs to ensure they can track and mitigate emerging threats. Implementing a rigorous configuration and patch management program will hamper sophisticated cyber threat actors' operations and protect organizations' resources and information systems.

Protect Credentials:

- Strengthen credential requirements and implement multi-factor authentication to protect individual accounts, particularly for webmail and VPN access and for accounts that access critical systems. Regularly change passwords and do not reuse passwords for multiple accounts.
- Audit all remote authentications from trusted networks or service providers.
- Detect mismatches by correlating credentials used within internal networks with those employed on external-facing systems.
- Log use of system administrator commands, such as net, ipconfig, and ping.
- Audit logs for suspicious behavior.
- Enforce principle of least privilege.

Network Hygiene and Monitoring:

- Actively scan and monitor internet-accessible applications for unauthorized access, modification, and anomalous activities.
- Actively monitor server disk use and audit for significant changes.
- Log DNS queries and consider blocking all outbound DNS requests that do not originate from approved DNS servers. Monitor DNS queries for C2 over DNS.
- Develop and monitor the network and system baselines to allow for the identification of anomalous activity. Identify and suspend access of users exhibiting unusual activity.
- Use whitelist or baseline comparison to monitor Windows event logs and network traffic to detect when a user maps a privileged administrative share on a Windows system.
- Leverage multi-sourced threat-reputation services for files, DNS, URLs, IPs, and email addresses.
- Network device management interfaces, such as Telnet, SSH, Winbox, and HTTP, should be turned off for WAN interfaces and secured with strong passwords and encryption when enabled. Identify and suspend access of users exhibiting unusual activity.
- When possible, segment critical information on air-gapped systems. Use strict access control measures for critical data.

Administrative Note

This product is marked TLP:WHITE. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Your Feedback on the Value of this Product Is Critical

Was this product of value to your organization? Was the content clear and concise? Your comments are very important to us and can be submitted anonymously. Please take a moment to complete the survey at the link below. Feedback should be specific to your experience with our written products to enable the FBI to make quick and continuous improvements to such products. Feedback may be submitted online here:

https://www.ic3.gov/PIFSurvey

Please note that this survey is for feedback on content and value only.