Tactics, Techniques, and Procedures of Indicted APT40 Actors Associated with China's MSS Hainan State Security Department

us-cert.cisa.gov/ncas/alerts/aa21-200a

Summary

This Joint Cybersecurity Advisory was written by the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) to provide information on a Chinese Advanced Persistent Threat (APT) group known in open-source reporting as APT40. This advisory provides APT40's tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) to help cybersecurity practitioners identify and remediate APT40 intrusions and established footholds.

APT40—aka BRONZE MOHAWK, FEVERDREAM, G0065, Gadolinium, GreenCrash, Hellsing, Kryptonite Panda, Leviathan, MUDCARP, Periscope, Temp.Periscope, and Temp.Jumper—is located in Haikou, Hainan Province, People's Republic of China (PRC), and has been active since at least 2009. APT40 has targeted governmental organizations, companies, and universities in a wide range of industries—including biomedical, robotics, and maritime research—across the United States, Canada, Europe, the Middle East, and the South China Sea area, as well as industries included in China's Belt and Road Initiative.

On July 19, 2021, the U.S. Department of Justice (DOJ) unsealed an indictment against four APT40 cyber actors for their illicit computer network exploitation (CNE) activities via front company Hainan Xiandun Technology Development Company (Hainan Xiandun). Hainan Xiandun employee Wu Shurong cooperated with and carried out orders from PRC Ministry of State Security (MSS) Hainan State Security Department (HSSD) intelligence officers Ding Xiaoyang, Zhu Yunmin, and Cheng Qingmin to conduct CNE. Wu's CNE activities resulted in the theft of trade secrets, intellectual property, and other high-value information from companies and organizations in the United States and abroad, as well as from multiple foreign governments. These MSS-affiliated actors targeted victims in the following industries: academia, aerospace/aviation, biomedical, defense industrial base, education, government, healthcare, manufacturing, maritime, research institutes, and transportation (rail and shipping).

Click here for a PDF version of this report.

(Updated July 19, 2021)

Click here for indicators of compromise (IOCs) in STIX format. **Note:** to uncover malicious activity, incident responders search for IOCs in network- and host-based artifacts and assess the results—eliminating false positives during the assessment. For example, some MD5 IOCs in the STIX file identify legitimate tools—such as Putty, cmd.exe, svchost.exe, etc.—as indicators of compromise. Although the tools themselves are not malicious, APT40 attackers placed and used them from non-standard folders on victim systems during computer intrusion activity. If a legitimate tool is identified by an incident responder, then the location of the tool should be assessed to eliminate false positives or to uncover malicious activity. See Technical Approaches to Uncovering and Remediating Malicious Activity for more incident handling guidance.

Technical Details

This Joint Cybersecurity Advisory uses the MITRE ATT&CK® framework, version 9. See the ATT&CK for Enterprise framework for all referenced threat actor tactics and techniques.

APT40 [G0065] has used a variety of tactics and techniques and a large library of custom and open-source malware—much of which is shared with multiple other suspected Chinese groups—to establish initial access via user and administrator credentials, enable lateral movement once inside the network, and locate high value assets in order to exfiltrate data. Table 1 provides details on these tactics and techniques. **Note:** see the appendix for a list of the domains, file names, and malware MD5 hash values used to facilitate this activity.

Table 1: APT40 ATT&CK Tactics and Techniques

Tactics	Activities and Techniques
Reconnaissance [TA0043] and *Resource Development* [TA0042]	• Gathered victim identity information [T1589] by collecting compromised credentials [T1589.001] • Acquire infrastructure [T1583] to establish domains that impersonate legitimate entities [T1583.001], aka 'typosquatting', to use in watering hole attacks and as command and control (C2) [TA0011] infrastructure • Establish new [T1585.002] and compromise existing [T1586.002] email and social media accounts [1585.001] to conduct social engineering attacks
Initial Access [TA0001]	• External remote services (e.g., virtual private network [VPN] services) [T1133] • Spearphishing emails with malicious attachments [T1566.001] and links [T1566.002] • Drive-by compromises [T1189] and exploitation of public-facing applications [T1190] • Access to valid [T1078], compromised administrative [T1078.001] accounts

Execution [TA0002]	• Command and scripting interpreters [T1059] such as PowerShell [T1059.001] • Exploitation of software vulnerabilities in client applications to execute code [T1203] using lure documents that dropped malware exploiting various Common Vulnerabilities and Exposures (CVEs) • User execution [T1204] of malicious files [T1204.002] and links [T1566.002] attached to spearphishing emails [T1566.001]
Persistence [TA0003], *Privilege Escalation* [TA0004], *Credential Access* [TA0006], *Discovery* [TA0007], and *Lateral Movement* [TA0008]	APT40 has used a combination of tool frameworks and malware to establish persistence, escalate privileges, map, and move laterally on victim networks. Additionally, APT40 conducted internal spearphishing attacks [T1534]. • BADFLICK/Greencrash • China Chopper [S0020] • Cobalt Strike [S0154] • Derusbi/PHOTO [S0021] • Gh0stRAT [S0032] • GreenRAT • jjdoor/Transporter • jumpkick • Murkytop (`mt.exe`) [S0233] • NanHaiShu [S0228] • Orz/AirBreak [S0229] • PowerShell Empire [S0363] • PowerSploit [S0194] • Server software component: Web Shell [TA1505.003]
Defense Evasion [TA0005], *Command and Control* [TA0011], *Collection* [TA0009], and *Exfiltration* [TA0010]	• Use of steganography [T1027.003] to hide stolen data inside other files stored on GitHub • Protocol impersonation [T1001.003] by using Application Programming Interface (API) keys for Dropbox accounts in commands to upload stolen data to make it appear that the activity was a legitimate use of the Dropbox service • Protocol tunneling [T1572] and multi-hop proxies [T1090.003], including the use of Tor [S0183] • Use of domain typosquatting for C2 infrastructure [T1583.001] • Archive [T1560], encrypt [T1532], and stage collected data locally [T1074.001] and remotely [T1074.002] for exfiltration • Exfiltration over C2 channel [T1041]

Mitigations

Network Defense-in-Depth

Proper network defense-in-depth and adherence to information security best practices can assist in mitigating the threat and reducing the risk. The following guidance may assist organizations in developing network defense procedures.

Patch and Vulnerability Management

- Install vendor-provided and verified patches on all systems for critical vulnerabilities, prioritizing timely patching of internet-connected servers 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.
- Routinely audit configuration and patch management programs to ensure the ability to track and mitigate emerging threats. Implementing a rigorous configuration and patch management program will hamper sophisticated cyber threat actors' operations and protect resources and information systems.
- Review the articles in the References section for more information on Chinese APT exploitation of common vulnerabilities.

Protect Credentials

- Strengthen credential requirements, regularly change passwords, and implement multi-factor authentication to protect individual accounts, particularly for webmail and VPN access and for accounts that access critical systems. 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` .
- 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 Domain Name Service (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. Audit logs for suspicious behavior.
- Identify and suspend access of users exhibiting unusual activity.
- Use allowlist 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, IP addresses, and email addresses.
- Network device management interfaces—such as Telnet, Secure Shell (SSH), Winbox, and HTTP—should be turned off for wide area network (WAN) interfaces and secured with strong passwords and encryption when enabled.
- When possible, segment critical information on air-gapped systems. Use strict access control measures for critical data.

APPENDIX: APT40 Indicators of Compromise

APT40 used the following domains, file names, and malware MD5 hash values to facilitate the CNE activity outlined in this CSA between 2009 through 2018.

Domains

airbusocean[.]com	https://pastebin[.]com/vfb5mbbu	pacifichydrologic[.]c
cargillnotice[.]com	huntingtomingalls[.]com	philippinenewss[.]c
ccidmeekparry[.]info	indiadigest[.]in	philstarnotice[.]com
ccvzvhjhdf[.]website	jack-newnb[.]com	porndec143.chicker
cdigroups[.]com	kAty197.chickenkiller[.]com	santaclarasystem[.]
checkecc[.]com	louisdreyfu[.]com	scsnewstoday[.]con
chemscalere[.]com	mail2.ignorelist[.]com	secbkav[.]com
cnnzapmeta[.]com	masterroot[.]pw	Soure7788.chicken
corycs[.]com	microsql-update[.]info	tccoll[.]com
deltektimes[.]com	mihybb[.]com	teledynegroup[.]cor
Engaction[.]com	mlcdailynews[.]com	teledyneinstrument
ens-smithjonathan.rhcloud[.]com	movyaction[.]net	testdomain2019.chi
fishgatesite.wordpress[.]com	msusanode[.]com	thestar[.]live
goo2k88yyh2.chickenkiller[.]com	newbb-news[.]com	thrivedataview[.]cor
gttdoskip[.]com	nfmybb[.]com	thyssemkrupp[.]con
http://gkimertds.wordpress[.]com/feed/	nmw4xhipveaca7hm[.]onion.link/en_US/all.js	thyssenkrupp-marir
http://stackoverflow[.]com/users/3627469/angle-swift	nobug[.]uk.to	togetno992.mooo[.]
http://stackoverflow[.]com/users/3804206/swiftr-angle	notesof992.wordpress[.]com	tojenner97.chickenk
http://stackoverflow[.]com/users/3863346/gkimertdssdads	onlinenewspapers[.]club	trafficeco[.]com
vser.mooo[.]com	onlineobl[.]com	transupdate[.]com
https://pastebin[.]com/p1mktQpD	oyukg43t[.]website	troubledate[.]com
ultrasocial[.]info	wsmcoff[.]com	xbug.uk[.]to
usdagroup[.]com	www.yorkshire-espana-sa[.]com/english/servicios/	yootypes[.]com
	https://github[.]com/slotz/sharp-loader/commit/f9de338fb474fd970a7375030642d04179b9245d	

MD5 Malware Hashes

(Updated July 19, 2021) **Note:** to uncover malicious activity, incident responders search for indicators of compromise (IOCs) in network- and host-based artifacts and assess the results—eliminating false positives during the assessment. For example, some MD5 IOCs in the table below identify legitimate tools—such as PuTTY, cmd.exe, svchost.exe, etc.—as indicators of compromise. Although the tools themselves are not malicious, APT40 attackers placed and used them from non-standard folders on victim systems during computer intrusion activity. If a legitimate tool is identified by an incident responder, then the location of the tool should be assessed to eliminate false positives or to uncover malicious activity. See Technical Approaches to Uncovering and Remediating Malicious Activity for more incident handling guidance.

01234c0e41fc23bb5e1946f69e6c6221
018d3c34a296edd32e1b39b7276dcf7f
019b68e26df8750e2f9f580b150b7293
01fa52a4f9268948b6c508fef0377299
022bd2040ec0476d8eb80d1d9dc5cc92
039d9ca446e79f2f4310dc7dcc60ec55
043f6cdca33ce68b1ebe0fd79e4685af
04918772a2a6ccd049e42be16bcbee39
04dc4ca70f788b10f496a404c4903ac6
060067666435370e0289d4add7a07c3b
062c759d04106e46e027bbe3b93f33ef
07083008885d2d0b31b137e896c7266c
079068181a728d0d603fe72ebfc7e910
0803f8c5ee4a152f2108e64c1e7f0233
09143a14272a29c56ff32df160dfdb30
0985f757b1b51533b6c5cf9b1467f388
09aab083fb399527f8ff3065f7796443
0b7bb3e23a1be2f26b9adf7004fc6b52
0b9a614a2bbc64c1f32b95988e5a3359
0bbe092a2120b1be699387be16b5f8fb
0bbe769505ca3db6016da400539f77aa
0c3c00c01f4c4bad92b5ba56bd5a9598
0c4fa4dfbe0b07d3425fea3efe60be1c
0ca936a564508a1f9c91cb7943e07c30
0d69eefede612493afd16a7541415b95
0da08b4bfe84eacc9a1d9642046c3b3c
0dd7f10fdf60fc36d81558e0c4930984
0e01ec14c25f9732cc47cf6344107672
10191b6ce29b4e2bddb9e57d99e6c471
105757d1499f3790e69fb1a41e372fd9
207e3c538231eb0fd805c1fc137a7b46
20e52d2d1742f3a3caafbac07a8aa99a
226042db47bdd3677bd16609d18930bd
22823fed979903f8dfe3b5d28537eb47
2366918da9a484735ec3a9808296aab8
239a22c0431620dc937bc36476e5e245
2499390148fc99a0f38148655d8059e7
24dbcd8e8e478a35943a05c7adfc87cc
25a06ab7675e8f9e231368d328d95344
25b79ba11f4a22c962fea4a13856da7f
25fc4713290000cdf01d3e7a0cea7cef
11166f8319c08c70fc886433a7dac92d
1223302912ec70c7c8350268a13ad226
139e071dd83304cdcfd5280022a0f958
13c93dc9186258d6c335b16dc7bb3c8c
14e2b0e47887c3bfbddb3b66012cb6e8
15437cfedfc067370915864feec47678
15e1816280d6c2932ff082329d0b1c76
166694d13ac463ea1c2bed64fbbb7207
16a344cd612cca4f0944ba688609e3ac
16c0011ea01c4690d5e76d7b10917537
1734a2b176a12eba8b74b8ca00ef1074
18144e860d353600bbd2e917aed21fde
1815c3a7a4a6d95f9298abb5855a3701
181a5b55b7987b62b5236965f473ba3b
18c26c5800e9e2482f1507c96804023e
1932ce50b7b6c88014cf082228486e5c
1af78c50aca90ee3d6c3497848ac5705
1b44fb4aaff71b1f96cd049a9461eaf5
1bb8f32e6e0e089d6a9c10737cf19683
1c35a87f61953baace605fff1a2d0921
1c945a6b0deccc6cd2f63c31f255d0ec
1cb216777039fe6a8464fc6a214c3c86
1d3a10846819a07eef66deefcc33459a
1dd6c80b4ea5d83aff4480dcbbef520c
1e91f0f52994617651e9b4a449af551a
1eb568559e335b3ed78588e5d99f9058
1ef9c42efe6e9a08b7ebb16913fa0228
1f2befede815fcf65c463bf875fcf497
1f9bdc0435ff0914605f01db8ca77a65
1ffd883095ff3279b31650ca3a50ad3c
34521c0f78d92a9d95e4f3ff15b516db
34681367cbcc3933f0f4b36481bde44e
34aa195c604d0725d7dd2aa4cc4efe28
354b95e858bcaced369ecbfdec327e2b
35f456afbe67951b3312f3b35d84ff0a
3647d11c155d414239943c8c23f6e8ec
37578c69c515f1d0d49769930fba25ce
375cbb0a88111d786c33510bff258a21
37b9b4ed979bd2cf818e2783499bfb5e
3810a18650dbacecd10d257312e92f61
3975740f65c2fa392247c60df70b1d6d

2639805ae43e60c8f04955f0fe18391c
270df5aab66c4088f8c9de29ef1524b9
280e5a3b9671db31cf003935c34f8cf9
28366de82d9c4441f82b84246369ad3b
28628f709a23d5c02c91d6445e961645
28c6f235946fd694d2634c7a2f24c1ba
29c1b4ec0bc4e224af2d82c443cce415
2b8a06d1de446db3bbbd712cdb2a70ce
2bf998d954a88b12dbec1ee96b072cb9
2c408385acdb04f0679167223d70192b
2c9737c6922b6ca67bf12729dcf038f9
2dd9aab33fcdd039d3a860f2c399d1b1
2de0e31fda6bc801c86645b37ee6f955
2e5b59c62e6e2f3b180db9453968d817
2ee7168c0cc6e0df13d0f658626474bb
2eee367a6273ce89381d85babeae1576
2f0a52ce4f445c6e656ecebbcaceade5
2f9995bc34452c789005841bc1d8da09
30701b1d1e28107f8bd8a15fcc723110
31a72e3bf5b1d33368202614ffd075db
3389dae361af79b04c9c8e7057f60cc6
33d18e29b4ecc0f14c20c46448523fc8
46e80d49764a4e0807e67101d4c60720
480f3a13998069821e51cda3934cc978
48101bbdd897877cc62b8704a293a436
48548309036005b16544e5f3788561dc
4a23e0f2c6f926a41b28d574cbc6ac30
4ab825dc6dabf9b261ab1cf959bfc15d
4b18b1b56b468c7c782700dd02d621f4
4b93159610aaadbaaf7f60bea69f21a4
4beb3f7fd46d73f00c16b4cc6453dcdb
4dd6eab0fa77adb41b7bd265cfb32013
4e79e2cade96e41931f3f681cc49b60a
4ef1c48197092e0f3dea0e7a9030edc8
503f8dc2235f96242063b52440c5c229
50527c728506a95b657ec4097f819be6
5064dc5915a46bfa472b043be9d0f52f
513f559bf98e54236c1d4379e489b4bc
51e21a697aec4cc01e57264b8bfaf978
51f31ed78cec9dbe853d2805b219e6e7
52b0f7d77192fe6f08b03f0d4ea48e46
53ceeaf0a67239b3bc4b533731fd84af
3a4ec0d0843769a937b5dadbe8ea56b1
3ab6bf23d5d244bc6d32d2626bd11c08
3bf8bb90d71d21233a80b0ec96321e90
3c2fe2dbdf09cfa869344fdb53307cb2
3c3d453ecf8cc7858795caece63e7299
3cbb46065f3e1dccbd707c340f38ce6b
3cf9dc0fdc2a6ab9b6f6265dc66b0157
3e89c56056e5525bf4d9e52b28fbbca7
3eb6f85ac046a96204096ab65bbd3e7e
3f50eedf4755b52aa7a7b740bd21daa6
3fefa55daeb167931975c22df3eca20a
4012acd80613aaa693a5d6cd4e7239ba
40528e368d323db0ac5c3f5e1efe4889
407c1ea99677615b80b2ffa2ed81d513
417949c717f78dc9e55ca81a5f7ade3e
4260e71d89f622c6a3359c5556b3aad7
429c10429a2ebb5f161e04159a59cf5b
4315975499cdc50098dbdb5b8aa4a199
44fa9c5df4ae20c50313aae02ba8fb95
4519b5d443a048a8599144900c4e1f28
45eb058edde4e5755a5ea1aff3ce3db7
460dc00ce690efacb5db8273c80e2b23
5b3050df93629f2f6cb3801ed19963c5
5b37ac4d642b96c4bf185c9584c0257a
5b3e945cd32a380f09ea98746f570758
5b72df8f6c110ae1d603354fcd8fe104
5c6f5cd81b099014718056e86b510fa2
5d63a3a02df2beda9d81f53abbd8264a
5d9c3cb239fa24bed2781bcf2898f153
5e353d1d17720c0f7c93f763e3565b3f
5f1c7f267fbe12210d3c80944f840332
5f393838220a6bf0cd9fd59c7cf97f5b
5f771966ef530ee0c2b42ef5cc46ad3a
6034ff91b376d653dc30f79664915b4e
603935efa89d93ea39b4b4d4a52ec529
607ea06890a6eedd723f629133576f20
60b2ce5ef4a076d1fa8675b584c27987
60cff7381b8fb64602816f9e5858930b
614909c72fa811ae41ea3d9b70122cee
6372d578e881abf76a4ec61e7a28da7d
63bf28f5dc6925a94c8b4e033a95be10
646cbeb4233948560ac50de555ea85ca

56a9ff904b78644dee6ef5b27985f441
56b18ba219c8868a5a7b354d60429368
56d6d3aa1297c62c6b0f84e5339a6c22
57849bb3949b73e2cd309900adafc853
5826e0bd3cd907cb24c1c392b42152ca
5875dfe9a15dd558ef51f269dcc407b5
58e7fd4530a212b05481f004e82f7bc1
5957ef4b609ab309ea2f17f03eb78b2d
5984955cbc41b1172ae3a688ab0246c5
59ce71ffb298a5748c3115bc834335bf
5a8d488819f2072caed31ead6aeaf2fc
5acac898428f6d20f6f085d79d86db9c
5b2cddac9ebd7b0cd3f3d3ac15026ffb
6f6d12da9e5cf8b4a7f26e53cc8e9fbd
700d2582ccb35713b7d1272aa7cfc598
70206725df8da51f26d6362e21d8fadb
70e0052d1a2828c3da5ae3c90bc969ea
7204c1f6f1f4698ac99c6350f4611391
72a7fd2b3d1b829a9f01db312fdd1cd7
7327993142260cee445b846a12cf4e85
7525bc47e2828464ce07fa8a0db6844f
76adaa87f429111646a27c2e60bda61e
76c5dca8dc9b1241b8c9a376abab0cc5
782202b09f72b3cfdc93ffb096ca27de
7836c4a36cc66d4bcbd84abb25857d21
78a0af31a5c7e4aee0f9acde74547207
7969dc3c87a3d5e672b05ff2fe93f710
7a09bf329b0b311cc552405a38747445
7a63ea3f49a96fa0b53a84e59f005019
7b3f959ab775032a3ca317ebb52189c4
7b710f9731ad3d6e265ae67df2758d50
7bd10b5c8de94e195b7da7b64af1f229
7c036ba51a3818ddc8d51cf5a6673da4
7c49efe027e489134ec317d54de42def
7d63f39fb0100a51ba6d8553ef4f34de
7ef6802fc9652d880a1f3eaf944ce4a3
7f7d726ea2ed049ab3980e5e5cb278a3
7fe679c2450c5572a45772a96b15fcb1
83076104ae977d850d1e015704e5730a
8361b151c51a7ad032ad20cecf7316f4
838ceb02081ac27de43da56bec20fc76
84865f8f1a2255561175ab12d090da7c
64db8e54d9a2daaa6d9cf156a8b73c18
675fe822243dfd1c3ace2a071d0aa6dd
67dbecfb5e0f2f729e57d0f1eda82c67
685cbba8cf2584a3378d82dec65aa0bb
693a4c2fcaa67fb87e62f150fb65e00e
6ad33ab8b9ff3f02964a8aab2a40ebb5
6b540be7ac7159104b0ffa536747f1bf
6b7276e4aa7a1e50735d2f6923b40de4
6b930be55ed4bf8e16b30eadc3873dfd
6c67f275d50f6bfee4848de6d4911931
6c9cfada134ede220b75087c7698ebf2
6e843ef4856336fe3ef4ed27a4c792b1
6e97bf1b7c44edc66622b43e81105779
86e50d6dc28283dbd295079252787577
870fbad5b9a54cb6720c122d1fa321ec
88b3b94574ba1eeb711a66eb04021eed
8956a045306b672d3cc852419a72c4b0
8a9ac1b3ef2bf63c2ddfadbbbfd456b5
8b3b96327fbddebefe727ac2edad5714
8baa499b3e2f081ff47f8cf06a5e7809
8bc20fcd09adb7ea86dda2c57477633b
8be0c21b6ee56d0f68e0d90f7d0a26d7
8c80dd97c37525927c1e549cb59bcbf3
8d2416d9f6926fb0dc12ab5dafef691d
8d74922b2b31354ce588cefac71d9a9b
8e8fb7632c3a7e96cf0ea5299d564018
8ee6c9e1adb71b2623d5e7aa45df5f4d
8efaa987959ef95179a0f5be05c10faf
8fbf53f77c98daba277dae7661b86f02
8fc825df73977eeffaaa1587565f7505
90a3e3a2049c6eb9e39d113d9451a83f
932d355d9f2df2e8d8449d85454fc983
9450980a4413dfdbc60a62b257a7b019
947892152b8419a2dfe498be5063c1da
94d42ff06a588587131c2cd8a9b2fe96
95c15b7961e2d6fad96defa7ff2c6272
96ba4bf00d8b4acee9f550286610dcc7
97004f1962e2aed917dc2be5c908278f
972077c1bb73ca78b7cad4ac6d56c669
991ebcd03ace627093acc860fae739b5
99949240bc4eae33cac4bbb93b72349d
9a0a8048d53dedc763992fff32584741

8520062de440b75f65217ff2509120f7
85862c262c087dd4470bb3b055ef8ea5
85e5b11d79a7570c73d3aa96e5a4e84d
85ecef9ca15e25835a9300a85f9bcd2a
9d3fd2ff608e79101b09db9e361ea845
9d5206f692577d583b93f1c3378a7a90
9e592d0918c029aa49635f03947026e8
9f847b3618b31ef05aebd81332067bd8
9fdd77dc358843af3d7b3f796580c29d
a025881cd4ae65fab39081f897dc04fd
a0e3561633bdf674b294094ffa06a362
a13715be3d6cbd92ed830a654d086305
a2256f050d865c4335161f823b681c24
a26e600652c33dd054731b4693bf5b01
a2c66a75211e05b20b86dd90ba534792
a2cb95be941b94f5488eab6c2eec7805
a320510258668504ed0140e7b58ee31e
a34db95c0fcb78d9c5452f81254224eb
a3c0151e0b6289376f383630a8014722
a42a91354d605165d2c1283b6b330539
a4711b8414445d211826b4da3f39de0a
a4a70ce528f64521c3cd98dce841f6f3
a5ac89845910862cfef708b20acd0e44
a67fcb5dcfc9e3cfbfd7890e65d4f808
a68bf5fce22e7f1d6f999b7a580ae477
a6b9bbb87eb08168fc92271f69fa5825
a6cab9f2e928d71ed8ecf2c28f03a9a2
a7e4f42ad70ddd380281985302573491
a83b1aed22de71baee82e426842eeb48
a91dca76278cf4f4155eb1b0fc427727
a96dca187c3c001cad13440c3f7e77e8
aa73e7056443f1dd02480a22b48bdd46
aaafb1eeee552b0b676a5c6297cfc426
ab662cee6419327de86897029a619aeb
ab8f72562d02156273618d1f3746855c
abdb86d8b58b7394be841e0a4da9bec7
ace585625de8b3942cc3974cf476f8de
beea0da01409b73be94b8a3ef01c4503
befc121916f9df7363fead1c8554df9a
bf250a8c0c9a820cd1a21e3425acfe37
bfb0dcd9ef6ac6e016a8a5314d4ef637
bff56d7e963ea28176b0bcb60033635d
9a0e3e80cd7c21812de81224f646715e
9a61ed5721cf4586abd1d49e0da55350
9b26999182ea0c2b2cac91919697289e
9c656ce22c93ca31c81ff8378a0a91ee
ace620a0cc2684347e372f7e40e245d5
ad3b9e45192ec7c8085c3588cacb9c58
adb4f6ecb67732b7567486f0cee6e525
afa03ddb9fc64a795aadb6516c3bc268
b0269263ce024fc9de19f8f30bd51188
b04e895827c24070eb7082611ab79676
b059c9946ff67c62c074d6d15f356f6e
b07299a907a4732d14da32b417c08af3
b1dadfcf459f8447b9ec44d8767da36d
b2f1d2fefe9287f3261223b4b8219d03
b36f3e12cb88499f8795b8740ae67057
b4204f08c1a29fd4434e28b6219bfbc6
b4878c233d7f776a407f55a27b5effbc
b6c12d88eeb910784d75a5e4df954001
b7ab5c6926f738dbe8d3a05cb4a1b4f5
b80dcd50e27b85d9a44fc4f55ff0a728
b8a61b1fda80f95a7dcdb0137bc89f67
b9642c1b3dbcccc9d84371b3163d43e0
b9647f389978f588d977ef6ef863938f
b977bed98ae869a9bb9bf725215ef8e5
b9b627c470de997c01fdef4511029219
ba629216db6cf7c0c720054b0c9a13f3
badf0957c668d9f186fb218485d0d0f6
bb165b815e09fe95fa9282bce850528d
bbfb478770a911cf055b8dfd8dcb36e4
bc4c189e590053d2cf97569c495c9610
bc9089c39bcdb1c3ef2e5bd25c77ed68
bd42303e7c38486df2899b0ccf3ce8f7
bd452dc2f9490a44bcff8478d875af4b
bd6031dd85a578edf0bf1560caf36e02
bd63832e090819ea531d1a030fb04e9b
be39ff1ec88a1429939c411113b26c02
be88741844bf7c47f81271270abe82dc
ce26e91fc13ccb1be4b6bf6f55165410
ce449d7cb0a11b53b0513dde3bd57b1c
ceba742bccb23304cf05d6c565dc53f8
cebe44b8a9a2d6e15a03d40d9e98e0ed
cf946bc0faecb2dc8e8edc9e6ce2858f

c05e5bc5adb803b8a53cff7f95621c73
c0ad63a680fbdc75d54b270cbedb4739
c0d9f3a67a8df0ed737ceb9e15bacc47
c112456341a1c5519e7039ce0ba960fa
c161f10fccecec67c589cdd24a05f880
c183e7319f07ccc591954068e15095db
c2e023b46024873573db658d7977e216
c380675a29f47dba0b1401c7f8e149dc
c3996bf709cad38d58907da523992e3b
c583ae5235ddea207ac11fff4af82d9b
c71f125fb385fed2561f3870b4593f18
c75a2b191da91114ceea80638bc54030
c78ee46ffbe5dd76d84fb6a74bf21474
c79b27fe1440b11a99a5611c9d6c6a78
c808d2ed8bb6b2e3c06c907a01b73d06
c8930a4fd33dcf18923d5cf0835272bd
c8940976a63366f39cfcdc099701093b
c89e8f0bc93d472a4f863a5fa7037286
c8a850a027fa4a3cdae7f87cc1c71ba0
cab21cb7ba1c45a926b96a38b0bdaaef
cbe63b9c0c9ac6e8c0f5b357df737c5e
cbfc1587f89f15a62f049e9e16cccf68
cd049c2b76c73510ae70610fd1042267
cd058dd28822c72360bc9950a6c56c45
cd427b4afea8032c77e907917608148a
cd81267e9c82d24a9f40739fa6bf1772
cdc22f7913eb93d77d629e59ac2dc46a
cdc585a1fd677da07163875cd0807402
e0b7e6c17339945bba43b8992a143485
e119a70f50132ae3afba3995fdf1aca6
e1512a0bf924c5a2b258ec24e593645a
e195d22652b01a98259818cfbab98d33
e1ab3358b5356adefaffbc15bc43a3f9
e1b840bbf5b54aeb19e6396cab8f4c6a
e26a29c0fc11cfb92936ab3374730b79
e284c25c50ba59d07a4fa947dc1a914a
e3867f6e964a29134c9ea2b63713f786
e3eb703ef415659f711b6bc5604e131e
e498718fd286aca7bb78858f4636f2db
e4d2c63a73a0f1c6b5e60bde81ac0289
e5478fb5e8d56334d19d43cae7f9224a
e5f7efcee5b15cf95a070a5cd05dbda9
d09fcd9fa9ed43c9f28bcd4bd4487d22
d0b5c11ee5df0d78bdde3fdc45eaf21d
d0d8243943053256bc1196e45fbf92d2
d0efc042ba4a6b207cf8f5b6760799d8
d20d01038e6ea10a9dcc72a88db5e048
d31596fe58ca278be1bb46e2a0203b34
d3df8c426572a85f3afa46e4cd2b66cd
d59a77a8da7bec1f4bad7054a41b3232
d76b1c624e9227131a2791957955dddc
d79477c9c688a8623930f4235c7228f6
d8a483d21504e73f0ba4b30bc01125d3
da46994fee26782605842005aabcd2fe
daa232882b74d60443dfec8742401808
dab45ac39e34cfee60dcb005c3d5a668
dbc583d6d5ec8f7f0c702b209af975e2
dbe92b105f474efc4a0540673da0eb9c
dbee8be5265a9879b61853cd9c0e4759
dc15ca49b39d1d17b22ec7580d32d905
dc386102060f7df285e9498f320f10e0
dd43cd0eddbb6f7cb69b1f469c37ec35
dd4e0f997e0b2cc9df28dca63ded6816
ddbdc6a3801906de598531b5b2dac02a
dde4ff4e41f86426051f15da48667f5f
ddecce92a712327c4068fabf0e1a7ff1
de608439f2bcc097b001d352b427bb68
deeb9b4789ac002aa8b834da76e70d74
df6475642f1fe122df3d7292217f1cff
e011784958e7a00ec99b8f2320e92bf4
ec4cdc752c2ecd0d9f97491cc646a269
edb648f6c3c2431b5b6788037c1cd8ef
ee3e297abd0a5b943dce46f33f3d56fb
ee4862bc4916fc22f219e1120bea734a
ef14448bf97f49a2322d4c79e64bb60b
ef2738889e9d041826d5c938a256bc45
ef6fcdd1b55adf8ad6bcdf3d93fd109e
efb5499492f08c1f10fecdeb703514d5
f0098aab593b65d980061a2df3a35c21
f073de9c169c8fcb2de5b811bff51cee
f0881d5a7f75389deba3eff3f4df09ac
f172ad4e906d97ed8f071896fc6789dc
f2b6bffa2c22420c0b1c848b673055ed
f446d8808a14649bddcc412f9e754890

e6348ee5beb9c581eeeaf4e076c5d631
e637f47c4f17c01a68539fcfcc4bc44f
e63fbc864b7911be296c8ee0798f6527
e68f9b39caf116fb108ccb5c9c4ce709
e6a757114c0940b6d63c6a5925ade27f
e6adc73df12092012f8cd246ba619f90
e8881037f684190d5f6cc26aab93d40f
e890fa6fd8a98fec7812d60f65bf1762
e8bc927ee0ae288609e1c37665a3314e
e8e73156316df88dee28214fb203658b
e957c36c9d69d6a8256b6ddf7f806f56
e9ce9b35e2386bf442e22a49243a647e
eadcae9ecba1097571c8d08e9b1c1a9c
eb06648b43d34f20fc1c40e509521e99
eb5e5db77540516e6400a7912ad0ef0d
eb5e999753f5ea094d59bdae0c66901c
eb5ee94048730b321e35394a0fb10a5d
eb64867dc48f757f0afe05dbf605b72d
eb88f415336f0dccedfc93405330c561
fae03ff044d6bb488e1a6f1c6428c510
fc2142bd72bd520338f776146903be67
fc9b8262905a80cc5381d520813d556d
fccd3de1df131f9d74949d69426c24af
fcd912fd7ed80e2cdf905873c6ced4ad
ff804e266a83974775814870cc49b66b
f4dbe32f3505bc17364e2b125f8dd6df
f4dd628f6c0bc2472d29c796ee38bf46
f4e67343e13c37449ada7335b9c53dd1
f53e332b0a6dbe8d8d3177e93b70cb1e
f5ae03de0ad60f5b17b82f2cd68402fe
f5ce889a1fa751b8fd726994cdb8f97e
f5fdbfce1a5d2c000c266f4cd180a78d
f7202dea71cc638e0c2dbeb92c2ce279
f7cef381c4ee3704fc8216f00f87552a
f7ffbbbc68aadcbfbace55c58b6da0a7
f8b91554d221fe8ef4a4040e9516f919
f906571d719828f0f4b6212fc2aa7705
f9155052a43832061357c23de873ff9f
f9abacc459e5d50d8582e8c660752c4e
f9f608407d551f49d632bd6bd5bd7a56
f9fc9359dc5d1d0ac754b12efb795f79
fa27742b87747e64c8cb0d54aa70ef98
fa3c8d91ef4a8b245033ddb9aa3054a2
fad93907d5587eb9e0d8ebc78a5e19c2

Contact Information

To report suspicious or criminal activity related to information found in this Joint Cybersecurity Advisory, contact your local FBI field office at www.fbi.gov/contact-us/field, or the FBI's 24/7 Cyber Watch (CyWatch) at (855) 292-3937 or by email at CyWatch@fbi.gov. When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact. To request incident response resources or technical assistance related to these threats, contact CISA at CISAServiceDesk@cisa.dhs.gov.

References

Revisions

July 19, 2021: Initial version

Updated July 19, 2021: Added note and STIX file

Please share your thoughts.

We recently updated our anonymous product survey; we'd welcome your feedback.