Newly identified StrongPity operations

cybersecurity.att.com/blogs/labs-research/newly-identified-strongpity-operations

Summary

Alien Labs has identified an unreported and ongoing malware campaign, which we attribute with high confidence to the adversary publicly reported as “StrongPity”. Based on compilation times, infrastructure, and public distribution of samples - we assess the campaign operated from the second half of 2018 into today (July 2019).

This post details new malware and new infrastructure which is used to control compromised machines. We have also identified StrongPity deploying malicious versions of the WinBox router management software, WinRAR, and other trusted software to compromise targets.

Background

StrongPity was first publicly reported on in October 2016 with details on attacks against users in Belgium and Italy in mid-2016. In this campaign, StrongPity used watering holes to deliver malicious versions of WinRAR and TrueCrypt file encryption software. Microsoft released an intelligence report in December 2016 which details the PROMETHIUM adversary group and its links to the Kaspersky StrongPity blog. In the report, Microsoft details how PROMETHIUM (StrongPity) has been active since at least 2012 and made use of CVE-2016-4117 during 2016 operations.

In December 2017, ESET publicly reported on a campaign in which users attempting to download a variety of legitimate software were rerouted to downloading StrongPity malware, which seeks out documents and folders from the victims.

On March 2018, The Citizen Lab publicly reported on activity against users in Turkey and Syria which redirected a large number of users to download malicious StrongPity versions of legitimate software. Cylance followed up in October 2018 with a blog post containing new intelligence on the adversary as they were shifting, likley in response to previous reporting, and attempting to evade detection and continue operations.

Technical details

In early July 2019 Alien Labs began identifying new samples resembling StrongPity. The new malware samples have been unreported and generally appear to have been created and deployed to targets following a toolset rebuild in response to the above public reporting during the fourth quarter of 2018. Based on compilation times, infrastructure build and use, and public distribution of samples, we assess the below activity continues to operate successfully as of this report.

One sample identified is a malicious installer for WinBox. WinBox is a utility that allows administration of Mikrotik RouterOS using a simple GUI. The malicious version of the software installs StrongPity malware without any obvious signs to the victim, and then operates as if it were a standard unaltered version of the trusted software:

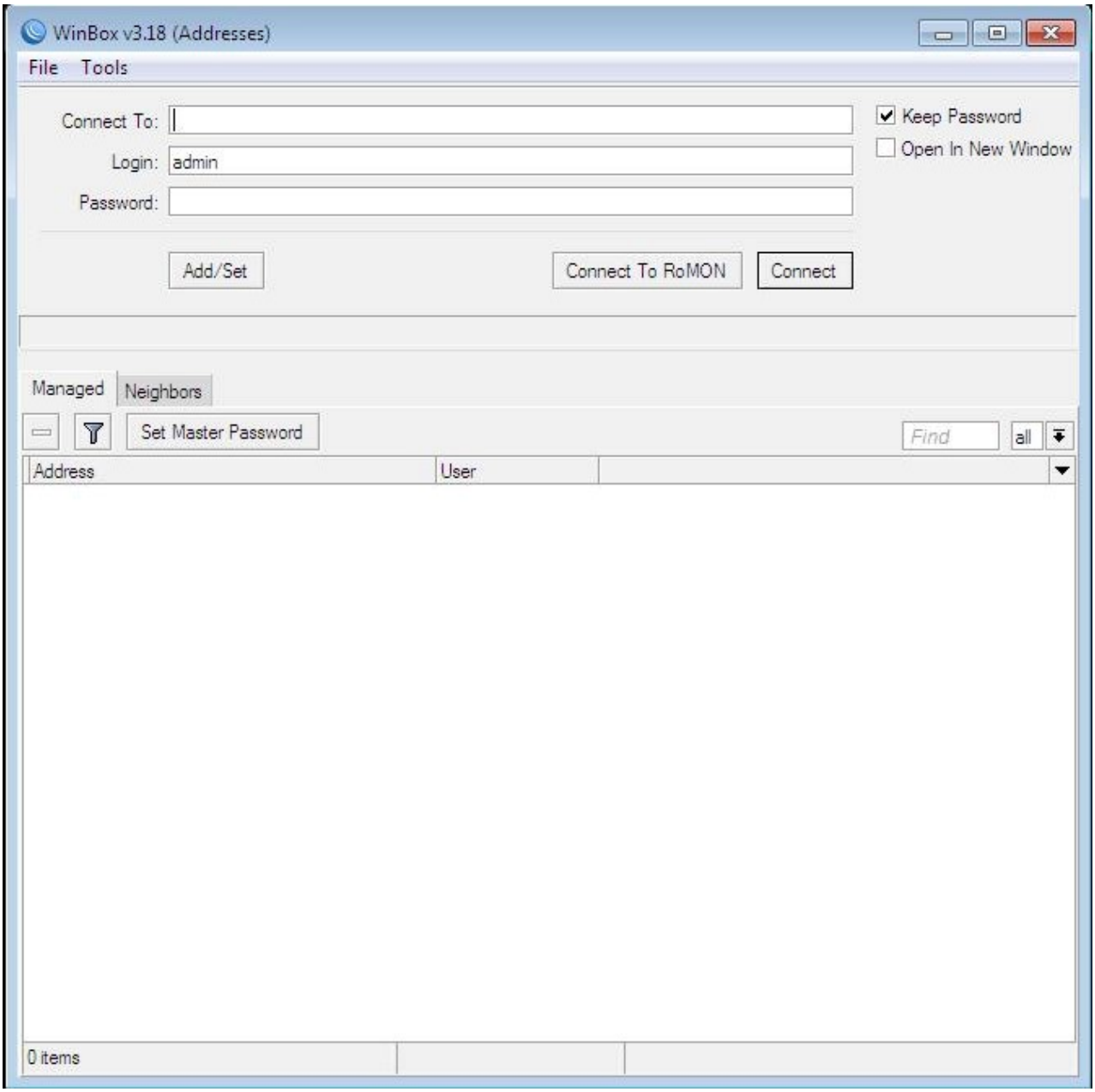


Figure 1: GUI of malicious WinBox software shown after install.

The malware generally operates in a similar fashion to previous reports of StrongPity. With complete spyware capability, the malware seeks out stored documents and retains the ability for further remote access. The malicious WinBox installer drops the StrongPity sample into the Windows Temporary directory as %temp%\DDF5-CC44CDB42E5\wintcsr.exe. Similar to previous reports of StrongPity, the malware communicates with the C2 server over SSL.

In this sample, the victim will beacon to https://srv-cdn3-system[.]com/p5pss34gvx21pxo0bz25vlqu.php. It is noteworthy to mention the /p5pss34gvx21pxo0bz25vlqu.php beacon destination continues to be the adversary choice even though it was previously publicly reported. We have also identified the URI of /goN9Z2In7mYQmN92dzX11CQL.php in addition to previously reported campaigns using kU2QLsNB6TzexJv5vGdunVXT.php and p55C3xhxTuD5rkBQbB8wE99Q.php.

Reviewing the compilation timestamps of the identified malware, various clusters of individual campaign start times can be noticed, stretching back into the previous reports of early 2018

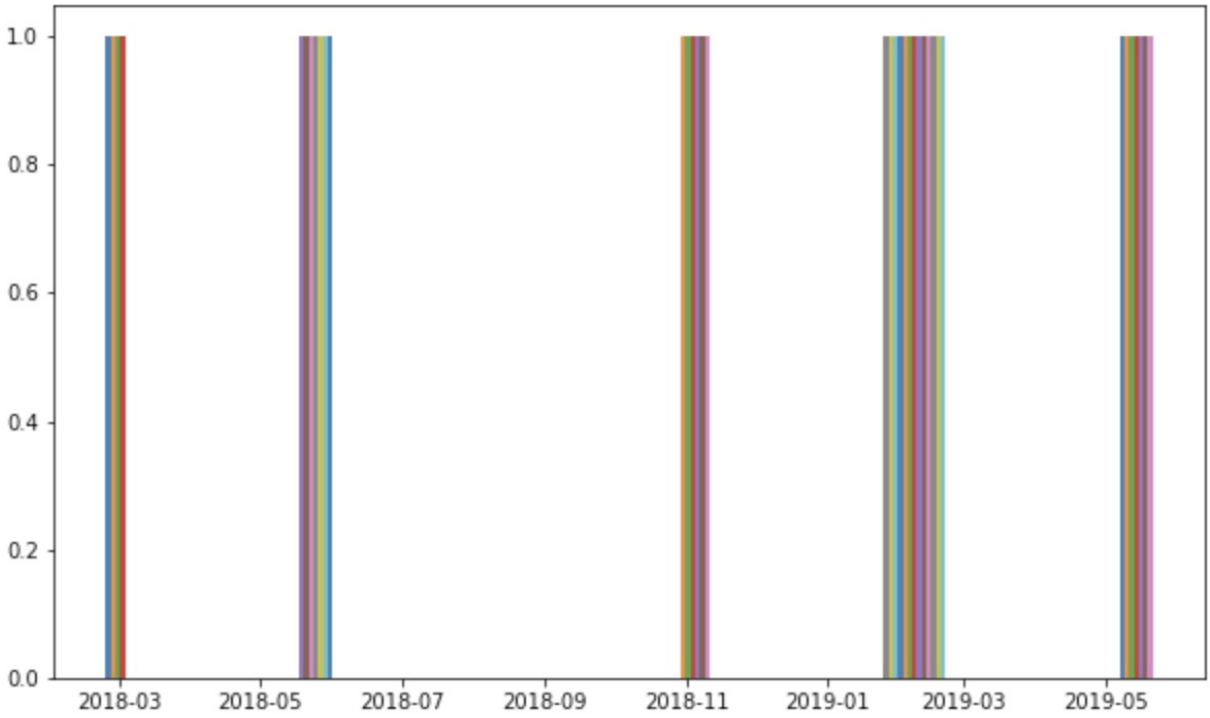


Figure 2: Compilation times of identified StrongPity malware.

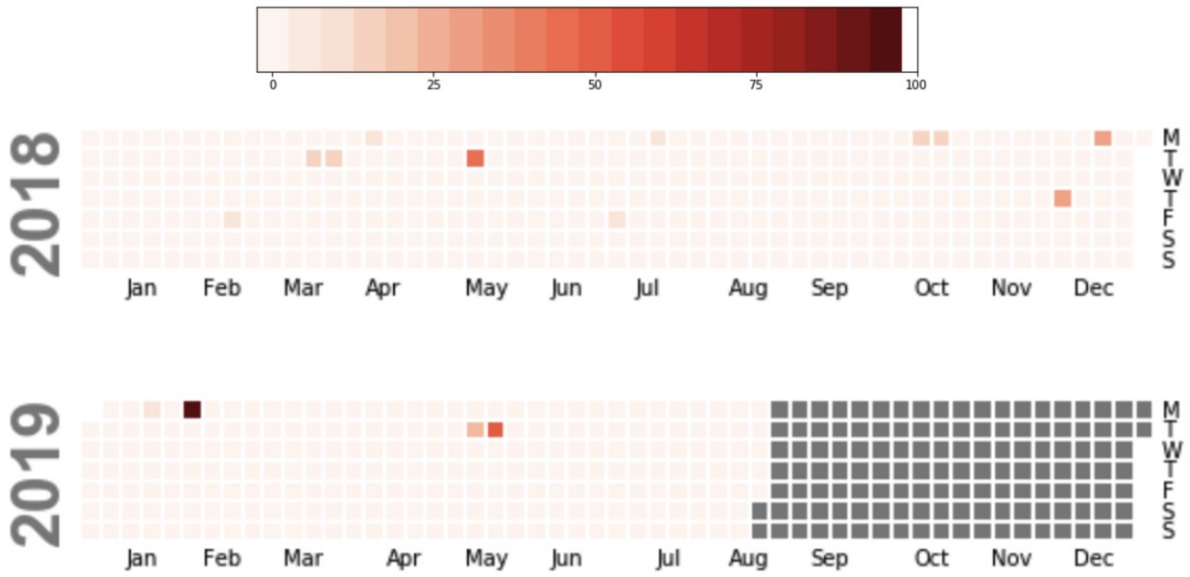


Figure 3: Timeline of PE complication times and C2 domain registration.

We have observed a variety of other software used as installers for StrongPity as well. For example, newer versions WinRAR and a tool called Internet Download Manager (IDM) which maliciously installs StrongPity and communicates with related adversary infrastructure:

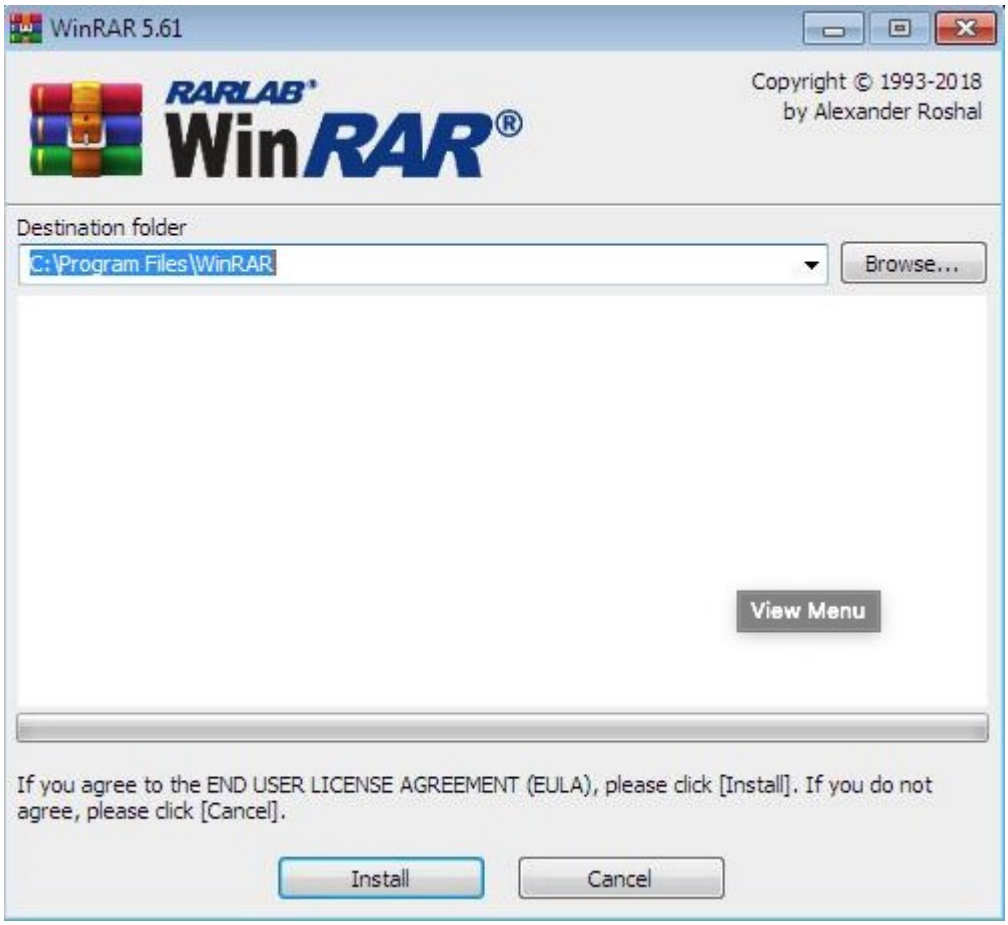


Figure 4: A sample of malicious WinRAR Installer GUI.

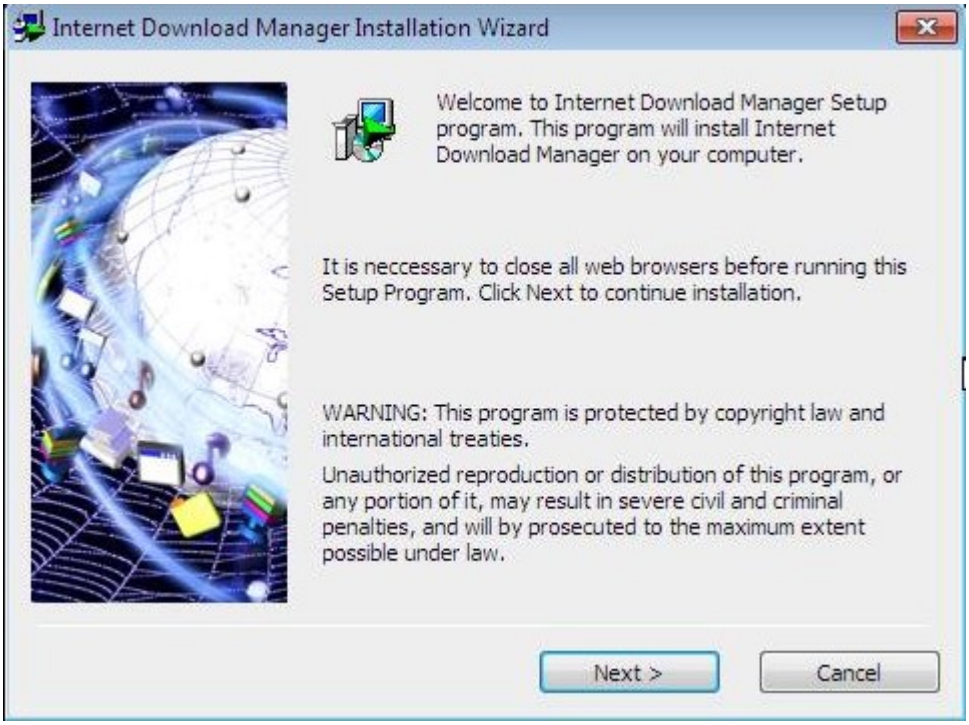


Figure 5: A sample of malicious IDM Installer GUI.

As of this report we are unable to confirm the specifics around delivery of the malicious installers. However it is likely that methods previously documented by the previous reports of StrongPity, such as regional download redirecting from ISPs, is still occuring. Based on the type of software used as the installer (WinRAR, WinBox, IDM, etc.), the type of targets may continue to be technically-oriented, again similar to past reports.

A potential insight into the adversary can be gained from reviewing the compilation hours of the large collection of malware samples. Based on this report's findings, all samples fit into a standard eight hour workday between 7AM UTC and 3PM UTC.

Overall, the identified TTPs, newer versions of StrongPity, and the legitimate software used to deliver it operate in ways similar to how the adversary has historically operated. This is likely due to the high amounts of operational success for the adversary with minimal modification to evade detection following public reporting over the years.

Indicators of Compromise

A complete list of indicators is available in the from the OTX pulse.

A list of unique PE certificate serial numbers and issuers by count, followed by a list of confirmed hashes and domains can be found below.

Type	String	Fre-quency

Serial	5a:df:10:5e:7f:2c:e3:9d:45:b3:af:ea:ba:30:5c:59	6
Serial	6a:8b:4a:2c:ca:28:91:8c:4e:e7:b8:46:b4:55:64:9d	12
Issuer	/C=AC/ST=Ascention/L=Ascention/O=FG/OU=IT/CN=FG/emailAddress=fg@fg.mail.com	2
Issuer	/C=AD/ST=Andorra/L=Andorra/O=AxSoft/OU=IT/CN=AtSoft/emailAddress=atsoft@atsoft.com	2
Issuer	/C=AX/ST=Mariehamn/L=Mariehamn/O=IER/OU=IT/CN=IER/emailAddress=ier@ier.com	1
Issuer	/C=NR/ST=NR/L=Yaren/O=Web Dev. Corp./OU=IT./CN=Web Dev. Corp/emailAddress=webdevcorp@webdevcorp.com	1
Issuer	/C=SV/ST=San Salvador/L=San Salvador/O=MKSoft/OU=IT/CN=MKSoft/emailAddress=mksoft@mksoft.com	1
Issuer	/emailAddress=contact@digestsecurity.com/C=ZD/ST=W/L=NY/O=DGS Software/OU=IT/CN=Digest	6
Issuer	/emailAddress=info@itlights.com/C=BJ/ST=PortoNovo/L=PortoNovo/O=IT Lights/OU=IT/CN=IT Lights	12

Type	IOC
SHA256	6dd0b3a09ea27e8bb346f58784e2858ec43843ff76e25291c4c877b427cc71d7
SHA256	d77901484e91445d8d11b82ff487b9e56b48930fe3086e5858ea754e9f490c1f
SHA256	9cd7b03de50ae5902794efdfd62775f37674af4b02ee1f6336e9cca637faa7e3
SHA256	df4f0530c1f60796a7555a35b567341b104b79f19d90027fb6675aa245aa7a56
SHA256	f694f02ee26d544ad41f543ecd166bd71d02b3723b8a5ee515a9c2944a667971

SHA256	6424307ea25f1889e4b9fb8a64d860e42681cddf71a5a70af7963ab282225c8d
SHA256	8e3993583cd2506ccbac4b247949d-dee7d6971432576a0f9c485f9f0942054ae
SHA256	89fb07c40277ce147a66648dece08e39d-da19c150c0965809293d1d6d8cb7184
SHA256	01359609dd66117fd9e8c1804cf6615f58ac199053525db1dc606dc63acc7736
SHA256	d40a3503a960663187a83f560e94563cd11606a610a4b176b0ac065af037f175
SHA256	0de13f1d74dda01de51794c0b559eb528c972e6dcb18fe873207275940cc16b3
SHA256	a97702b25fea7863bff4a1f37b5e5a4733f2772f9e0cb55e73956acaddf53ab1
SHA256	7c195b85528b3ed75672fbcea0d32a2f45d541cf8c71e855b03d6266a8facdc0
SHA256	645c3ae40a8572fc18ba5808e000dbd52fb1ffff679c044c497189abbcc5c549
SHA256	2a7898573bd8be121eda249e7521efd2d599354d51fabae7edafef9d60dae8b1
SHA256	64a448ee194fe58c8c212faa4fbe737f8088ef387cc4551a0f1d86e9d4bdab02
SHA256	d63533b-b200525a0a88a68c592c8d4f534fcf83b0acf8ec6be24b7059b0352ae
SHA256	123ddaeefd339fcaddecab0be8a5910bf4b8d76b6ab7f78c178f9fe433fc36d4
SHA256	6b0a28fe1954ae41e17ffd6b83a2ac7112cc98b64ba6b2a05448d200b42bb2dc
SHA256	79f02a935266a6a8322dec44c7007f7a148d4327f99b3251cba23625de5d5d5e
SHA256	3f4b3a29133dd95c6815cf6f13ca015abd8f444b884f2f74a011530b814a400e
SHA256	bd49847b4d4023f7e6df079eca96e95543d2aac853fd60a62eb-b10d400f520db

SHA256	35f03cb2dbc71b0450a8eeea0f379e22e2371cc78f956a8d98fa75a576ab5638
SHA256	b3d73538b2b207a0547fe7fa443caa1da9cd20559a1439c5fd7effadcfcabe9e
SHA256	6f0b9fdc7edf43a9d1262263320e623a7e2b349f54185491262fe5184413222f
SHA256	79fd60840ebcd513b33028d8bafc778e9ed86a15f5932fe16482cc3135de73a9
SHA256	586fc08567a69f4abbafd05c98be469dfaaa9b93eaccc5043dcf22d2b666bf63
SHA256	904d237729d99a5eacc6b9721ed6d4914f303131cc855ead-12b21b0b9c8d3332
SHA256	ef0be37db67bd4ac97d695c9c043a30119df798c43e7dfbc299b3890bb5c694f
SHA256	7ae0aa490bad2fa152cd097caaaebfcef7a393a74e886a02b22109b38a4d9fc4
SHA256	c94e52455826c63a8800e6a66d72db467e1266f3b06aab-baad14c0d7463ee266
SHA256	821c643002e1eed1a5bc7cb3d15be6df5f7a4b9cb4c938d0008827a3c-c29b0b0
SHA256	bd21bf716c3bdff02f1eebae207a1a4e07c5a7f11565b3c3aabff9d925330dcf
SHA256	b93ccc818024a91b20e595b2db9157df33a64ae12a18192bb0bf1350e76daa7b
SHA256	c00c6d8052bdc047089b2d4827c3f07d88025263bb47e79fb591d-c39eaed275d
SHA256	e8e2f7538530b6ea3f4726b13bf76c4e0696cdaf1a0547294b447c21df1c594d
SHA256	0c30d15d2d8e1ce4bc3afca9ec87250dc75ee8620483884f7063f793ea766078
SHA256	fd85f006ea35f4f781568b98258e19c7455d58fccb3a673fb7c35d9bddf51c9a
SHA256	13811cb738fa74172f668251cb41dd1a4abf6fad78ed037b1e931916ee8aa9c2

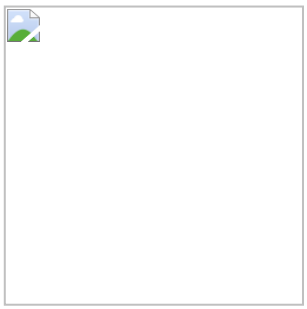
SHA256	a2ae773a283b19aef30588b56708df81748eb99ab0df00f2c0423088c07b7-ca3
SHA256	a2035a826d94a0d9e63cb90f80acffd03caff3db6b73bf4e03fa84eddd8806b0
SHA256	aa1b7dde6e7ddc3d159cb80990998da66ca6d44ed51c4b42cdef59e0b68-fad05
SHA256	d1357a1c418edc769dd125d026324a890faa5f1050f3f59c80ecb29291217cc5
SHA256	a4377256776becf75f0f61874cfec3729e17e894f5c9fc1576321f0398142878
SHA256	44ba0bfe401a07f4570fd3ca26f5955350ac831a21326face55465f8d9a7ec52
SHA256	05f41ba0a7c163f57707e8c82602ecd280f37225b5ca0a9f3ca6b6452b43fda8
SHA256	05be705bfc38c5daff3e1050d3b1424127f3eb555e185cf0bc93cc4a36fe306f
SHA256	b98a6b29b953745ce720eac71359af843e35a26bad0e37672d-d9b176e5988a67
SHA256	a60455d7cc8c1fae39b4aed818c57afcf6c37244424acf75c860c90e2044dd9d
SHA256	a17509f34fb2cbea23f444768563cbe0670ede83eda50900b197915eafbe5a83
SHA256	0205b7c1f74ca5708a56807bd5ffcb7a73e91b502d5eb514e28aa52cd53c54fc
SHA256	bbd0c42035cf1218e877139c9f36a5745ea5f325b5edb7a9917d4d9b665e652d
SHA256	d2426af686785808b956450388c6be912a2402d074d6c9d5786f49e-fae66c5d7
SHA256	68f5819687e8f410dea315f32cd04e33ca7c3ec62e9bb9bae9e03b5ded29970e
SHA256	c2c020dc44cf10072bc37f2912c970d7e74707ea0fe7612ce989ce2564a0dc4f
SHA256	ba6f004480ba615ded016729bc6209305cff9ba4c84849344f27df3faff9c554

SHA256	9d3f80ea72f6ca8397218a8fa7e92c08f44ee318c8028f7d13e455695b697a55
SHA256	d912445a5e8beda7e842756fd6e598d91ef0526c913a6f1e6135957f19fa64ca
SHA256	0ef8e41eb0123c582cb6545f84241103bb8b920b8456f95e8699e7fb6d239f9d
SHA256	d2b000fcc074ec493c0bb197c1366124ac05ef1da220e173573c863700cf8ff8
SHA256	89046ce710d44655584e8ca9c712b210627de9bb34a7456d5240c8f686ab-faac
SHA256	8ae1481a38c97008ba5ac7eafb6e18d7658d28746e4adf2f49c5e0030d1fc48d
SHA256	6684c2348d205962d41977b2db6263733809b635cd-c039447373c34e04d6bc20
SHA256	db3398c3c78f52164266cbd06959e00dc556cfbd7599c7a80fbd3fdce02ee46e
SHA256	81ee5ff2194be02bf0e6a089df7cc19ea4c74ee4ac58eae239e9f932ec5b45e1
SHA256	db3398c3c78f52164266cbd06959e00dc556cfbd7599c7a80fbd3fdce02ee46e
SHA256	81ee5ff2194be02bf0e6a089df7cc19ea4c74ee4ac58eae239e9f932ec5b45e1
SHA256	689e307438d19f7a3470f03f277221e0ff5cb76bc53721c44863fbd1d821cd70
SHA256	a34d525492d589e8d37f63134fd-cec9371404d996d78c09025a76ae0806e38d1
Domain	cdn2-svr-state[.]com
Domain	apn-state-upd2[.]com
Domain	app-mx3-delivery[.]com
Domain	cdn2-state-upd[.]com

Domain	oem-sec4-mx32[.]com
Domain	srv-cdn3-system[.]com
Domain	srv5-upd51-mx3-sec22[.]com
Domain	svr-sec2-system[.]com
Domain	sys4-upload2-srv[.]com
Domain	system6-mxe-ups3[.]com
Domain	upd-network-ms2[.]com
Domain	upd-secure-srv1[.]com
Domain	upd2-app-state[.]com
Domain	upd56-state3-cdn7-mx8[.]com
Domain - Lower Confidence	upd-ncx4-server[.]com
Domain - Lower Confidence	cdn4-rxe3-map[.]com
Domain - Lower Confidence	upd3-srv-system-app[.]com
Domain - Lower Confidence	mx-upd2-cdn-state[.]com

Domain - Lower Confi-dence	upn-sec3-msd[.]com

About the Author: Tom Hegel



Tom is a Security Researcher at Alien Labs, a part of AT&T Cybersecurity. He can be found on LinkedIn and Twitter.

Read more posts from Tom Hegel ›