LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

Chinese State-Sponsored Cyber Activity

11/19/2020

Report #: 202011191030

Agenda

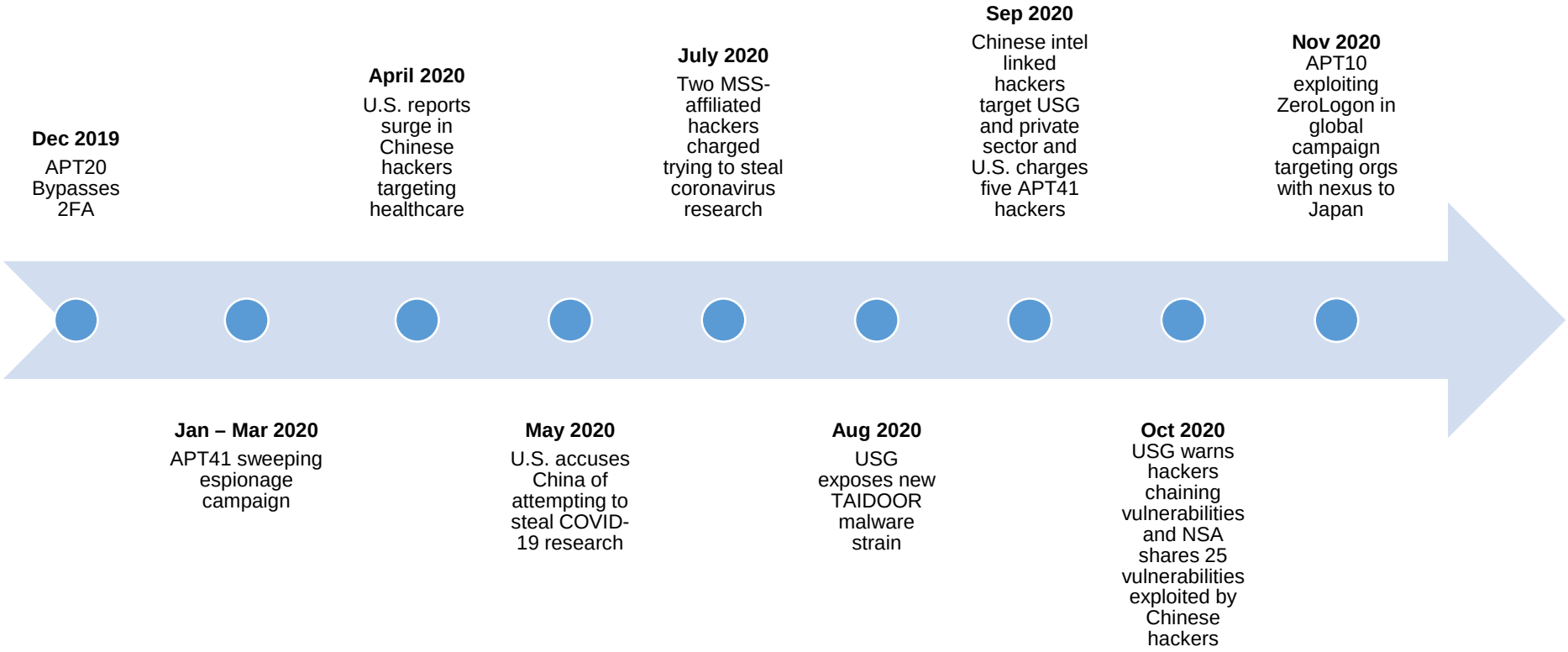
- Timeline of Recent Activity
- Chinese APT Groups
- Pre-pandemic Targeting
- Targeting during COVID-19
- Exploited Vulnerabilities
- Patches and Mitigations
- Outlook

Slides Key:

Non-Technical: Managerial, strategic and high-level (general audience)

Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

Timeline of Recent Activity



Chinese APT Groups Targeting HPH Sector

- According to industry experts, China has the most number of active APTs and threat actor groups when compared to other countries, followed by Russia, Iran and North Korea.
- FireEye currently publicly tracking a **total of at least 28 APT groups** with suspected attribution to China
- Out of these 28 Chinese APT groups, at least 8 of them are known to have previously targeted the healthcare and public health (HPH) sector:

1. APT41
2. APT24 AKA PittyTiger
3. APT22
4. APT20 AKA Twivy
5. APT18 AKA Wekby
6. APT10 AKA Menupass
7. APT9 AKA Nightshade Panda
8. APT1 AKA Unit 61398, Comment Crew

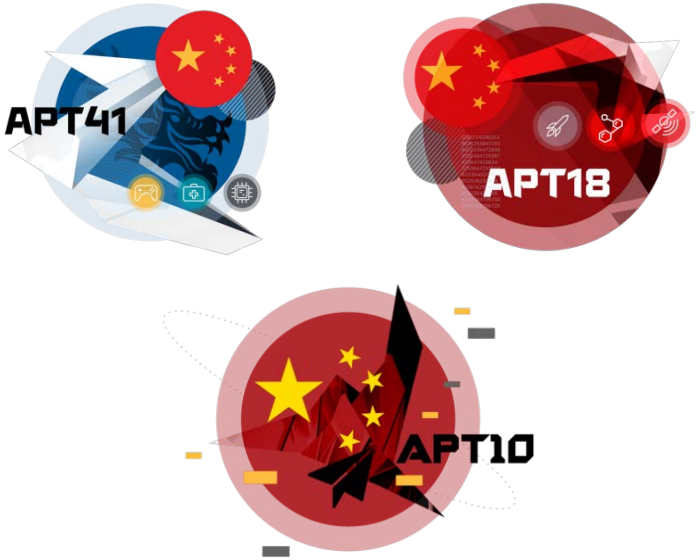


Image source: fireeye.com

APT41

Suspected attribution: China

Target sectors: APT41 has directly targeted organizations in at least 14 countries dating back to as early as 2012. The group's espionage campaigns have targeted healthcare, telecoms, and the high-tech sector, and have historically included stealing intellectual property. Their cyber crime intrusions are most apparent among video game industry targeting, including the manipulation of virtual currencies, and attempted deployment of ransomware. APT41 operations against higher education, travel services, and news/media firms provide some indication that the group also tracks individuals and conducts surveillance.

Image source: fireeye.com

Overview: APT41 is a prolific cyber threat group that carries out Chinese state-sponsored espionage activity in addition to financially motivated activity potentially outside of state control.

Associated malware: CROSSWALK, HIGHNOON, xDoor, Xmrig, ASPXSpy, China Chopper, BEACON, MESSAGETAP, Gh0st, njRAT, PlugX, ZxShell, Mimikatz, and BLACKCOFFEE, POISONPLUG

Attack vectors: APT41 often relies on spear-phishing emails with attachments such as compiled HTML (.chm) files to initially compromise their victims. Once in a victim organization, APT41 can leverage more sophisticated TTPs and deploy additional malware. For example, in a campaign running almost a year, APT41 compromised hundreds of systems and used close to 150 unique pieces of malware including backdoors, credential stealers, keyloggers, and rootkits. APT41 has also deployed rootkits and Master Boot Record (MBR) bootkits on a limited basis to hide their malware and maintain persistence on select victim systems.

APT41 Wanted Poster (September 2020)
Image source: FBI

APT24

Also known as: PittyTiger

Suspected attribution: China

Target sectors: APT24 has targeted a wide variety of industries, including organizations in the healthcare, government, construction and engineering, mining, nonprofit, and telecommunications industries.

Overview: This group is known to have targeted organizations headquartered in countries including the U.S. and Taiwan usually for the goal of intellectual property theft. APT24 has historically used the RAR archive utility to encrypt and compress stolen data prior to transferring it out of the network. Data theft exfiltrated from this actor mainly focused on documents with political significance, suggesting its intent is to monitor the positions of various nation states on issues applicable to China's ongoing territorial or sovereignty dispute.

Associated malware: PITTYTIGER, Mimikatz, ENFAL, TAIDOOR, Gh0st RAT, PoisonIvy

Attack vectors: APT24 has used phishing emails that use military, renewable energy, or business strategy themes as lures. PittyTiger also attempts to obtain legitimate credentials during operations (T1078) and has leveraged vulnerabilities in Microsoft Office products.

Image source: fireeye.com

APT22

Also known as: Barista

Suspected attribution: China

Target sectors: Healthcare, biomedical, and pharmaceutical as well as a broad set of political, military, and economic entities in East Asia, Europe, and the U.S.

Overview: APT22 likely has a nexus to China and has been operational since at least early 2014, carrying out intrusions and attack activity against public and private sector entities, including dissidents. Conducted multi-year targeting of health center focused on cancer research.

Associated malware: PISCES, SOGU (AKA PlugX), FLATNOTE, ANGRYBELL, BASELESS, SEAWOLF, LOGJAM

Attack vectors: APT22 threat actors have used strategic web compromises in order to passively exploit targets of interest. APT22 actors have also identified vulnerable public-facing web servers on victim networks and uploaded web shells to gain access to the victim network.

Image source: fireeye.com

APT20

Also known as: Twivy

Suspected attribution: China

Target sectors: Healthcare, construction and engineering, non-profit organizations, defense industrial base and chemical research and production companies, MSPs

Overview: APT20 engages in cyber operations where the goal is data theft. APT20 conducts intellectual property theft but also appears interested in stealing data from or monitoring the activities of individuals with particular political interests. Based on available data, this is likely a freelancer group with some nation state sponsorship located in China.

Associated malware: QIAC, SOGU (AKA DestroyRAT, PlugX, Korplug), Gh0st RAT, ZXSHELL, Poison Ivy, BEACON (Cobalt Strike), HOMEUNIX, STEW

Attack vectors: APT20 has exploited vulnerabilities in Jboss web servers using 'living off the land' techniques and succeeded in moving laterally throughout network to compromise systems and dump passwords of admin accounts. The group has also successfully bypassed two-factor authentication (2FA) on VPN accounts.

Image source: fireeye.com

APT18

Also known as: Wekby, TG-0416, Dynamite Panda

Suspected attribution: China

Target sectors: Health and Biotechnology, Aerospace and Defense, Construction and Engineering, Education, High Tech, Telecommunications, Transportation

Overview: Very little has been released publicly about this group but APT18 is believed to be responsible for the 2014 attack on Community Health Systems Inc. which resulted in theft of SSNs and PII for 4.5 million patients.

Associated malware: Gh0st RAT, HTTPBrowser, pisloader, PoisonIvy

Attack vectors: Frequently developed or adapted zero-day exploits for operations, which were likely planned in advance. Used data from Hacking Team leak, which demonstrated how the group can shift resources (i.e. selecting targets, preparing infrastructure, crafting messages, updating tools) to take advantage of unexpected opportunities like newly exposed exploits. APT18 previously exploited the OpenSSL Heartbleed vulnerability in 2014.

Image source: fireeye.com

APT10

Also known as: Menupass Team, Stone Panda, Red Apollo, Cicada, CVNX, HOGFISH, Cloud Hopper

Suspected attribution: China

Target sectors: Healthcare, construction and engineering, aerospace, and telecom firms, and governments in the United States, Europe, and Japan

Overview: APT10 is a Chinese cyber espionage group tracked since 2009. Researchers believe that the targeting of these industries has been in support of Chinese national security goals, including acquiring valuable military and intelligence information as well as the theft of confidential business data to support Chinese corporations.

Associated malware: HAYMAKER AKA ChChes AKA Scorpion, SNUGRIDE, BUGJUICE AKA RedLeaves (overlap with PlugX), QUASARRAT AKA xRAT

Attack vectors: Traditional spear phishing and access to victim's networks through managed service providers (MSPs). APT10 spear phishes have been relatively unsophisticated, leveraging .lnk files within archives, files with double extensions. APT10 has successfully remained undetected in victim environments for up to a year. The group has been seen leveraging 'living off the land' techniques, DLL-side-loading and custom DLL loaders, ZeroLogon vulnerability, RAR archiving, certutil, adfind, csvde, ntdsutil, WMIExec, and PowerShell as well as using legitimate cloud file hosting services for exfiltration.

Image source: fireeye.com

APT9

Also known as: Nightshade Panda

Suspected attribution: Based on available data, we assess that this is a freelancer group with some nation-state sponsorship, possibly China.

Target sectors: Organizations headquartered in multiple countries and in industries such as health care and pharmaceuticals, construction and engineering, and aerospace and defense.

Overview: APT9 engages in cyber operations where the goal is data theft, usually focusing on the data and projects that make a particular organization competitive within its field.

Associated malware: SOGU (AKA DestroyRAT, PlugX, Korplug), HOMEUNIX, PHOTO (AKA Derusbi), FUNRUN, Gh0st, ZXSHEL

Attack vectors: APT9 was historically very active in the pharmaceuticals and biotechnology industry. Researchers observed this actor use spearphishing, valid accounts, as well as remote services for Initial Access. On at least one occasion, analysts observed APT9 at two companies in the biotechnology industry and suspect that APT9 actors may have gained initial access to one of the companies by using a trusted relationship between the two companies. APT9 use a wide range of backdoors, including publicly available backdoors, as well as backdoors that are believed to be custom, but are used by multiple APT groups.

Image source: fireeye.com

Threat Group Profile: APT1 AKA Comment Crew

Also known as: Comment Crew, TG-8223, Group 3, Byzantine Candor

Suspected attribution: China's People's Liberation Army (PLA) General Staff Department's 3rd Department, Unit 61398

Target sectors: Healthcare, Information Technology, Scientific Research and Consulting, International Organizations, Food and Agriculture, Education, and many more

Overview: APT1 has systematically stolen hundreds of terabytes of data from at least 141 organizations, and has demonstrated the capability and intent to steal from dozens of organizations simultaneously. The group focuses on compromising organizations across a broad range of industries in English-speaking countries. The size of APT1's infrastructure implies a large organization with at least dozens, but potentially hundreds of human operators.

Associated malware: TROJAN.ECLTYS, BACKDOOR.BARKIOFORK, BACKDOOR.WAKEMINAP, TROJAN.DOWNBOT, BACKDOOR.DALBOT, BACKDOOR.REVIRD, TROJAN.BADNAME, BACKDOOR.WUALESS, PoisonIvy, Gh0st RAT, Mimikatz, Seasalt (similar to OceanSalt)

Attack vectors: Spear phishing for initial compromise leveraging malicious attachment or hyperlink to malicious file; use of mainly custom but also some public backdoors; usually installs numerous backdoors in victim environments

Image source: SecurityAffairs

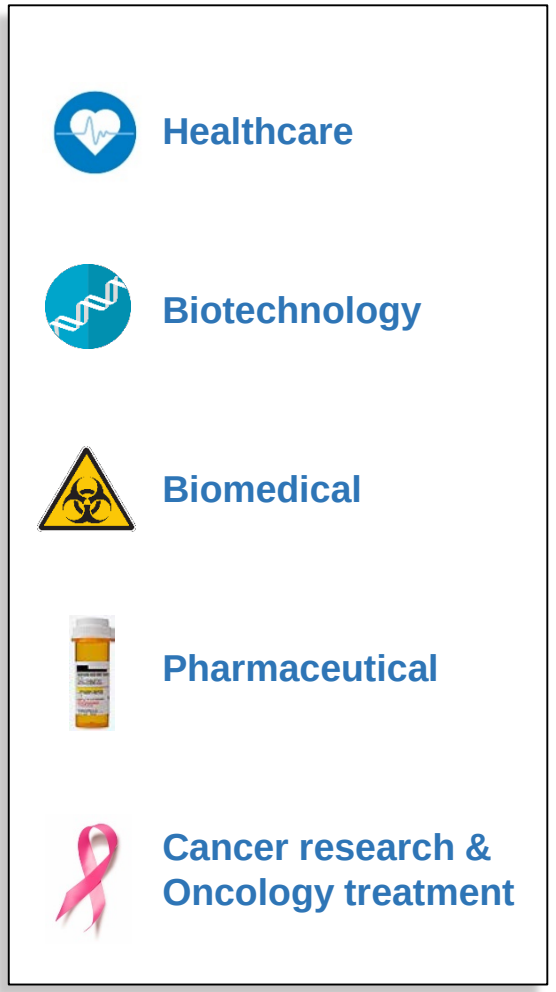
Five Chinese Military Hackers Charged with Cyber Espionage Against U.S.

From left, Chinese military officers Gu Chunhui, Huang Zhenyu, Sun Kailiang, Wang Dong, and Wen Xinyu have been indicted on cyber espionage charges.

Members APT1 AKA Comment Crew, Unit 61398 Wanted Poster (May 2014)
Image source: FBI

- China has long been driven by an interest in acquiring medical research and collecting large data sets of information, potentially for the purposes of fostering intelligence operations.
- Actors observed targeting the healthcare sector include China-nexus APT10 (Menupass) and APT41
- In early April 2019, suspected Chinese cyber espionage actors targeted a U.S.-based health center—with a strong focus on cancer research—with EVILNUGGET malware. One of the lure documents referenced a conference hosted by the targeted organization. In alignment with a trend we continue to witness affecting healthcare, this same organization has been targeted by multiple Chinese threat actors in the past.
  - A year prior in 2018, China-nexus APT41 used CROSSWALK malware to spearphish individuals at this same healthcare entity.
  - APT22—a Chinese group that has focused on biomedical, pharmaceutical, and healthcare organizations in the past, and continues to be active—also targeted this same organization in prior years.
- August 2019: Chinese hackers focused on cancer research

Targeted Industries



- More aggressive targeting of organization involved in COVID-19 response and Operation Warp Speed (OWS)
- Biotech and other firms publicly known for work on COVID-19 vaccines, treatments, and testing technology in the US and abroad
  - **January 2020**: LI searched for vulnerabilities at a Maryland biotech firm which had days prior announced work on COVID-19 vaccine
  - **February 2020**: LI searched for vulnerabilities in network of a California biotech firm that had just announced research for antiviral drugs to treat COVID-19
  - **May 2020**: LI searched for vulnerabilities in network of California diagnostics company publicly known to be involved in development of COVID-19 testing kits
  - **June 2020**: reconnaissance on network of a Massachusetts biotech firm focused on cancer treatment (possibly also involved in COVID-19 vaccine development)

Targeted Industries


Healthcare


Biotechnology


Biomedical


Pharmaceutical


COVID-19 research & vaccine development

July 2020: Indictment of Two MSS-Affiliated Hackers

WANTED BY THE FBI

CHINA MSS GUANGDONG STATE SECURITY DEPARTMENT HACKERS

Unauthorized Access; Conspiracy to Access Without Authorization and Damage Computers; Conspiracy to Commit Theft of Trade Secrets; Conspiracy to Commit Wire Fraud; Aggravated Identity Theft

Li Xiaoyu

Dong Jiazhi

CAUTION

On July 7, 2020, a grand jury in the United States District Court for the Eastern District of Washington indicted Li Xiaoyu and Dong Jiazhi for their alleged participation in a long-running campaign of computer network operations targeting the networks of United States and foreign companies across a wide variety of industries, including high tech manufacturing; civil, heavy, and medical device engineering; business, educational, and gaming software; solar energy; pharmaceuticals; and defense. The indictment highlighted Li and Dong's alleged actions, including a recent focus on COVID-19 research, testing, and treatment; the targeting of political dissidents, religious minorities, and human rights advocates in mainland China, Hong Kong, the United States, and Canada; and the intrusions into corporate networks of countries in Europe and Asia.

Some of Li and Dong's network operations were allegedly undertaken for their own economic benefits, while others were allegedly for the benefits of China's Ministry of State Security (MSS), including the Guangdong State Security Department.

If you have any information concerning these individuals, please contact your local FBI office, or the nearest American Embassy or Consulate.

Field Office: Seattle

www.fbi.gov

Wanted poster for Li Xiaoyu and Dong Jiazhi.
Image source: FBI

Exploited Vulnerabilities

CVE Number	Affected Product	Vulnerability Type
CVE-2019-11510 (CRITICAL)	Pulse Secure VPN	Arbitrary file reading vulnerability which can lead to exposure of keys or passwords
CVE-2020-5902 (CRITICAL)	F5 BIG-IP proxy / load balancer devices TMUI	Remote code execution vulnerability in undisclosed pages
CVE-2019-19781 (CRITICAL)	Citrix ADC Citrix Gateway	Directory traversal which can lead to remote code execution without credentials
CVE-2020-8193 CVE-2020-8195 CVE-2020-8196 (MEDIUM)	Citrix ADC Citrix Gateway Citrix SDWAN WAN-OP	Improper access control and input validation which allows unauthenticated access to certain URL endpoints and information disclosure to low-privileged users
CVE-2019-0708 (CRITICAL)	Microsoft Windows11 XP - 7, Microsoft Windows Server12 2003 - 2008.	Remote code execution vulnerability in Remote Desktop Services
CVE-2020-15505 (CRITICAL)	MobileIron mobile device management (MDM)	Remote code execution vulnerability which allows attackers to execute arbitrary code from unspecified vectors

Exploited Vulnerabilities (cont.)

CVE Number	Affected Product	Vulnerability Type
CVE-2020-1350 (CRITICAL)	Microsoft Windows Server 2008 - 2019	A remote code execution vulnerability exists in Windows® Domain Name System servers when they fail to properly handle requests.
CVE-2020-1472 (CRITICAL)	Microsoft Windows Server 2008 – 2019	An elevation of privilege vulnerability exists when an attacker establishes a vulnerable Netlogon secure channel connection to a domain controller, using the Netlogon Remote Protocol (MS-NRPC), aka 'Netlogon Elevation of Privilege Vulnerability'.
CVE-2019-1040 (MEDIUM)	Microsoft Windows 7 - 10, Microsoft Windows Server 2008 - 2019	A tampering vulnerability exists in Microsoft Windows® when a man-in-the-middle attacker is able to successfully bypass the NTLM MIC (Message Integrity Check) protection.
CVE-2018-6789 (CRITICAL)	Exim before 4.90.1.	Sending a handcrafted message to Exim mail transfer agent may cause a buffer overflow. This can be used to execute code remotely.
CVE-2020-0688 (HIGH)	Microsoft Exchange Server	A Microsoft Exchange validation key remote code execution vulnerability exists when the software fails to properly handle objects in memory.
CVE-2020-8515 (CRITICAL)	DrayTek Vigor	DrayTek Vigor devices allow remote code execution as root (without authentication) via shell metacharacters.

Exploited Vulnerabilities (cont.)

CVE Number	Affected Product	Vulnerability Type
CVE-2018-4939 (CRITICAL)	Adobe ColdFusion	Certain Adobe ColdFusion®14 versions have an exploitable Deserialization of Untrusted Data vulnerability. Successful exploitation could lead to arbitrary code execution.
CVE-2015-4852 (N/A)	Oracle WebLogic Server	The WLS Security component in Oracle WebLogic15 Server allows remote attackers to execute arbitrary commands via a crafted serialized Java16 object.
CVE-2020-2555 (HIGH)	Oracle Coherence	A vulnerability exists in the Oracle Coherence product of Oracle Fusion Middleware. This easily exploitable vulnerability allows unauthenticated attacker with network access via T3 to compromise Oracle Coherence.
CVE-2019-3396 (CRITICAL)	Atlassian Confluence	The Widget Connector macro in Atlassian Confluence17 Server allows remote attackers to achieve path traversal and remote code execution on a Confluence Server or Data Center instance via server-side template injection.
CVE-2019-11580 (CRITICAL)	Atlassian Crowd	Attackers who can send requests to an Atlassian Crowd or Crowd Data Center instance can exploit this vulnerability to install arbitrary plugins, which permits remote code execution.
CVE-2020-10189 (CRITICAL)	Zoho ManageEngine Desktop Central	Zoho ManageEngine®18 Desktop Central allows remote code execution because of deserialization of untrusted data.

Exploited Vulnerabilities (cont.)

CVE Number	Affected Product	Vulnerability Type
CVE-2019-18935 (CRITICAL)	Progress Telerik UI	Progress Telerik®19 UI for ASP.NET AJAX contains a .NET deserialization vulnerability. Exploitation can result in remote code execution.
CVE-2020-0601 (HIGH)	Microsoft Windows 10, Server 2016 - 2019.	A spoofing vulnerability exists in the way Windows® CryptoAPI (Crypt32.dll) validates Elliptic Curve Cryptography (ECC) certificates. An attacker could exploit the vulnerability by using a spoofed code-signing certificate to sign a malicious executable, making it appear that the file was from a trusted, legitimate source.
CVE-2019-0803 (HIGH)	Microsoft Windows 7 - 10, Microsoft Windows Server 2008 - 2019.	An elevation of privilege vulnerability exists in Windows® when the Win32k component fails to properly handle objects in memory.
CVE-2017-6327 (HIGH)	Symantec Messaging Gateway	The Symantec Messaging Gateway can encounter a remote code execution issue.
CVE-2020-3118 (HIGH)	Cisco IOS XR	A vulnerability in the Cisco® Discovery Protocol implementation for Cisco IOS®23 XR Software could allow an unauthenticated, adjacent attacker to execute arbitrary code or cause a reload on an affected device.

- Keep systems and products updated and patched as soon as possible after patches are released.
- Expect that data stolen or modified (including credentials, accounts, and software) before the device was patched will not be alleviated by patching, making password changes and reviews of accounts a good practice.
- Disable external management capabilities and set up an out-of-band management network.
- Block obsolete or unused protocols at the network edge and disable them in device configurations.
- Isolate Internet-facing services in a network Demilitarized Zone (DMZ) to reduce the exposure of the internal network.
- Enable robust logging of Internet-facing services and monitor the logs for signs of compromise.
- Additional mitigations specific to each vulnerability provided in NSA Cybersecurity Advisory Oct 2020
- Health Industry Cybersecurity Practices, Cybersecurity Act of 2015, Section 405(d) guidance

Outlook

- Cyber threat activity unlikely to subside even after COVID-19
- Continue to exploit known vulnerabilities in common products for remote access and external web services
- Possibility that Chinese APT actors not traditionally focused on healthcare sector shift targeting to adapt to national priorities
- Multiple Chinese APT groups may attempt to compromise the same target(s)
- While there has been much attention on ransomware and Eastern European threat actors targeting the US HPH sector lately, the Chinese threat has not gone away
- If critical vulnerabilities remain unpatched, cyber threat actors can carry out attacks without the need to develop custom malware and exploits or use previously unknown vulnerabilities to target a network

Reference Materials

References

- NSA: Top 25 vulnerabilities actively abused by Chinese hackers
  - https://www.bleepingcomputer.com/news/security/nsa-top-25-vulnerabilities-actively-abused-by-chinese-hackers/
- NSA Warns Chinese State-Sponsored Malicious Cyber Actors Exploiting 25 CVEs
  - https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/2387347/nsa-warns-chinese-state-sponsored-malicious-cyber-actors-exploiting-25-cves/
- US charges five hackers from Chinese state-sponsored group APT41 (16 September 2020)
  - https://www.zdnet.com/article/us-charges-five-hackers-part-of-chinese-state-sponsored-group-apt41/
- Chinese state-sponsored cyber actors are targeting bugs in F5, Citrix, Pulse and Microsoft Exchange Servers, US agencies warn (15 September 2020)
  - https://www.computing.co.uk/news/4020188/chinese-sponsored-cyber-actors-targeting-bugs-f5-citrix-pulse-microsoft-exchange-servers-us-agencies-warn
- Feds warn that Chinese attempts to hack health care, drug firms threaten U.S. COVID-19 response (13 May 2020)
  - https://www.nbcnews.com/politics/national-security/feds-warn-chinese-attempts-hack-health-care-drug-firms-threaten-n1206151
- HC3, APT and Cybercriminal Targeting of HCS (9 June 2020)
  - https://www.hhs.gov/sites/default/files/apt-and-cybercriminal-targeting-of-hcs.pdf

References

- FireEye, Beyond Compliance: Cyber Threats and Healthcare (2019)
  - https://www.fireeye.com/content/dam/collateral/en/wp-beyond-compliance-cyber-threats-and-healthcare.pdf
- Chinese-speaking hackers increase activity and diversify cyberattack methods (5 August 2020)
  - https://www.techradar.com/news/chinese-speaking-hackers-increase-activity-and-diversify-cyberattack-methods
- State-Sponsored Cyberattacks Target Medical Research (21 August 2019)
  - https://www.darkreading.com/threat-intelligence/state-sponsored-cyberattacks-target-medical-research/d/d-id/1335590
- Chinese State-Sponsored Actors Exploit Publicly Known Vulnerabilities
  - https://otx.alienvault.com/pulse/5f8f08e03e906183f28915dc
  - https://media.defense.gov/2020/Oct/20/2002519884/-1/-1/0/CSA_CHINESE_EXPLOIT_VULNERABILITIES_UOO179811.PDF
- 2nd China Army Unit Implicated in Online Spying
  - https://www.nytimes.com/2014/06/10/technology/private-report-further-details-chinese-cyberattacks.html
- FireEye, APT10: New Tools, Global Campaign Latest Manifestation of Longstanding Threat (6 April 2017)
  - https://www.fireeye.com/blog/threat-research/2017/04/apt10_menupass_grou.html

References

- Chinese intelligence-linked hackers are exploiting known flaws to target Washington, US says
  - https://www.cyberscoop.com/chinese-intelligence-hackers-us-government-agencies-ministry-state-security/
- Alert (AA20-258A): Chinese Ministry of State Security-Affiliated Cyber Threat Actor Activity
  - https://us-cert.cisa.gov/ncas/alerts/aa20-258a
- CSIS, Strategic Technologies Program, Significant Cyber Incidents Database
  - https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents
- Malware Analysis Report (AR20-216A) MAR-10292089-1.v2 – Chinese Remote Access Trojan: TAIDOOR
  - https://us-cert.cisa.gov/ncas/analysis-reports/ar20-216a
- Reversing Labs, Taidoor - a truly persistent threat (22 September 2020)
  - https://blog.reversinglabs.com/blog/taidoor-a-truly-persistent-threat
- Bloomberg, U.S. Says China Hackers Stole Secrets, Sought Virus Data (21 July 2020)
  - https://www.bloomberg.com/news/articles/2020-07-21/u-s-accuses-chinese-hackers-of-stealing-virus-trade-secrets
- US DOJ, Two Chinese Hackers Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including COVID-19 Research (21 July 2020)
  - https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion

References

- FireEye, This Is Not a Test: APT41 Initiates Global Intrusion Campaign Using Multiple Exploits (March 2020)
  - https://www.fireeye.com/blog/threat-research/2020/03/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.html
- Operation Wocao: Shining a light on one of China's hidden hacking groups
  - https://www.fox-it.com/en/news/whitepapers/operation-wocao-shining-a-light-on-one-of-chinas-hidden-hacking-groups/
- Reuters, Community Health says data stolen in cyber attack from China (18 August 2014)
  - https://www.reuters.com/article/us-community-health-cybersecurity/community-health-says-data-stolen-in-cyber-attack-from-china-idUSKBN0GI16N20140818
- McAfee, 'Operation Oceansalt' Attacks South Korea, U.S., and Canada With Source Code From Chinese Hacker Group (2018, October 18)
  - https://www.mcafee.com/enterprise/en-us/assets/reports/rp-operation-oceansalt.pdf
- CFR, PLA Unit 61398
  - https://www.cfr.org/cyber-operations/pla-unit-61398
- APT20: The limits of MFA exposed by a Chinese hacker group (5 February 2020)
  - https://medium.com/@Sekoia_team/apt20-the-limits-of-mfa-exposed-by-a-chinese-hacker-group-fe4cc4b3b107

Questions

Upcoming Briefs

- Disinformation and the Healthcare Sector (12/3)
- LOLBins use against healthcare (12/10)

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV** or call us Monday-Friday, between 9am-5pm (EST), at **(202) 691-2110.**

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback. If you wish to provide feedback please complete the HC3 Customer Feedback Survey.

HC3 Customer Feedback

Disclaimer

These recommendations are advisory and are not to be considered as Federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. HHS does not endorse any specific person, entity, product, service, or enterprise.

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Directed communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft and general notifications to the HPH about currently impacting threats via the HHS OIG

White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar

Briefing document and presentation that provides actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic or want to join our listserv? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.
Visit us at: www.HHS.Gov/HC3

Contact

www.HHS.GOV/HC3

(202) 691-2110

HC3@HHS.GOV