Threat Roundup for Feb. 22 to March 1

By Joe Marshall

Published: 2019-03-01 · Archived: 2026-04-05 19:22:57 UTC

Friday, March 1, 2019 12:16

Today, Talos is publishing a glimpse into the most prevalent threats we've observed between Feb. 22 and March 01. As with previous roundups, this post isn't meant to be an in-depth analysis. Instead, this post will summarize the threats we've observed by highlighting key behavioral characteristics, indicators of compromise, and discussing how our customers are automatically protected from these threats.

As a reminder, the information provided for the following threats in this post is non-exhaustive and current as of the date of publication. Additionally, please keep in mind that IOC searching is only one part of threat hunting. Spotting a single IOC does not necessarily indicate maliciousness. Detection and coverage for the following threats is subject to updates, pending additional threat or vulnerability analysis. For the most current information, please refer to your Firepower Management Center, Snort.org, or ClamAV.net.

For each threat described below, this blog post only lists 25 of the associated file hashes. An accompanying JSON file can be found here that includes the complete list of file hashes, as well as all other IOCs from this post. As always, please remember that all IOCs contained in this document are indicators, and one single IOC does not indicated maliciousness.

The most prevalent threats highlighted in this roundup are:

- **Win.Malware.Bladabindi-6872031-8**
  Malware
  njRAT, also known as Bladabindi, is a remote access trojan (RAT) that allows attackers to execute commands on the infected host, log keystrokes and remotely turn on the victim's webcam and microphone. njRAT was developed by the Sparclyheason group. Some of the largest attacks using this malware date back to 2014.
- **Win.Malware.Vbtrojan-6871444-0**
  Malware
  This is a malicious tool used to exploit Visual Basic 5.
- **Win.Malware.Ekstak-6871246-0**
  Malware
  This malware persists with SYSTEM privileges by installing itself as a new service called "localNETService."
- **Win.Trojan.Zbot-6871232-0**
  Trojan
  Zbot, also known as Zeus, is trojan that steals information such as banking credentials using a variety of methods, including key-logging and form-grabbing.

- **Win.Trojan.Bifrost-6871028-0**
  Trojan
  Bifrost is a backdoor with more than 10 variants. Bifrost uses the typical server, server builder, and client backdoor program configuration to allow a remote attacker, who uses the client, to execute arbitrary code on the compromised machine. Bifrost contains standard RAT features including a file manager, screen capture utility, keylogging, video recording, microphone and camera monitoring, and a process manager. In order to mark its presence in the system, Bifrost uses a mutex that may be named "Bif1234," or "Tr0gBot."
- **Doc.Malware.Emotet-6866090-1**
  Malware
  Emotet is one of the most widely distributed and active malware families today. It is a highly modular threat that can deliver a wide variety of payloads. Emotet is commonly delivered via Microsoft Office documents with macros, sent as attachments on malicious emails.

Threats

Win.Malware.Bladabindi-6872031-8

Indicators of Compromise
Registry Keys

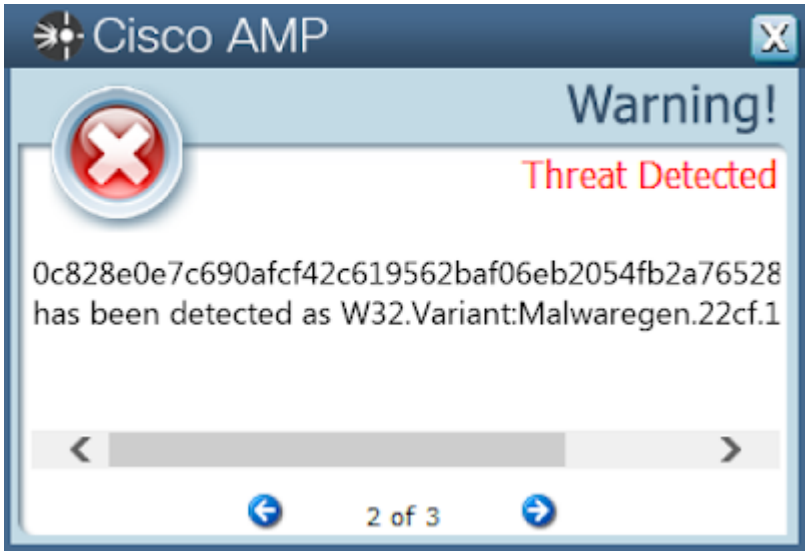
- <HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN
- Value Name: internat.exe
- <HKLM>\System\CurrentControlSet\Services\NapAgent\Shas
- <HKLM>\System\CurrentControlSet\Services\NapAgent\Qecs
- <HKCU>\Software\Microsoft\Windows\CurrentVersion\Explorer\StartPage2
- <HKLM>\System\CurrentControlSet\Services\NapAgent\LocalConfig
- <HKLM>\SYSTEM\CONTROLSET001\SERVICES\NAPAGENT\LOCALCONFIG\Enroll\HcsGroups
- <HKLM>\SYSTEM\CONTROLSET001\SERVICES\NAPAGENT\LOCALCONFIG\UI
- <HKCU>\Software\76cbed672042da4827cdb3dabad9650b
- <HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN
- Value Name: 76cbed672042da4827cdb3dabad9650b
- <HKLM>\SOFTWARE\WOW6432NODE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN
- Value Name: 76cbed672042da4827cdb3dabad9650b **Mutexes**
- N/A **IP Addresses** contacted by malware. Does not indicate maliciousness
- 75[.]115[.]14[.]18 **Domain Names** contacted by malware. Does not indicate maliciousness
- aaasssddd[.]ddns[.]net **Files and or directories created**
- %AppData%\Microsoft\Windows\Start Menu\Programs\Startup\548909871980771980909080791 8.exe
- %LocalAppData%\Temp\rat.exe
- %AppData%\Microsoft\Windows\Start Menu\Programs\Startup\76cbed672042da4827cdb3dabad9650b.exe
- %SystemDrive%\Documents and Settings\Administrator\Start Menu\Programs\Startup\548909871980771980909080791 8.exe **File Hashes**

- 00c1545a8341307c8fbfbe10315ddd6742ff0a7471e959a25569456e901e3b64
- 0c828e0e7c690afcf42c619562baf06eb2054fb2a76528c6e3d6374e6deee1b7
- 17dc39add1ec5e7823521ef2b19f5a38525a20fd8af022f3f984b9b2c52fabcd
- 23be58294c82887a32eddf964f9aa636092ab0199bbeebbc01027dac24ac741d
- 2ee7564a6f0efbeb49e5e18a9bc922c9dee4b6a9825b442eab6c24b1e5c178d8
- 36ac1e4bdb49d9a8e344daedded3f7135e5529b9170448ac640ad9887ec7cc3c
- 3c49af04461bcf44feff0a1476d4c2aa0e8727589c5bcdd94ff61801dc606cd2
- 3e6dc73e416087dff822e7b1155dacd150f8f55e522a0ea2c669ffb070b7349b
- 4011bacd5f28a2ea3d6f5cb8aa6f903a11d724de952efb43fec2c4dc6290b1c0
- 56f7759b5a937d04cc3b52b4776002621b1cbb4cca2a8c03e9a663dd0685bddc
- 5710aca5b05ba6e9936dbbb64f09f634bd0d7aabafa805bc1e898af204bc842e
- 5a8894812ad5ffb8786ece426c56316907d57cf690991eaf1f36ba31abcd8f1d
- 5ef1459ea87c9092b343f92cae360bdde926b0d160e46fa0202bb2575d4bb16b
- 6440a66af66551ca6997993e14acca0c00cf7d608b189e62ce9621cf66db371f
- 64dba074080613d0d1950f4edda64830a5aa5c94dc4170de00b90470b925fcdc
- 673f48756e3692c5bb50c1e4b73973eace36e1b4e1f23925864d570508efd1ab
- aa491525b45991154405aa5382b354494d69d24130bc61c96f02b2b13598d2e7
- b44fa6d7da5bc0dccd76440f17ed79b0accd7229f7f380ebfad498ef4bab71de
- e0bec776e2059e85dbae9ccead0ad5404f7ff1be4e44fec99fc1905ea9d82dd5
- fbe3e1d761cc96909caa72abc3443dd15236adb17091abdac00fde2044554496

Coverage

Product	Protection
AMP	✓
Cloudlock	N/A
CWS	✓
Email Security	✓
Network Security	✓
Threat Grid	✓
Umbrella	N/A
WSA	✓

Screenshots of Detection AMP



ThreatGrid

	Title	Categories	Tags	Hits	Score
+	njRAT Trojan Mutex Detected	rat	backdoor, RAT, mutex, registry, njRAT	1	100
+	Artifact Flagged Malicious by Antivirus Service	antivirus	file, antivirus	4	95
+	User Directory FireWall Exception	weakening	file, trojan, artifact, compound	1	95
+	Registry Persistence Mechanism Refers to an Executable in a Temporary Folder	persistence	process, autorun, registry, compound	2	90
+	Machine Learning Model Identified Executable Artifact as Likely Malicious	antivirus	cognitive, antivirus, machine learning	4	81
+	Sample Launched Copy Of Itself	pattern	evasion, persistence	1	71
+	Netsh.exe Used to Alter Windows Firewall	information	process, firewall, bypass, networking	1	70
+	Netsh.exe Used to Add Program to Firewall Allowed Program List	information	process, firewall, bypass, networking	1	70
+	Process Modified an Executable File	dynamic-anomaly	executable, file, process, PE	2	60
+	Process Created an Executable in a User Directory	creation	executable, file, process, PE	2	57
+	Process Modified File in a User Directory	dynamic-anomaly	executable, file, process	2	56
+	Process Modified Autorun Registry Key Value	persistence	process, autorun, registry	3	48
+	Process Created a File in the Windows Start Menu Folder	persistence	startup, file, folder, process, autorun	1	40
+	Potential Code Injection Detected	code-injection	memory	163	25

Win.Malware.Vbtrojan-6871444-0

Indicators of Compromise

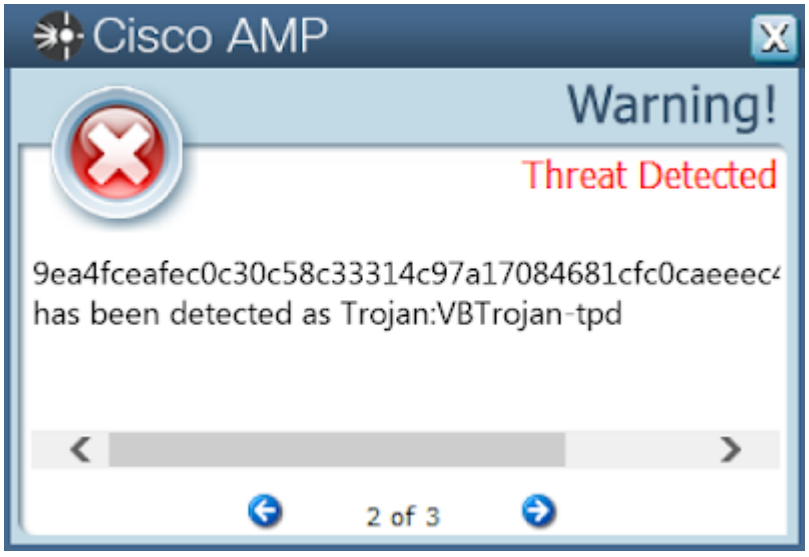
Registry Keys

- N/A **Mutexes**
- N/A **IP Addresses** contacted by malware. Does not indicate maliciousness
- N/A **Domain Names** contacted by malware. Does not indicate maliciousness
- N/A **Files and or directories created**
- %LocalAppData%\Temp\Ahk2Exe.tmp
- %LocalAppData%\Temp\AutoHotkeySC.bin
- %LocalAppData%\Temp\dnfahk.tmp
- %LocalAppData%\Temp\upx.exe
- %SystemDrive%\ReadMe.txt
- %SystemDrive%\SetInterval.bat
- %SystemDrive%\keyboard.reg **File Hashes**
- 050f57560e1691e7b09ccd86e92ec1c2c4ac361ba09862697ad908d6dfa93090
- 2d2358fa90431448800c75dce6080b7c6132fcb574a3a0ef7eff8d6d90808ec7
- 38eb2684819f7ae15b5b66bfabf0a123ff7af22dca1f014d52e8de8f88011cc6
- 39ef144fefb739ea1ff1582e9c3da0f42566855c6769f9ed4c2d7f9427edf717
- 4113c20eefdb7e002a631e2216e26b80c654f3e77f80908049176ccc7c105db3
- 707c28b3f66d708609d8f31b506dade16aad80b157582abbcb90aa1352513160
- 78bb2e2c086a0252e83307667178ed3e5d64a73dfcef3b82b05f4c64e4496009
- 7b670e0cfa7367552b892ff42a79c2a79f80d91511f6a34f01dc1250ffe2a538
- 7da38b9e6dbe8e58d688fe1488505275d54749bf063cf35cba4b151f0bfab0c7
- 9ea4fceafec0c30c58c33314c97a17084681cfc0caeeec45eead64d3a94f2ba7
- a82ae00d8c84291c08a8edf86a8ca60bdca351ad94dd06135414636312b64809
- cfdea8ab0d2f4b82bf9d103b053b8a10eb456bd7e7896f29bed3d1f3649d2001
- dae4d4b71a86a15defa8f63fe3ef28e11436069d6869092b3b23fd0f95f465dd
- e3bd392d634b990676115698db9344201480c0cf6fd27bfaa6247f0728d41625
- e698f2b3d4b2d0b9544592ae05270bedfdedbdd01d356cb6bab740791f5b0263
- f0c556af8fab1d03cdd7592d0dfd999233555a0e7622b54c5f2cab6fae2d95da

Coverage

Product	Protection
AMP	✓
Cloudlock	N/A
CWS	✓
Email Security	✓
Network Security	N/A
Threat Grid	✓
Umbrella	N/A
WSA	N/A

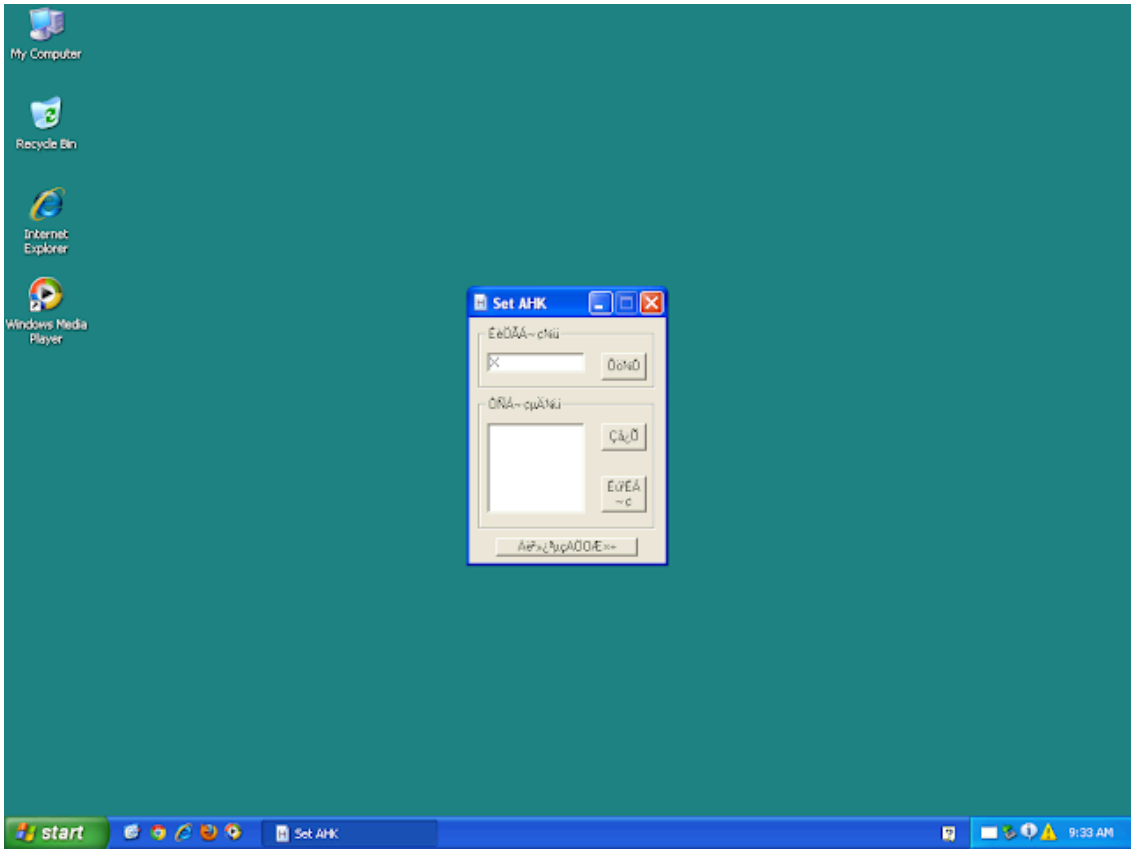
Screenshots of Detection AMP



ThreatGrid

	Title	Categories	Tags	Hits	Score
+	Artifact Flagged as Known Trojan by Antivirus	antivirus	trojan, RAT	3	95
+	Artifact Flagged Malicious by Antivirus Service	antivirus	file, antivirus	2	95
+	Artifact Flagged by Antivirus and Machine Learning Model	antivirus	cognitive, antivirus, machine learning	2	95
+	Machine Learning Model Identified Executable Artifact as Likely Malicious	antivirus	cognitive, antivirus, machine learning	2	81
+	Artifact Flagged by Antivirus	antivirus	file	6	72
+	File Name of Executable on Disk Does Not Match Original File Name	static-anomaly	file, attributes, anomaly	1	64
+	Process Modified an Executable File	dynamic-anomaly	executable, file, process, PE	1	60
+	Process Created an Executable in a User Directory	creation	executable, file, process, PE	1	57
+	Process Modified File in a User Directory	dynamic-anomaly	executable, file, process	4	56
+	Executable Artifact has Misleading File Extension	static-anomaly	PE	2	54
+	Static Analysis Flagged Artifact As Anomalous	static-anomaly	anomaly, static	5	48
+	Potential Code Injection Detected	code-injection	memory	2	25
+	Sample Created A Batch File	creation	Installation, cleanup, deletion, script, batch	1	25
+	PE Has Sections Marked Executable and Writable	static-anomaly	file, attributes, anomaly	4	24
+	Executable Artifact Uses Visual Basic	attribute	artifact, library, PE	2	21
+	Hook Procedure Detected in Executable	information	artifact, Symbol, library, keylogging, fraud,	1	14

Malware



Win.Malware.Ekstak-6871246-0

Indicators of Compromise

Registry Keys

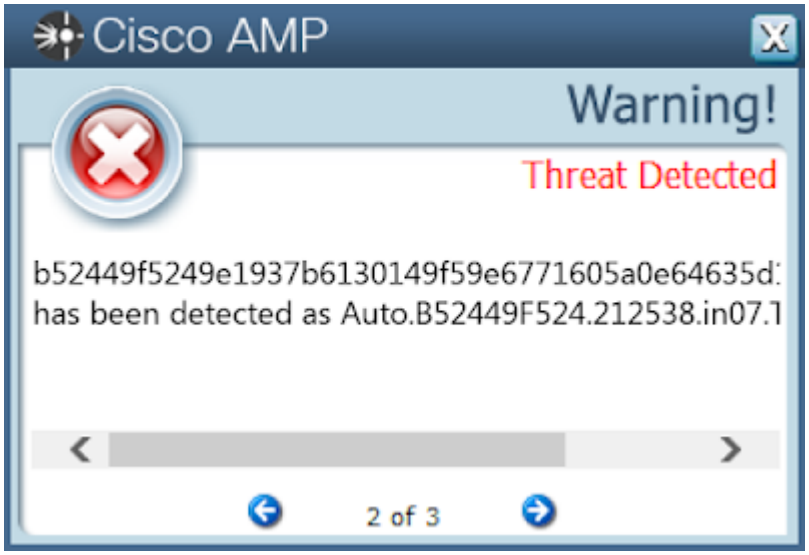
- <HKLM>\SYSTEM\CONTROLSET001\SERVICES\localNETService
- <HKLM>\SYSTEM\CONTROLSET001\SERVICES\LOCALNETSERVICE
- Value Name: Start
- <HKLM>\SYSTEM\CONTROLSET001\SERVICES\LOCALNETSERVICE
- Value Name: ImagePath
- <HKLM>\SOFTWARE\WOW6432NODE\LOCALNETSERVICE
- Value Name: Value_42632 **Mutexes**
- N/A **IP Addresses** contacted by malware. Does not indicate maliciousness
- 216[.]218[.]206[.]69 **Domain Names** contacted by malware. Does not indicate maliciousness
- N/A **Files and or directories created**
- %AllUsersProfile%\localNETService\localNETService.exe
- %LocalAppData%\Temp\tsc131118.dat **File Hashes**
- 02aebb6edf1d2ae7df3d9adca31b397c9032b6e0844a2796e0028b17c19cf345
- 055f622eae00bf5cbe062b706bbf55ff4b4d9ac0ae4ac91b0552d2b32f4ccb05
- 220a6e183611bd6730eeb2cfdd4536eca6829283566e2c0d5c410adc6552a058
- 387a3f8e33297a952ab2b93dd4f6c0a97fe797e18ead0c9cf050f0918758d1dc
- 3bd06213aae4214b81d1dd83d8d456a593122584708b86980e02f3f2e0472710
- 3bd551b75a97dda9d0aa66d9ae24fbee3e0d4dcae0b4a4aa98be994a4ec59d9f

- 5d6ce39c286eca1777a5e5bd93bd52e76ce042d0249db6ca32648611d30a5b2d
- 6073475e3a8bd7eba6a13f771a51245c929e49e40afe97c0eccf3887df18826d
- 63806671769e485496408fd6c1c4e845ef35087c74b02fb104dc06a52b90d636
- 6f0702d5a7a8a07c0f27da9850c0953634577bbfef272016d26795c40b1e95c7
- 7372e040d1d26c864f261ac7df8c7a509594c3efce26e03c3e14389e55c526bf
- 81376a8e386940982bd552e0be5fd0cbfffb9ae39bbb97280e7f6096fc4a7af1
- 81cc82b599e1cc44fd7dde9366315886f5a1c40e7cae7f4edbbcb2dd104a69e9
- 825b8e7b877bacf8d24afe1e1082eff72e43633b3a411104d624d0b66e3f8dce
- 9fbe12ce5275b09a48bd1efdd6208b7ffae37878febf82fd1805db49212578e1
- a24a1a691d04ff091d2b99970d40108726c188224dc4503b1e3a7f9a22df4ebb
- a295919ff4794ccccaf3750a5540476e6868766512d13db1a859bb64b4af59db
- b4ac2fb4da484e90e08e20db2270de2f15d6684e614d239abe2586896076a7f1
- b52449f5249e1937b6130149f59e6771605a0e64635d151ce8e2f5819c99d93c
- b5cb0d3df17907248b6d84a57279b26fa39c123c4a240b1507ae7b8233f2ec0d
- b9b0fea1d1dbc027dd27c1b4d07d5411a35cc60d43ed137d00a958a34292f4bb
- c48fbacb48492d59dac5fd7d2e9d8474e7282ca84d2605b23794e49f15229693
- c7974f414e32a93836f9e3a710251a23c4163a89cb2967bc99010c080034d9e3
- cc4bd522847f7673dcfdc37b7e330b470eacf5e9a47bd0f6d466267f5b152e3e
- d98eb303771aed9508601074db1e05dedeb028d1c09aa7313b0b15eff40f7eb7

Coverage

Product	Protection
AMP	✓
Cloudlock	N/A
CWS	✓
Email Security	✓
Network Security	✓
Threat Grid	✓
Umbrella	N/A
WSA	✓

Screenshots of Detection AMP



ThreatGrid

	Title	Categories	Tags	Hits	Score
+	Artifact Flagged Malicious by Antivirus Service	forensics	file, antivirus	3	95
+	Process Modified an Executable File	file, persistence	executable, file, process, PE	1	60
+	Static Analysis Flagged Artifact As VM Aware	forensics	vm, static	3	56
+	Potential Code Injection Detected	evasion	memory	2	25
+	Process Added a Service to the ControlSet Registry Key	persistence	registry, process	1	25
+	PE Resource Indicates Russian Origin	attribute	file, attributes	3	15
+	Executable Signed With Digital Certificate	attribute	file, attributes	9	10
+	Executable with Encrypted Sections	forensics	packer, crypter, encoding, PE	3	9
+	Executable Uses Armadillo	attribute	packer, encoding, PE	3	9

Win.Trojan.Zbot-6871232-0

Indicators of Compromise

Registry Keys

- <HKCU>\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\RUN
- Value Name: internat.exe
- <HKU>\Software\Microsoft\Internet Explorer\PhishingFilter
- <HKCU>\SOFTWARE\MICROSOFT\Qaygra
- <HKU>\Software\Microsoft\Windows\CurrentVersion\Run
- <HKU>\Software\Microsoft\Nabu **Mutexes**
- N/A **IP Addresses** contacted by malware. Does not indicate maliciousness
- 23[.]253[.]126[.]58
- 104[.]239[.]157[.]210

- 104[.]239[.]157[.]210 **Domain Names** contacted by malware. Does not indicate maliciousness
- macrshops[.]eu **Files and or directories created**
- %LocalAppData%\Temp\tmpa9735385.bat
- %AppData%\Icda
- %AppData%\Icda\ehday.exe
- %AppData%\Vyarqe\erezu.loe
- %SystemDrive%\DOCUME~1\ADMINI~1\LOCALS~1\Temp\tmp2ad79550.bat
- %AppData%\Kyba\ryisl.ubo
- %AppData%\Leve\yhqy.exe **File Hashes**
- 21a58e23e14143301c847d9f6151d024a8f38db8922e2797b2548a9b1e6b9b47
- 2531e7bbc454b8b643c5f21fbd7ed88c71aed73dc3a4fcf20815092eefeefbe7
- 2c8c8e0b5b378425b6a5d2ccff3e2274230734ffe419970a49c87c26d8d41047
- 399dad77516c27f0b2f5a36605a5fa25aff0e6a0ec66feae6854838336ee8b0d
- 3f32cdf15d079fe250d8b42a5abd58d1ff3012599f8478b074dd096bb25b537f
- 48d0fd82b8625c9c789284fc23cd0ee9cb9bb3ef96728c61de4a25ce7d6fc21c
- 5827e6c1a8a5ca100482c127b7c0402788ca4d870057eed2af089bc9d858bfb2
- 5c46b61ca41c03433e5ab3f156116e312cda1b50079189af82f1df8721e3a73b
- 739b9fec48a683f39fd924a24eaa0dcde0207cac1bcad4463223ff731f007ad3
- 9f3129449f2ece4a84ddef0b071d9721945db8fa93bb06ac6bdb3b7f0388c35c
- abc68f3b8db8e6a50c56605c2f7fb153717a7c7f96a905b527059182fbdb8688
- bde83f62cdf8f9565146e44b2796c35368f81b9a38fed73670879cff44bc2956

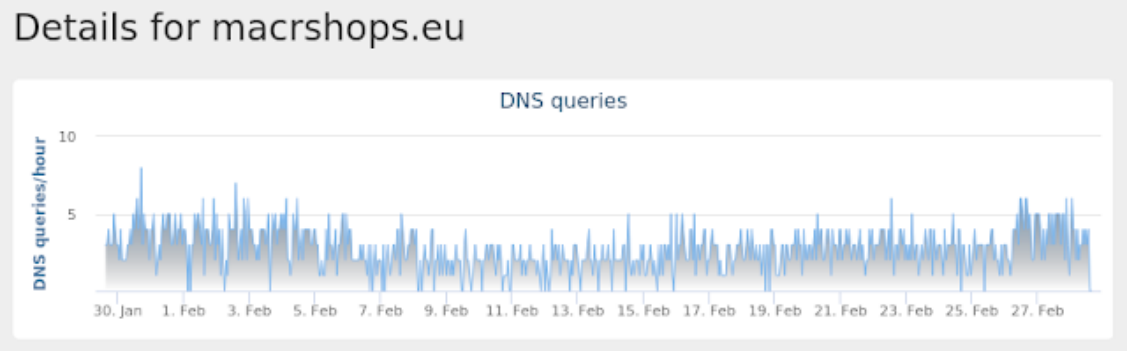
Coverage

Product	Protection
AMP	✓
Cloudlock	N/A
CWS	✓
Email Security	✓
Network Security	✓
Threat Grid	✓
Umbrella	✓
WSA	✓

Screenshots of Detection ThreatGrid

	Title	Categories	Tags	Hits	Score
+	Possible ZeuS Variant Detected by Antivirus	banker	trojan, zeus, fraud, banker, compound	2	100
+	Artifact Flagged as Known Trojan by Antivirus	antivirus	trojan, RAT	4	95
+	Artifact Flagged Malicious by Antivirus Service	antivirus	file, antivirus	2	95
+	Process Hollowing Detected	code-injection	process, hollowing, obfuscation	1	95
+	Artifact Flagged by Antivirus	antivirus	file	4	72
+	Sample Launched Copy Of Itself	pattern	evasion, persistence	1	71
+	Potential Code Injection Detected	code-injection	memory	6	25
+	PE Checksum is Invalid	static-anomaly	attributes, checksum, PE	1	25
+	Executable Artifact Uses Visual Basic	attribute	artifact, library, PE	2	21

Umbrella



Win.Trojan.Bifrost-6871028-0

Indicators of Compromise

Registry Keys

- <HKLM>\SOFTWARE\Bifrost
- <HKU>\Software\Bifrost **Mutexes**
- \BaseNamedObjects\Bif1234 **IP Addresses** contacted by malware. Does not indicate maliciousness
- 148[.]81[.]111[.]121
- 204[.]95[.]99[.]100 **Domain Names** contacted by malware. Does not indicate maliciousness
- xyinyb[.]com
- rfyeoc[.]com
- owiueu[.]com
- paredx[.]com
- qlotay[.]com
- vlocie[.]com
- wbrthv[.]com
- pozswe[.]com
- kucqey[.]com

- tnsamu[.]com
- pydquj[.]com
- lbeewo[.]com
- pkoitz[.]com
- ufhspo[.]com
- qyevsy[.]com
- qsayev[.]com
- yvmoie[.]com
- lybcri[.]com
- ypauhr[.]com
- qdhoas[.]com **Files and or directories created**
- %System32%\drivers\etc\hosts
- %ProgramFiles%\Bifrost\server.exe **File Hashes**
- 0040b9166f09670f4c3b16d247f4fbfae7aa5e989407dcf5237f05594c4c150e
- 0082f04583eabadaa51f3f4a91c82d363eef5f553973765aacc58462c9b83525
- 0ea44f69cdee613bd907dc2e4c97fc942d2f4807f28f69914514d1737709f223
- 1eb3fb26576b32630aaf3f1ae2b81140e083639608a5ff4b695ee7805a70a87a
- 2225b77359e3ad87306d38a22713167c33846488d0b091fe1a6890b3b6560979
- 230afd73943ecb538ed51a50fda07b4ba0e37ee805dab7e263e2623a2dbb4dd9
- 27d6fd04978ac887712c25756e03b14152bcc3a0649307c4d0e6fe491b68a41e
- 2bbd0c136832d5e091ecae568a017e04ab6f3757e5e1a376c4700a4117e1b94e
- 31ff3f68aa25f1200040f390297a044ab8d313ff9b1f377e23d016267d092fca
- 4cf558585a8bef563e37238f9459092c627538e2fadb99ac1dbe9f22b63eb346
- 4cfa43c370fc0a19826f19f48f60a3abba75ee4811c6df4d0313d0f0c3274f58
- 50eba44b2ee65fc0c95539b3197a10ccafca91df34717b0f48f60553f6d694ee
- 59c8baa550d491782d9b3899c2252fc8d71971b2c399a807f81b1917a4e31c65
- 5e62499136f6391316d72edb7924744f2bc289776308c89a4b3a1a0d3ae081c1
- 64ddbc85e24f4acf10ca1945110b16e2b7f0d53f68be8ca711b025ae4561dade
- 6e5a78dc6bc5435005e4b5134d41d2469d76101e561e84dc23ce8bbf80e937d5
- 778d3552da4d5b5d5586962b6f0d092c2f0b5c029ed514c13ad4f39847f771cb
- 77b9574204c60ee0eb588ae3afbdf14912634fce0aefca81ffd0822c48f3468d
- 82858882f23741cd930cff314994761b135b06d8d04cc8be09fa54567dcb94f8
- 837301f97cdc69d729ab753bf6f284a988c0ff6793fe89924e3f360f467d0fba
- 872f04d1d11643a224e8535e71139b3074aa4f98c157ade42da7c74dda4208f2
- 875b76f081746c6299421dad1963ff5f212b43b0bb6217fe6681465e06a5d2b8
- 8d72e7115a4564541d30649d2f3203306cccab27c543d58ba6267b4752c4528f
- 914a3fb08cce05e93bfd8b2e41a8202341d8b7857f73b692190477a2bd0a1797
- 9917d5deaa1b02d329454f1e08e548f750d3f0b09a0f38d55e6c94f84243ab4d

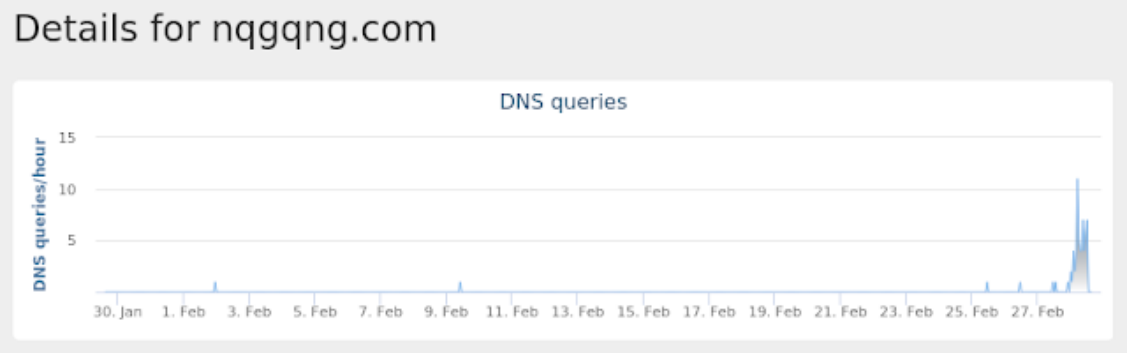
Coverage

Product	Protection
AMP	✓
Cloudlock	N/A
CWS	✓
Email Security	✓
Network Security	✓
Threat Grid	✓
Umbrella	✓
WSA	✓

Screenshots of Detection ThreatGrid

	Title	Categories	Tags	Hits	Score
+	Bifrost Default Mutex Detected	rat	trojan, host, process, lock, mutex, dropper, RAT	1	100
+	Artifact Flagged Malicious by Antivirus Service	antivirus	file, antivirus	2	95
+	Artifact Flagged as Known Trojan by Antivirus	antivirus	trojan, RAT	2	95
+	Artifact Flagged by Antivirus and Machine Learning Model	antivirus	cognitive, antivirus, machine learning	2	95
+	Process Hollowing Detected	code-injection	process, hollowing, obfuscation	1	95
+	Machine Learning Model Identified Executable Artifact as Likely Malicious	antivirus	cognitive, antivirus, machine learning	2	81
+	Artifact Flagged by Antivirus	antivirus	file	2	72
+	Sample Launched Copy Of Itself	pattern	evasion, persistence	1	71
+	Process Modified File in a User Directory	dynamic-anomaly	executable, file, process	1	56
+	Potential Code Injection Detected	code-injection	memory	7	25
+	PE Checksum is Invalid	static-anomaly	attributes, checksum, PE	1	25
+	PE Has Sections Marked Executable and Writable	static-anomaly	file, attributes, anomaly	4	24
+	Executable Artifact Uses Visual Basic	attribute	artifact, library, PE	2	21
+	Executable with Encrypted Sections	attribute	packer, crypter, encoding, PE	2	9
+	PE DOS Header Size of the Header in Paragraphs Abnormal	attribute	file, attributes, anomaly, PE	2	3

Umbrella



Doc.Malware.Emotet-6866090-1

Indicators of Compromise

Registry Keys

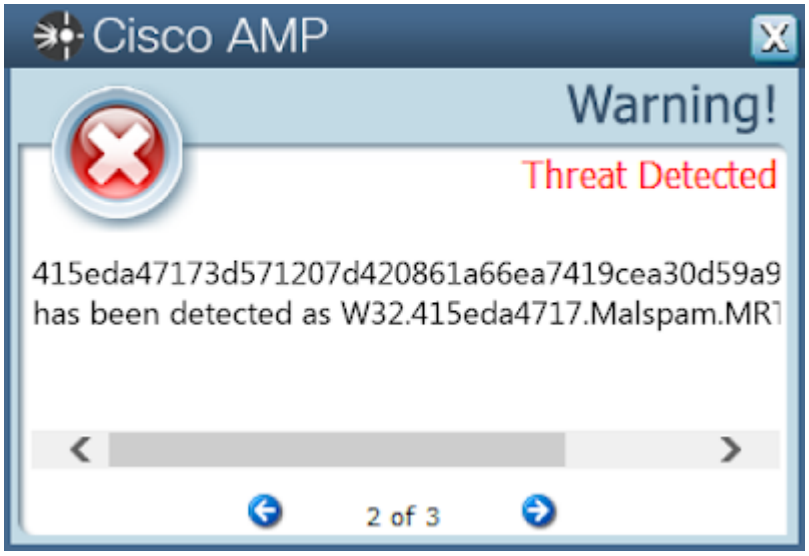
- <HKLM>\SYSTEM\CONTROLSET001\SERVICES\startedturned
- <HKLM>\SYSTEM\CONTROLSET001\SERVICES\STARTEDTURNED
- Value Name: Start
- <HKLM>\SYSTEM\CONTROLSET001\SERVICES\STARTEDTURNED
- Value Name: ImagePath **Mutexes**
- N/A **IP Addresses** contacted by malware. Does not indicate maliciousness
- 212[.]83[.]51[.]248
- 159[.]65[.]186[.]223
- 74[.]59[.]106[.]11 **Domain Names** contacted by malware. Does not indicate maliciousness
- lenkinabasta[.]com **Files and or directories created**
- %UserProfile%\880.exe
- %WinDir%\SysWOW64\d1Ltzcv.exe
- %LocalAppData%\Temp\CVR3F73.tmp
- %LocalAppData%\Temp\ysrbsuxx.yb3.ps1
- %LocalAppData%\Temp\zh5htpos.q5s.psm1 **File Hashes**
- 26bda8a7e04a3b4ba47ff57f776cb65b0ed11870bc5fa65b33353c53ab718566
- 363371e71bfd3a0f6e8e0ffe1017918d65d5afe7ce1c6d7ea26f5604b26144ce
- 3a162a09d1f8a4ee0248d72a60ff0ddbc2cef8084c3d2aed1cfb73192f628d42
- 3d48920206c69924bd3c388e2d7a48845e48ba6a525f06ae466db235deaa6832
- 415eda47173d571207d420861a66ea7419cea30d59a901f716354c8167c8373b
- 4c70e7e49082dc78f27ac863bfaf671ce823ed43575d608e309cb6e839f093ce
- 6055cf5b67690819f88a3a96685386afd8819377dd31454fab559809fc9ef6eb
- 949bd24349829221977de531f8a1dc80d401bf5e0a8fc69a1b386261b474ee43
- 9fa9d852c7f7a94a022347e7bf2325d41032163fb7ec61d362bfeb94a0ed9ee8
- ba0b908255f68bff48e58cc7d2ac0caa55e369b7a282fce5b9d58ae1df34b681
- bd1f913c5ceaf2042070666fba37fa0a8108f1e82ac19e516a7f74e9d5da5ea8
- cb83759cf47a4b6e44e5afcf6f85f64b475a6f4bbcd0bff82b31b45f048a64c9
- d523914940ef79338eeba96e8befae59574d1552f13ddff5c41500bf43d9192d
- db0478556a516ed5d8508f165251efd10fd3e68c84fda7d720730f6409af61b8

- e881930c362396744a2338740d28ac26377cf19c33b460cdac987fcb1255f804

Coverage

Product	Protection
AMP	✓
Cloudlock	N/A
CWS	✓
Email Security	✓
Network Security	✓
Threat Grid	✓
Umbrella	✓
WSA	✓

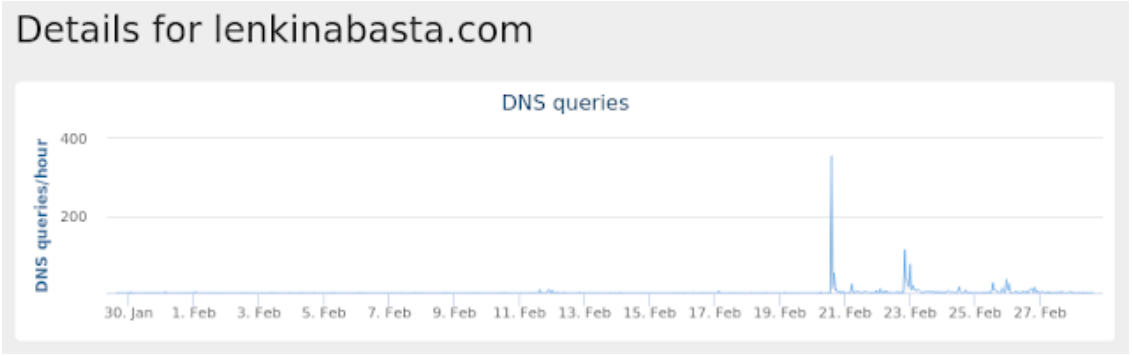
Screenshots of DetectionAMP



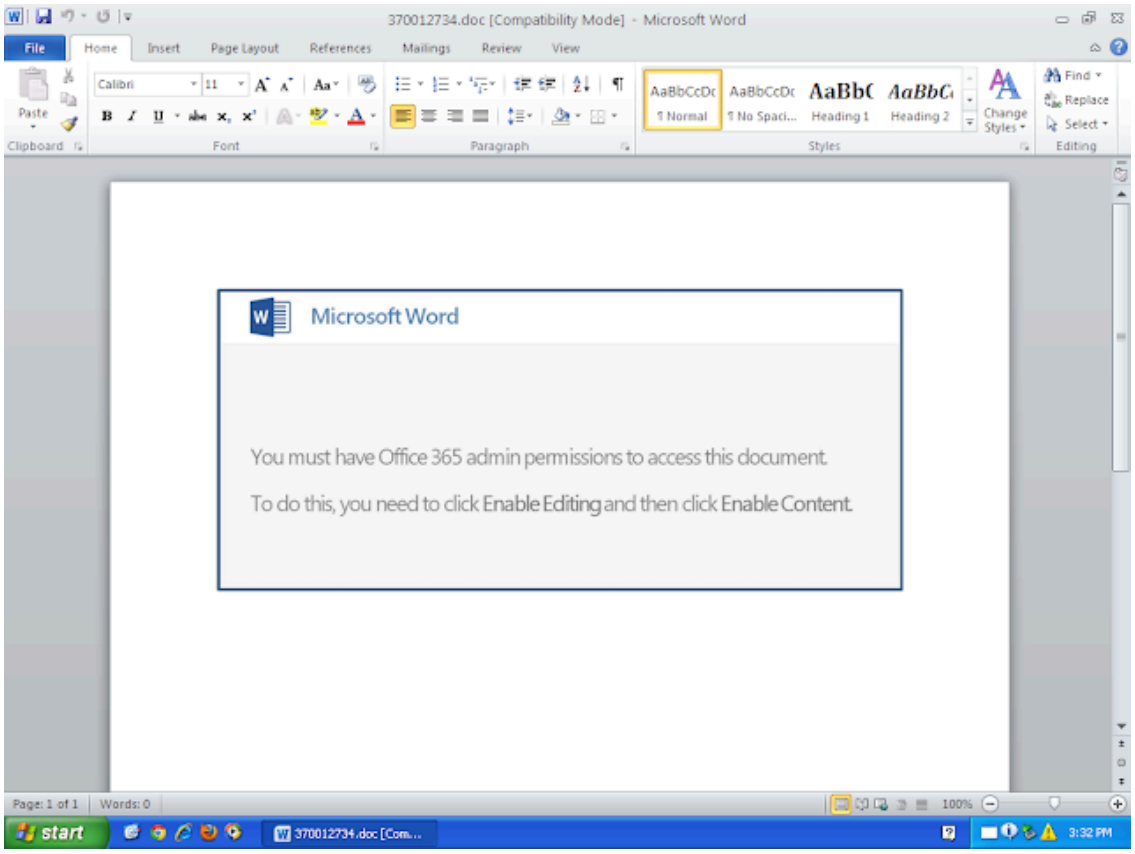
ThreatGrid

	Title	Categories	Tags	Hits	Score
+	Emotet Malware Detected	banker	trojan, banker, RAT, fraud	2	100
+	Document Created an Executable File	pattern	obfuscation, dropper, phishing	2	100
+	Office Document Launches a Powershell	pattern	obfuscation, dropper, script, phishing	1	100
+	Artifact Flagged Malicious by Antivirus Service	antivirus	file, antivirus	2	95
+	PowerShell With Encoded Command and Obfuscation	evasion	process, system, encoding, script, obfuscation	1	95
+	A Domain Flagged By Cisco Umbrella Downloaded A PE	domain	umbrella, dns, compound	1	95
+	Document Submission Contacted Domain Flagged By Cisco Umbrella	domain	umbrella, dns, compound	1	95
+	Snort Triggered On A Domain Flagged Malicious By Umbrella	network-anomaly	network, compound, snort, umbrella	2	95
+	Specific Set of Indicators Signalling Highly Suspicious Word Document	heuristic	compound, phishing, threshold	1	95
+	Document Used WMI to Launch Process	pattern	obfuscation, dropper, process, compound	1	95
+	PowerShell With Encoded Command Downloads Data	evasion	process, system, encoding, script, download	1	95
+	A Document File Established Direct IP Communications	network-anomaly	dropper	1	90
+	A Document File with Embedded and Minimal Content Established Network Communications	pattern	dropper, macro, embedded, low content,	1	90

Umbrella



Malware



Source: https://blog.talosintelligence.com/2019/03/threat-roundup-for-feb-22-to-march-1.html