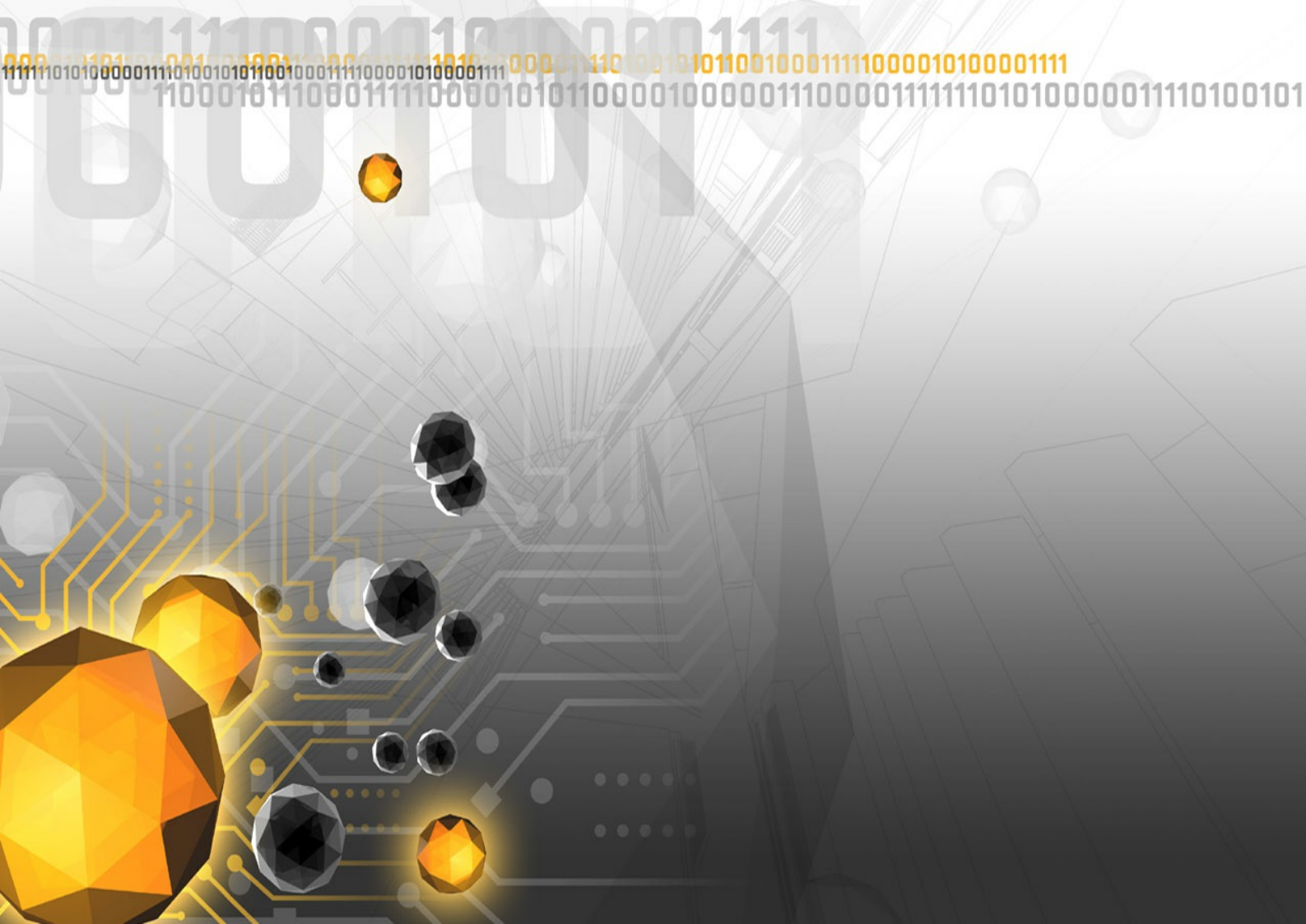
DeepSight™ INTELLIGENCE

TOOL SIMILARITIES BETWEEN OPERATION CLEAVER AND VOLATILE CEDAR CYBER ESPIONAGE GROUPS

MANAGED ADVERSARY AND THREAT INTELLIGENCE

DEEPSIGHT™ INTELLIGENCE | INTELLIGENCE REPORT | SYMC - 300145 | V.!
22 APR 2015 GMT



LEGAL NOTICE

SYMANTEC PROPRIETARY & CONFIDENTIAL - PERMITTED USE ONLY

Symantec assigns a high, medium, or low degree of confidence to assessments within its DeepSight™ Intelligence Portal Managed Adversary and Threat Intelligence (MATI) products. Confidence levels are determined against a three-point spectrum of source validity: variety and non-conflictive disparity of original sources, quality of source reporting, and reliability of source reporting. Confidence levels may be increased based on independent corroboration of information. High confidence generally suggests a solid judgment can be made, though such a judgment carries the risk of being wrong. Low confidence generally suggests tenuous inferences can be made, though information used to do so may have been questionable, fragmented, or singular.

Information Cut-Off Date: 08 Apr 2015 GMT

Tool Similarities between Operation Cleaver and Volatile Cedar Cyber Espionage Groups

DeepSight™ Intelligence | Intelligence Report | SYMC - 300145 | V.! | 22 Apr 2015 GMT

KEY FINDINGS

Symantec's analysis of the tools used by Volatile Cedar and Operation Cleaver suggests these two groups are likely using the same sources to obtain cyber espionage tools including an Iran-based cyber security company. Symantec observed the two groups use of variants of the AspxSpy webshell that contain the same Persian name, *Setareh*, in a comment. (Due to the public availability of the tools used, the similarities observed in Symantec's analysis do not substantiate formal or informal collaboration between the two groups.)

The Volatile Cedar cyber espionage campaign, active since at least November 2012, has targeted defense, telecommunications, and educational organizations in 10 different countries including the United States, Canada, United Kingdom, Turkey, Lebanon, and Israel.

Symantec expects to see ongoing similarities between the tools and tactics used by the Volatile Cedar and Operation Cleaver groups. Organizations should remain aware of developments in the tools and tactics used by Iran-based cyber espionage groups such as Operation Cleaver, as they may be similar to future tools and tactics employed by the Volatile Cedar group.

EXECUTIVE SUMMARY

Symantec's analysis of the tools used by Volatile Cedar and Operation Cleaver suggest the two cyber espionage groups are likely using the same sources to obtain tools. (Note: The public availability of the tools used by both groups makes this link insufficient to suggest formal or informal collaboration between the two groups.)

The Volatile Cedar cyber espionage campaign, active since at least November 2012, has targeted organizations in the United States, Canada, United Kingdom, Turkey, Lebanon, and Israel in the defense, telecommunications, and education industries. The Volatile Cedar group uses a variety of webshells, backdoors, and a custom implant called Explosive, which Symantec detects as Trojan.Explod, Trojan.Explod!g1, Trojan.Explod!g2, and Trojan.Explod!g3. The Volatile Cedar group takes advantage of vulnerabilities in public web servers as an initial intrusion vector.

Symantec expects to see continued similarities between the tools and tactics used by the Volatile Cedar and Operation Cleaver groups. Organizations should remain aware of developments in the tools and tactics used by Iran-based cyber espionage groups, as they may be similar to future tools and tactics employed by Volatile Cedar.

DETAILS

Symantec's analysis focused on the similarities in the tools used in the recent Volatile Cedar cyber espionage campaign and those used in Operation Cleaver activities.

Volatile Cedar Cyber Espionage Campaign

The Volatile Cedar cyber espionage campaign, described in a 30 March 2015 technical report by an Israel-based cyber security company, has been actively targeting organizations in the United States, Canada, United Kingdom, Turkey, Lebanon, and Israel in the defense, telecommunications, and education industries since at least November 2012. The report describes the Volatile Cedar group's activities, which are aligned with the political interests of Lebanon and characterized by the use of custom implants and a variety of commodity malware tools and webshells including the AspxSpy and caterpillar webshells.

In the 30 March 2015 report, the Israel-based cyber security company originally named the custom implant used by the group as the "Explosive implant." Symantec detects the Explosive implant as Trojan.Explod, Trojan.Explod!g1, Trojan.Explod!g2, and Trojan.Explod!g3. The Explosive implant contains a keylogger, clipboard logger, memory monitor, and functionality to ensure the activity and security of the command-and-control connection. Actors using the Explosive implant can obtain information on Internet Explorer browsing history, saved passwords, registry values, running processes, and folder contents, as well as access the command line.

Use of Tools Linked to Operation Cleaver Cyber Activity

Symantec's analysis of the tools used by Volatile Cedar and Operation Cleaver suggest the two cyber espionage groups are likely using the same sources to obtain tools. Because the tools identified are available in open sources, the similarities in tool choices are not definitive indications of formal or informal collaboration between the two groups.

Both cyber espionage groups use a non-standard AspxSpy variant containing the Persian name *Setareh* in a comment field suggesting the groups may have access to the same repository of tools that have been modified from their original forms. Furthermore, both groups have been linked to the use of backdoors developed by the Iran-based cyber security company ITSecTeam.

According to a 30 March 2015 technical report by an Israel-based cyber security company, the company links the file named 404.aspx (MD5: 40c5bf03868c12275c15dd596b8507b2), a variant of the AspxSpy webshell, to Volatile Cedar cyber operations. Symantec's analysis of the file uncovered the string *Setareh,* a Persian name that means "star" or "fate," within a comment in the file. Symantec identified the same string in an AspxSpy variant file named ide.aspx (MD5: 1df8c4f9bf04afa0345dcc8622061456); a 9 December 2014 technical report by a United States-based government agency linked the file to Iran-based Operation Cleaver cyber operations. The default AspxSpy file contained the comment *//admin*, so the modification to include *//Setareh* represents a non-standard configuration of the webshell.

According to Symantec technical research, as of 8 April 2015 a server hosting the caterpillar webshell—the most common webshell that Volatile Cedar uses according to a 30 March 2015

technical report by an Israel-based cyber security company—also contained a backdoor with attribution information for *Amin Shokahi (Pejvak) – ITSecTeam*. The file named db.php (MD5: 932a8451bbf103287651bebd1b4ce6c3) linked to Operation Cleaver cyber operations also contained a signature indicating that it was developed by the ITSecTeam.

OUTLOOK

Symantec expects to see ongoing similarities between the tools and tactics used by the Volatile Cedar and Operation Cleaver groups as the overlaps between their tool choices suggest they use the same sources for cyber espionage tools. Organizations should remain informed and enact defenses against the changing tools and tactics of Iran-based cyber espionage groups; doing so will likely improve defenses against Volatile Cedar actors based on operational similarities.

TECHNICAL DETAILS

See the ***Metadata*** tab for additional technical details related to this report.

METADATA

EXTRACTED INDICATORS

Indicator	Indicator Related CVE	Indicator Type
69.64.90.94		ip_address
50.60.129.74		ip_address
85.25.20.27		ip_address
213.204.122.130		ip_address
213.204.122.133		ip_address
184.107.97.188		ip_address
69.94.157.80		ip_address
saveweb.wink.ws		domain
carima2012.site90.com		domain
explorerdotnt.info		domain
dotnetexplorer.info		domain
dotntexplorere.info		domain
xploreredotnet.info		domain
erdotntexplore.info		domain
eb7042ad32f41c0e577b5b504c7558ea		file_md5
e2e6ed82703de21eb4c5885730ba3db42f3ddda8b94beb2ee0c3af61bc435747		file_sha256
44b5a3af895f31e22f6bc4eb66bd3eb7		file_md5
a98099541168c7f36b107e24e9c80c9125fefb787ae720799b03bb4425aba1a9		file_sha256
08c988d6cebdd55f3b123f2d9d5507a6		file_md5
b74bd5660baf67038353136978ed16dbc7d105c60c121cf64c61d8f3d31de32c		file_sha256
61b11b9e6baae4f764722a808119ed0c		file_md5
07529fae9e74be81fd302d022603d9f0796b4b9120b0d6131f75d41b979bbca5		file_sha256
c7ac6193245b76cc8cebc2835ee13532		file_md5
bdef2ddcd8d4d66a42c9cbafd5cf7d86c4c0e3ed8c45cc734742c5da2fb573f7		file_sha256
184320a057e455555e3be22e67663722		file_md5
388f5bc2f088769b361dfe8a45f0d5237c4580b287612422a03babe6994339ff		file_sha256
5d437eb2a22ec8f37139788f2087d45d		file_md5
5663b2d4a4aec55d5d6fb507e3fdcb92ffc978d411de68b084c37f86af6d2e19		file_sha256
1dcac3178a1b85d5179ce75eace04d10		file_md5
dea53e331d3b9f21354147f60902f6e132f06183ed2f4a28e67816f9cb140a90		file_sha256

Indicator	Indicator Related CVE	Indicator Type
9a5a99def615966ea05e3067057d6b37		file_md5
1952fa94b582e9af9dca596b5e51c585a78b8b1610639e3b878bbfa365e8e908		file_sha256
2b9106e8df3aa98c3654a4e0733d83e7		file_md5
03641e5632673615f23b2a8325d7355c4499a40f47b6ae094606a73c56e24ad0		file_sha256
ab3d0c748ced69557f78b7071879e50a		file_md5
3bedb4bdb17718fda1edd1a8fa4289dc61fdda598474b5648414e4565e88ecd5		file_sha256
c9a4317f1002fefcc7a250c3d76d4b01		file_md5
50414f60d7e24d25f9ebb68f99d67a46e8b12458474ac503b6e0d0562075a985		file_sha256
4f8b989bc424a39649805b5b93318295		file_md5
d8fdcdaad652c19f4f4676cd2f89ae834dbc19e2759a206044b18601875f2726		file_sha256
3f35c97e9e87472030b84ae1bc932ffc		file_md5
5d491ea5705e90c817cf0f5211c9edbcd5291fe8bd4cc69cdb58e8d0e6b6d1fe		file_sha256
7cd87c4976f1b34a0b060a23faddbd19		file_md5
fc085d9be18f3d8d7ca68fbe1d9e29abbe53e7582453f61a9cd65da06961f751		file_sha256
ea53e618432ca0c823fafc06dc60b726		file_md5
bc12d7052e6cfce8f16625ca8b88803cd4e58356eb32fe62667336d4dee708a3		file_sha256
034e4c62965f8d5dd5d5a2ce34a53ba9		file_md5
52cb02da0462fdd08d537b2c949e2e252f7a7a88354d596e9f5c9f1498d1c68f		file_sha256
5ca3ac2949022e5c77335f7e228db1d8		file_md5
30196c83a1f857d36fde160d55bd4e5b5d50fbb082bd846db295cbe0f9d35cfb		file_sha256
306d243745ba53d09353b3b722d471b8		file_md5
41dd95533d85a0fd099ee79fbb4c8699ae6f9299b74034b8bafa3b0ea4a1fb3a		file_sha256
e6f874b7629b11a2f5ed3cc2c123f8b6		file_md5
97ab07c8020aead6ce0d9196e03d3917045e65e8c65e52a16ec6ef660dd96968		file_sha256
5b505d0286378efcca4df38ed4a26c90		file_md5
bd039bb73f297062ab65f695dd6defafd146f6f233c451e5ac967a720b41fc14		file_sha256
7dbc46559efafe8ec8446b836129598c		file_md5
d0f059ba21f06021579835a55220d1e822d1233f95879ea6f7cb9d301408c821		file_sha256
1d4b0fc476b7d20f1ef590bcaa78dc5d		file_md5
1b76fdbd4cd92c7349bc99291137637614f4fb9598ae29df0a39a422611b86f8		file_sha256
66e2adf710261e925db588b5fac98ad8		file_md5
e5b68ab68b12c3eaff612ada09eb2d4c403f923cdec8a5c8fe253c6773208baf		file_sha256
tools.dll		file_name
c898aed0ab4173cc3ac7d4849d06e7fa		file_md5
37f4e9d0153221d9a236f299151c9f6911a6f78fff54c91b94ea64d1f3a8872b		file_sha256
22872f40f5aad3354bbf641fe90f2fd6		file_md5
ef47aaf4e964e1e1b7787c480e60a744550de847618510d2bf54bbc5bda57470		file_sha256

Indicator	Indicator Related CVE	Indicator Type
c19e91a91a2fa55e869c42a70da9a506		file_md5
b275c8978d18832bd3da9975d0f43cbc90e09a99718f4efaf1be7b43db46cf95		file_sha256
740c47c663f5205365ae9fb08adfb127		file_md5
bed0bec3d123e7611dc3d722813eeb197a2b8048396cef4414f29f24af3a29c4		file_sha256
edaca6fb1896a120237b2ce13f6bc3e6		file_md5
ea335556fecaf983f6f26b9788b286fbf5bd85ff403bb4a1db604496d011be29		file_sha256
d2074d6273f41c34e8ba370aa9af46ad		file_md5
0008065861f5b09195e51add72dacd3c4bbce6444711320ad349c7dab5bb97fb		file_sha256
6f11a67803e1299a22c77c8e24072b82		file_md5
d30f306d4d866a07372b94f7657a7a2b0500137fe7ef51678d0ef4249895c2c5		file_sha256
7031426fb851e93965a72902842b7c2c		file_md5
5a310669920099cd51f82bc9eb5459e9889b6357a21f7ce95ac961e053c79acb		file_sha256
981234d969a4c5e6edea50df009efedd		file_md5
bfc63b30624332f4fc2e510f95b69d18dd0241eb0d2fcd33ed2e81b7275ab488		file_sha256
29eca6286a01c0b684f7d5f0bfe0c0e6		file_md5
78201fd42dfc65e94774d8a9b87293c19044ad93edf59d3ff6846766ed4c3e2e		file_sha256
826b772c81f41505f96fc18e666b1acd		file_md5
6674ffe375f8ab54cfa2a276e4a39b414cf327e0b00733c215749e8a94385c63		file_sha256
da428bbf4f327fd2fde257630d7c507b		file_md5
e5f691e445f693a96145e6f14c3be4d15c05d7c4b1e087e1ec683ead9c35a90e		file_sha256
f38407f50905ff1c27c9bee007239983		file_md5
5953c9bf800c67b67f1a3d9691119488d3a1d6e6c6691f8a15d28436cd7122a7		file_sha256
5aadc6349663a3146cb8a323e7961e45		file_md5
d1299a5c75882de2407f50b47c8a111349d4660e5b3fb7fdedfc4cfc2ef98a91		file_sha256
70f063057b3a3131a95a34a204802156		file_md5
3becda7d601cf482d7ef236da6342239684694ed141a911601f321616440f6fa		file_sha256
8f4aa2963e2ba10e0549370af4f9c1ca		file_md5
47f45532108686fa535dbc32b5356f2005dc13c90f399170fa880ebd530f4645		file_sha256
8a520abc7998b8e5443fbacc62013526		file_md5
a616c039b0ffa2682f001a6978c5edfaac2c3f828b6b18de6bc91f4abaa2d9bb		file_sha256
cat.aspx,caterpillar.aspx		file_name
05f456529f76e4f4fa9266cbae5efc03		file_md5
2f2e794064e28a4cd6eb0c0e10d929453367c4b01a55fadf15037817c55e9cdb		file_sha256
a95a2d7cc06ca28b1f7639af3e90e025		file_md5
493007afc73a3d6573b2b53457d6c82e24e16591807565d6caf3e5b6b5d407a2		file_sha256
80ed1fc942a6b0d4f32c1ff2e45f2443		file_md5
b64d6e0e09b6daab209d14f2e684d819433605763208fbfc901a9ab7fd62ce05		file_sha256

Indicator	Indicator Related CVE	Indicator Type
6a8d62765ade6a58bcbaa295fd46c480		file_md5
c103c3c0a1d7983ca1951a72800346fad32a67b4be013a97361a3d85e0e8cd98		file_sha256
cmd.aspx		file_name
2144d75b09a61850a86e0af2e5128942		file_md5
e33118afd512762c79d840b782dd5cfa2472c97613103e60f8d5427a0a26beb3		file_sha256
dab2cbb34ec587587bdf0418f7fb06b1		file_md5
4de07466f24a26311fe011f92c8b04e7c2c3ef4df8f5853bde523404ac06c34f		file_sha256
2783cee3aac144175fef308fc768ea63		file_md5
973fbccbc6d917883d502c88cb7fadfc1a5657adbec377c7a4ed77292ebaeda9		file_sha256
f58f03121eed899290ed70f4d19af307		file_md5
ba168c69866ba2e370c9bfbfe06d5863af0e4b387ce05084928710af3c7c43ce		file_sha256
5a2338dd7d0fa0478e34b4407daabbc9		file_md5
26e64f95ee23a6ec3b9fb8f937bed8e6ea247379b1f0b2e95ef071dc113b420c		file_sha256
96b1221ba725f1aaeaaa63f63cf04092		file_md5
eb7042ad32f41c0e577b5b504c7558ea		file_md5
e2e6ed82703de21eb4c5885730ba3db42f3ddda8b94beb2ee0c3af61bc435747		file_sha256
44b5a3af895f31e22f6bc4eb66bd3eb7		file_md5
a98099541168c7f36b107e24e9c80c9125fefb787ae720799b03bb4425aba1a9		file_sha256
08c988d6cebdd55f3b123f2d9d5507a6		file_md5
b74bd5660baf67038353136978ed16dbc7d105c60c121cf64c61d8f3d31de32c		file_sha256
61b11b9e6baae4f764722a808119ed0c		file_md5
07529fae9e74be81fd302d022603d9f0796b4b9120b0d6131f75d41b979bbca5		file_sha256
c7ac6193245b76cc8cebc2835ee13532		file_md5
bdef2ddcd8d4d66a42c9cbafd5cf7d86c4c0e3ed8c45cc734742c5da2fb573f7		file_sha256
184320a057e455555e3be22e67663722		file_md5
388f5bc2f088769b361dfe8a45f0d5237c4580b287612422a03babe6994339ff		file_sha256
5d437eb2a22ec8f37139788f2087d45d		file_md5
5663b2d4a4aec55d5d6fb507e3fdcb92ffc978d411de68b084c37f86af6d2e19		file_sha256
1dcac3178a1b85d5179ce75eace04d10		file_md5
dea53e331d3b9f21354147f60902f6e132f06183ed2f4a28e67816f9cb140a90		file_sha256
9a5a99def615966ea05e3067057d6b37		file_md5
1952fa94b582e9af9dca596b5e51c585a78b8b1610639e3b878bbfa365e8e908		file_sha256
2b9106e8df3aa98c3654a4e0733d83e7		file_md5
03641e5632673615f23b2a8325d7355c4499a40f47b6ae094606a73c56e24ad0		file_sha256
ab3d0c748ced69557f78b7071879e50a		file_md5
3bedb4bdb17718fda1edd1a8fa4289dc61fdda598474b5648414e4565e88ecd5		file_sha256
c9a4317f1002fefcc7a250c3d76d4b01		file_md5

Indicator	Indicator Related CVE	Indicator Type
50414f60d7e24d25f9ebb68f99d67a46e8b12458474ac503b6e0d0562075a985		file_sha256
4f8b989bc424a39649805b5b93318295		file_md5
d8fdcdaad652c19f4f4676cd2f89ae834dbc19e2759a206044b18601875f2726		file_sha256
3f35c97e9e87472030b84ae1bc932ffc		file_md5
5d491ea5705e90c817cf0f5211c9edbcd5291fe8bd4cc69cdb58e8d0e6b6d1fe		file_sha256
7cd87c4976f1b34a0b060a23faddbd19		file_md5
fc085d9be18f3d8d7ca68fbe1d9e29abbe53e7582453f61a9cd65da06961f751		file_sha256
ea53e618432ca0c823fafc06dc60b726		file_md5
bc12d7052e6cfce8f16625ca8b88803cd4e58356eb32fe62667336d4dee708a3		file_sha256
034e4c62965f8d5dd5d5a2ce34a53ba9		file_md5
52cb02da0462fdd08d537b2c949e2e252f7a7a88354d596e9f5c9f1498d1c68f		file_sha256
5ca3ac2949022e5c77335f7e228db1d8		file_md5
30196c83a1f857d36fde160d55bd4e5b5d50fbb082bd846db295cbe0f9d35cfb		file_sha256
306d243745ba53d09353b3b722d471b8		file_md5
41dd95533d85a0fd099ee79fbb4c8699ae6f9299b74034b8bafa3b0ea4a1fb3a		file_sha256
e6f874b7629b11a2f5ed3cc2c123f8b6		file_md5
97ab07c8020aead6ce0d9196e03d3917045e65e8c65e52a16ec6ef660dd96968		file_sha256
5b505d0286378efcca4df38ed4a26c90		file_md5
bd039bb73f297062ab65f695dd6defafd146f6f233c451e5ac967a720b41fc14		file_sha256
7dbc46559efafe8ec8446b836129598c		file_md5
d0f059ba21f06021579835a55220d1e822d1233f95879ea6f7cb9d301408c821		file_sha256
1d4b0fc476b7d20f1ef590bcaa78dc5d		file_md5
1b76fdbd4cd92c7349bc99291137637614f4fb9598ae29df0a39a422611b86f8		file_sha256
66e2adf710261e925db588b5fac98ad8		file_md5
e5b68ab68b12c3eaff612ada09eb2d4c403f923cdec8a5c8fe253c6773208baf		file_sha256
tools.dll		file_name
c898aed0ab4173cc3ac7d4849d06e7fa		file_md5
37f4e9d0153221d9a236f299151c9f6911a6f78fff54c91b94ea64d1f3a8872b		file_sha256
22872f40f5aad3354bbf641fe90f2fd6		file_md5
ef47aaf4e964e1e1b7787c480e60a744550de847618510d2bf54bbc5bda57470		file_sha256
c19e91a91a2fa55e869c42a70da9a506		file_md5
b275c8978d18832bd3da9975d0f43cbc90e09a99718f4efaf1be7b43db46cf95		file_sha256
740c47c663f5205365ae9fb08adfb127		file_md5
bed0bec3d123e7611dc3d722813eeb197a2b8048396cef4414f29f24af3a29c4		file_sha256
edaca6fb1896a120237b2ce13f6bc3e6		file_md5
ea335556fecaf983f6f26b9788b286fbf5bd85ff403bb4a1db604496d011be29		file_sha256
d2074d6273f41c34e8ba370aa9af46ad		file_md5

Indicator	Indicator Related CVE	Indicator Type
0008065861f5b09195e51add72dacd3c4bbce6444711320ad349c7dab5bb97fb		file_sha256
6f11a67803e1299a22c77c8e24072b82		file_md5
d30f306d4d866a07372b94f7657a7a2b0500137fe7ef51678d0ef4249895c2c5		file_sha256
7031426fb851e93965a72902842b7c2c		file_md5
5a310669920099cd51f82bc9eb5459e9889b6357a21f7ce95ac961e053c79acb		file_sha256
981234d969a4c5e6edea50df009efedd		file_md5
bfc63b30624332f4fc2e510f95b69d18dd0241eb0d2fcd33ed2e81b7275ab488		file_sha256
29eca6286a01c0b684f7d5f0bfe0c0e6		file_md5
78201fd42dfc65e94774d8a9b87293c19044ad93edf59d3ff6846766ed4c3e2e		file_sha256
826b772c81f41505f96fc18e666b1acd		file_md5
6674ffe375f8ab54cfa2a276e4a39b414cf327e0b00733c215749e8a94385c63		file_sha256
da428bbf4f327fd2fde257630d7c507b		file_md5
e5f691e445f693a96145e6f14c3be4d15c05d7c4b1e087e1ec683ead9c35a90e		file_sha256
f38407f50905ff1c27c9bee007239983		file_md5
5953c9bf800c67b67f1a3d9691119488d3a1d6e6c6691f8a15d28436cd7122a7		file_sha256
5aadc6349663a3146cb8a323e7961e45		file_md5
d1299a5c75882de2407f50b47c8a111349d4660e5b3fb7fdedfc4cfc2ef98a91		file_sha256
70f063057b3a3131a95a34a204802156		file_md5
3becda7d601cf482d7ef236da6342239684694ed141a911601f321616440f6fa		file_sha256
8f4aa2963e2ba10e0549370af4f9c1ca		file_md5
47f45532108686fa535dbc32b5356f2005dc13c90f399170fa880ebd530f4645		file_sha256
8a520abc7998b8e5443fbacc62013526		file_md5
a616c039b0ffa2682f001a6978c5edfaac2c3f828b6b18de6bc91f4abaa2d9bb		file_sha256
cat.aspx,caterpillar.aspx		file_name
05f456529f76e4f4fa9266cbae5efc03		file_md5
2f2e794064e28a4cd6eb0c0e10d929453367c4b01a55fadf15037817c55e9cdb		file_sha256
a95a2d7cc06ca28b1f7639af3e90e025		file_md5
493007afc73a3d6573b2b53457d6c82e24e16591807565d6caf3e5b6b5d407a2		file_sha256
80ed1fc942a6b0d4f32c1ff2e45f2443		file_md5
b64d6e0e09b6daab209d14f2e684d819433605763208fbfc901a9ab7fd62ce05		file_sha256
6a8d62765ade6a58bcbaa295fd46c480		file_md5
c103c3c0a1d7983ca1951a72800346fad32a67b4be013a97361a3d85e0e8cd98		file_sha256
cmd.aspx		file_name
2144d75b09a61850a86e0af2e5128942		file_md5
e33118afd512762c79d840b782dd5cfa2472c97613103e60f8d5427a0a26beb3		file_sha256
dab2cbb34ec587587bdf0418f7fb06b1		file_md5
4de07466f24a26311fe011f92c8b04e7c2c3ef4df8f5853bde523404ac06c34f		file_sha256

Indicator	Indicator Related CVE	Indicator Type
2783cee3aac144175fef308fc768ea63		file_md5
973fbccbc6d917883d502c88cb7fadfc1a5657adbec377c7a4ed77292ebaeda9		file_sha256
f58f03121eed899290ed70f4d19af307		file_md5
ba168c69866ba2e370c9bfbfe06d5863af0e4b387ce05084928710af3c7c43ce		file_sha256
5a2338dd7d0fa0478e34b4407daabbc9		file_md5
26e64f95ee23a6ec3b9fb8f937bed8e6ea247379b1f0b2e95ef071dc113b420c		file_sha256
96b1221ba725f1aaeaaa63f63cf04092		file_md5

FILES

Detection Name	Name	MD5	SHA 256	Malicious
Trojan.Explod!g1		eb7042ad32f41c0e577b5b504c7558ea	e2e6ed82703de21eb4c5885730ba3db42f3ddda8b94beb2ee0c3af61bc435747	y
Trojan.Explod!g1		44b5a3af895f31e22f6bc4eb66bd3eb7	a98099541168c7f36b107e24e9c80c9125fefb787ae720799b03bb4425aba1a9	y
Trojan.Explod		08c988d6cebdd55f3b123f2d9d5507a6	b74bd5660baf67038353136978ed16dbc7d105c60c121cf64c61d8f3d31de32c	y
Trojan.Explod!g1		61b11b9e6baae4f764722a808119ed0c	07529fae9e74be81fd302d022603d9f0796b4b9120b0d6131f75d41b979bbca5	y
Trojan.Explod!g1		c7ac6193245b76cc8cebc2835ee13532	bdef2ddcd8d4d66a42c9cbafd5cf7d86c4c0e3ed8c45cc734742c5da2fb573f7	y
Trojan.Explod!g2		184320a057e455555e3be22e67663722	388f5bc2f088769b361dfe8a45f0d5237c4580b287612422a03babe6994339ff	y
Trojan.Explod!g2		5d437eb2a22ec8f37139788f2087d45d	5663b2d4a4aec55d5d6fb507e3fdcb92ffc978d411de68b084c37f86af6d2e19	y
Trojan.Explod!g2		1dcac3178a1b85d5179ce75eace04d10	dea53e331d3b9f21354147f60902f6e132f06183ed2f4a28e67816f9cb140a90	y
Trojan.Explod!g2		9a5a99def615966ea05e3067057d6b37	1952fa94b582e9af9dca596b5e51c585a78b8b1610639e3b878bbfa365e8e908	y
Trojan.Explod!g2		2b9106e8df3aa98c3654a4e0733d83e7	03641e5632673615f23b2a8325d7355c4499a40f47b6ae094606a73c56e24ad0	y
Trojan.Explod!g2		ab3d0c748ced69557f78b7071879e50a	3bedb4bdb17718fda1edd1a8fa4289dc61fdda598474b5648414e4565e88ecd5	y
Trojan.Explod!g2		c9a4317f1002fefcc7a250c3d76d4b01	50414f60d7e24d25f9ebb68f99d67a46e8b12458474ac503b6e0d0562075a985	y
Trojan.Explod!g2		4f8b989bc424a39649805b5b93318295	d8fdcdaad652c19f4f4676cd2f89ae834dbc19e2759a206044b18601875f2726	y
Trojan.Explod!g2		3f35c97e9e87472030b84ae1bc932ffc	5d491ea5705e90c817cf0f5211c9edbcd5291fe8bd4cc69cdb58e8d0e6b6d1fe	y
Trojan.Explod!g2		7cd87c4976f1b34a0b060a23faddbd19	fc085d9be18f3d8d7ca68fbe1d9e29abbe53e7582453f61a9cd65da06961f751	y
Trojan.Gen.2		ea53e618432ca0c823fafc06dc60b726	bc12d7052e6cfce8f16625ca8b88803cd4e58356eb32fe62667336d4dee708a3	y
Trojan.Explod		034e4c62965f8d5dd5d5a2ce34a53ba9	52cb02da0462fdd08d537b2c949e2e252f7a7a88354d596e9f5c9f1498d1c68f	y

Detection Name	Name	MD5	SHA 256	Malicious
Trojan.Explod!g2		5ca3ac2949022e5c77335f7e228db1d8	30196c83a1f857d36fde160d55bd4e5b5d50fbb082bd846db295cbe0f9d35cfb	y
Trojan.Explod		306d243745ba53d09353b3b722d471b8	41dd95533d85a0fd099ee79fbb4c8699ae6f9299b74034b8bafa3b0ea4a1fb3a	y
Trojan.Explod		e6f874b7629b11a2f5ed3cc2c123f8b6	97ab07c8020aead6ce0d9196e03d3917045e65e8c65e52a16ec6ef660dd96968	y
Trojan.Explod		5b505d0286378efcca4df38ed4a26c90	bd039bb73f297062ab65f695dd6defafd146f6f233c451e5ac967a720b41fc14	y
Trojan.Gen.2		7dbc46559efafe8ec8446b836129598c	d0f059ba21f06021579835a55220d1e822d1233f95879ea6f7cb9d301408c821	y
Trojan.Explod!g2		1d4b0fc476b7d20f1ef590bcaa78dc5d	1b76fdbd4cd92c7349bc992911376376 14f4fb9598ae29df0a39a422611b86f8	y
Trojan.Asprox.B		66e2adf710261e925db588b5fac98ad8	e5b68ab68b12c3eaff612ada09eb2d4c403f923cdec8a5c8fe253c6773208baf	y
Trojan.Explod	tools.dll	c898aed0ab4173cc3ac7d4849d06e7fa	37f4e9d0153221d9a236f299151c9f6911a6f78fff54c91b94ea64d1f3a8872b	y
Trojan.Explod		22872f40f5aad3354bbf641fe90f2fd6	ef47aaf4e964e1e1b7787c480e60a744550de847618510d2bf54bbc5bda57470	y
Trojan.Explod		c19e91a91a2fa55e869c42a70da9a506	b275c8978d18832bd3da9975d0f43cbc90e09a99718f4efaf1be7b43db46cf95	y
Trojan.Explod		740c47c663f5205365ae9fb08adfb127	bed0bec3d123e7611dc3d722813eeb197a2b8048396cef4414f29f24af3a29c4	y
Trojan.Explod		edaca6fb1896a120237b2ce13f6bc3e6	ea335556fecaf983f6f26b9788b286fbf5bd85ff403bb4a1db604496d011be29	y
Trojan.Explod		d2074d6273f41c34e8ba370aa9af46ad	0008065861f5b09195e51add72dacd3c4bbce6444711320ad349c7dab5bb97fb	y
Trojan.Explod		6f11a67803e1299a22c77c8e24072b82	d30f306d4d866a07372b94f7657a7a2b0500137fe7ef51678d0ef4249895c2c5	y
Trojan.Explod		7031426fb851e93965a72902842b7c2c	5a310669920099cd51f82bc9eb5459e9889b6357a21f7ce95ac961e053c79acb	y
Trojan.Explod		981234d969a4c5e6edea50df009efedd	bfc63b30624332f4fc2e510f95b69d18dd0241eb0d2fcd33ed2e81b7275ab488	y
Trojan.Explod		29eca6286a01c0b684f7d5f0bfe0c0e6	78201fd42dfc65e94774d8a9b87293c19044ad93edf59d3ff6846766ed4c3e2e	y
Trojan Horse,Trojan.Explode		826b772c81f41505f96fc18e666b1acd	6674ffe375f8ab54cfa2a276e4a39b414cf327e0b00733c215749e8a94385c63	y
Trojan.Explod!g1		da428bbf4f327fd2fde257630d7c507b	e5f691e445f693a96145e6f14c3be4d15c05d7c4b1e087e1ec683ead9c35a90e	y
Trojan.Explod!g3		f38407f50905ff1c27c9bee007239983	5953c9bf800c67b67f1a3d9691119488d3a1d6e6c6691f8a15d28436cd7122a7	y
Trojan.Explod!g3		5aadc6349663a3146cb8a323e7961e45	d1299a5c75882de2407f50b47c8a111349d4660e5b3fb7fdedfc4cfc2ef98a91	y
Trojan.Explod!g1		70f063057b3a3131a95a34a204802156	3becda7d601cf482d7ef236da6342239684694ed141a911601f321616440f6fa	y
Trojan.Explod!g2,Trojan.FakeAV!gen57		8f4aa2963e2ba10e0549370af4f9c1ca	47f45532108686fa535dbc32b5356f2005dc13c90f399170fa880ebd530f4645	y

Detection Name	Name	MD5	SHA 256	Malicious
Trojan.Explod!g3		8a520abc7998b8e5443fbacc62013526	a616c039b0ffa2682f001a6978c5edfaac2c3f828b6b18de6bc91f4abaa2d9bb	y
Trojan.Explod!g3	cat.aspx,caterpillar.aspx	05f456529f76e4f4fa9266cbae5efc03	2f2e794064e28a4cd6eb0c0e10d929453367c4b01a55fadf15037817c55e9cdb	y
Trojan.Explod!g3		a95a2d7cc06ca28b1f7639af3e90e025	493007afc73a3d6573b2b53457d6c82e24e16591807565d6caf3e5b6b5d407a2	y
Trojan.Explod!g3		80ed1fc942a6b0d4f32c1ff2e45f2443	b64d6e0e09b6daab209d14f2e684d819433605763208fbfc901a9ab7fd62ce05	y
Trojan.Explod!g3		6a8d62765ade6a58bcbaa295fd46c480	c103c3c0a1d7983ca1951a72800346fad32a67b4be013a97361a3d85e0e8cd98	y
Trojan.Explod!g3	cmd.aspx	2144d75b09a61850a86e0af2e5128942	e33118afd512762c79d840b782dd5cfa2472c97613103e60f8d5427a0a26beb3	y
Trojan.Explod!g3		dab2cbb34ec587587bdf0418f7fb06b1	4de07466f24a26311fe011f92c8b04e7c2c3ef4df8f5853bde523404ac06c34f	y
Archive		2783cee3aac144175fef308fc768ea63	973fbccbc6d917883d502c88cb7fadfc1a5657adbec377c7a4ed77292ebaeda9	y
Archive		f58f03121eed899290ed70f4d19af307	ba168c69866ba2e370c9bfbfe06d5863af0e4b387ce05084928710af3c7c43ce	y
Trojan.Explod		5a2338dd7d0fa0478e34b4407daabbc9	26e64f95ee23a6ec3b9fb8f937bed8e6ea247379b1f0b2e95ef071dc113b420c	y
		96b1221ba725f1aaeaaa63f63cf04092		y
Trojan.Explod!g1		eb7042ad32f41c0e577b5b504c7558ea	e2e6ed82703de21eb4c5885730ba3db42f3ddda8b94beb2ee0c3af61bc435747	y
Trojan.Explod!g1		44b5a3af895f31e22f6bc4eb66bd3eb7	a98099541168c7f36b107e24e9c80c9125fefb787ae720799b03bb4425aba1a9	y
Trojan.Explod		08c988d6cebdd55f3b123f2d9d5507a6	b74bd5660baf67038353136978ed16dbc7d105c60c121cf64c61d8f3d31de32c	y
Trojan.Explod!g1		61b11b9e6baae4f764722a808119ed0c	07529fae9e74be81fd302d022603d9f0796b4b9120b0d6131f75d41b979bbca5	y
Trojan.Explod!g1		c7ac6193245b76cc8cebc2835ee13532	bdef2ddcd8d4d66a42c9cbafd5cf7d86c4c0e3ed8c45cc734742c5da2fb573f7	y
Trojan.Explod!g2		184320a057e455555e3be22e67663722	388f5bc2f088769b361dfe8a45f0d5237c4580b287612422a03babe6994339ff	y
Trojan.Explod!g2		5d437eb2a22ec8f37139788f2087d45d	5663b2d4a4aec55d5d6fb507e3fdcb92ffc978d411de68b084c37f86af6d2e19	y
Trojan.Explod!g2		1dcac3178a1b85d5179ce75eace04d10	dea53e331d3b9f21354147f60902f6e132f06183ed2f4a28e67816f9cb140a90	y
Trojan.Explod!g2		9a5a99def615966ea05e3067057d6b37	1952fa94b582e9af9dca596b5e51c585a78b8b1610639e3b878bbfa365e8e908	y
Trojan.Explod!g2		2b9106e8df3aa98c3654a4e0733d83e7	03641e5632673615f23b2a8325d7355c4499a40f47b6ae094606a73c56e24ad0	y
Trojan.Explod!g2		ab3d0c748ced69557f78b7071879e50a	3bedb4bdb17718fda1edd1a8fa4289dc61fdda598474b5648414e4565e88ecd5	y
Trojan.Explod!g2		c9a4317f1002fefcc7a250c3d76d4b01	50414f60d7e24d25f9ebb68f99d67a46e8b12458474ac503b6e0d0562075a985	y

Detection Name	Name	MD5	SHA 256	Malicious
Trojan.Explod!g2		4f8b989bc424a39649805b5b93318295	d8fdcdaad652c19f4f4676cd2f89ae834dbc19e2759a206044b18601875f2726	y
Trojan.Explod!g2		3f35c97e9e87472030b84ae1bc932ffc	5d491ea5705e90c817cf0f5211c9edbcd5291fe8bd4cc69cdb58e8d0e6b6d1fe	y
Trojan.Explod!g2		7cd87c4976f1b34a0b060a23faddbd19	fc085d9be18f3d8d7ca68fbe1d9e29abbe53e7582453f61a9cd65da06961f751	y
Trojan.Gen.2		ea53e618432ca0c823fafc06dc60b726	bc12d7052e6cfce8f16625ca8b88803cd4e58356eb32fe62667336d4dee708a3	y
Trojan.Explod		034e4c62965f8d5dd5d5a2ce34a53ba9	52cb02da0462fdd08d537b2c949e2e252f7a7a88354d596e9f5c9f1498d1c68f	y
Trojan.Explod!g2		5ca3ac2949022e5c77335f7e228db1d8	30196c83a1f857d36fde160d55bd4e5b5d50fbb082bd846db295cbe0f9d35cfb	y
Trojan.Explod		306d243745ba53d09353b3b722d471b8	41dd95533d85a0fd099ee79fbb4c8699ae6f9299b74034b8bafa3b0ea4a1fb3a	y
Trojan.Explod		e6f874b7629b11a2f5ed3cc2c123f8b6	97ab07c8020aead6ce0d9196e03d3917045e65e8c65e52a16ec6ef660dd96968	y
Trojan.Explod		5b505d0286378efcca4df38ed4a26c90	bd039bb73f297062ab65f695dd6defafd146f6f233c451e5ac967a720b41fc14	y
Trojan.Gen.2		7dbc46559efafe8ec8446b836129598c	d0f059ba21f06021579835a55220d1e822d1233f95879ea6f7cb9d301408c821	y
Trojan.Explod!g2		1d4b0fc476b7d20f1ef590bcaa78dc5d	1b76fdbd4cd92c7349bc99291137637614f4fb9598ae29df0a39a422611b86f8	y
Trojan.Asprox.B		66e2adf710261e925db588b5fac98ad8	e5b68ab68b12c3eaff612ada09eb2d4c403f923cdec8a5c8fe253c6773208baf	y
Trojan.Explod	tools.dll	c898aed0ab4173cc3ac7d4849d06e7fa	37f4e9d0153221d9a236f299151c9f6911a6f78fff54c91b94ea64d1f3a8872b	y
Trojan.Explod		22872f40f5aad3354bbf641fe90f2fd6	ef47aaf4e964e1e1b7787c480e60a744550de847618510d2bf54bbc5bda57470	y
Trojan.Explod		c19e91a91a2fa55e869c42a70da9a506	b275c8978d18832bd3da9975d0f43cbc90e09a99718f4efaf1be7b43db46cf95	y
Trojan.Explod		740c47c663f5205365ae9fb08adfb127	bed0bec3d123e7611dc3d722813eeb197a2b8048396cef4414f29f24af3a29c4	y
Trojan.Explod		edaca6fb1896a120237b2ce13f6bc3e6	ea335556fecaf983f6f26b9788b286fbf5bd85ff403bb4a1db604496d011be29	y
Trojan.Explod		d2074d6273f41c34e8ba370aa9af46ad	0008065861f5b09195e51add72dacd3c4bbce6444711320ad349c7dab5bb97fb	y
Trojan.Explod		6f11a67803e1299a22c77c8e24072b82	d30f306d4d866a07372b94f7657a7a2b0500137fe7ef51678d0ef4249895c2c5	y
Trojan.Explod		7031426fb851e93965a72902842b7c2c	5a310669920099cd51f82bc9eb5459e9889b6357a21f7ce95ac961e053c79acb	y
Trojan.Explod		981234d969a4c5e6edea50df009efedd	bfc63b30624332f4fc2e510f95b69d18dd0241eb0d2fcd33ed2e81b7275ab488	y
Trojan.Explod		29eca6286a01c0b684f7d5f0bfe0c0e6	78201fd42dfc65e94774d8a9b87293c19044ad93edf59d3ff6846766ed4c3e2e	y
Trojan Horse,Trojan.Explode		826b772c81f41505f96fc18e666b1acd	6674ffe375f8ab54cfa2a276e4a39b414cf327e0b00733c215749e8a94385c63	y

Detection Name	Name	MD5	SHA 256	Malicious
Trojan.Explod!g1		da428bbf4f327fd2fde257630d7c507b	e5f691e445f693a96145e6f14c3be4d15c05d7c4b1e087e1ec683ead9c35a90e	y
Trojan.Explod!g3		f38407f50905ff1c27c9bee007239983	5953c9bf800c67b67f1a3d9691119488d3a1d6e6c6691f8a15d28436cd7122a7	y
Trojan.Explod!g3		5aadc6349663a3146cb8a323e7961e45	d1299a5c75882de2407f50b47c8a111349d4660e5b3fb7fdedfc4cfc2ef98a91	y
Trojan.Explod!g1		70f063057b3a3131a95a34a204802156	3becda7d601cf482d7ef236da6342239684694ed141a911601f321616440f6fa	y
Trojan.Explod!g2,Trojan.FakeAV!gen57		8f4aa2963e2ba10e0549370af4f9c1ca	47f45532108686fa535dbc32b5356f2005dc13c90f399170fa880ebd530f4645	y
Trojan.Explod!g3		8a520abc7998b8e5443fbacc62013526	a616c039b0ffa2682f001a6978c5edfaac2c3f828b6b18de6bc91f4abaa2d9bb	y
Trojan.Explod!g3	cat.aspx,caterpillar.aspx	05f456529f76e4f4fa9266cbae5efc03	2f2e794064e28a4cd6eb0c0e10d929453367c4b01a55fadf15037817c55e9cdb	y
Trojan.Explod!g3		a95a2d7cc06ca28b1f7639af3e90e025	493007afc73a3d6573b2b53457d6c82e24e16591807565d6caf3e5b6b5d407a2	y
Trojan.Explod!g3		80ed1fc942a6b0d4f32c1ff2e45f2443	b64d6e0e09b6daab209d14f2e684d819433605763208fbfc901a9ab7fd62ce05	y
Trojan.Explod!g3		6a8d62765ade6a58bcbaa295fd46c480	c103c3c0a1d7983ca1951a72800346fad32a67b4be013a97361a3d85e0e8cd98	y
Trojan.Explod!g3	cmd.aspx	2144d75b09a61850a86e0af2e5128942	e33118afd512762c79d840b782dd5cfa2472c97613103e60f8d5427a0a26beb3	y
Trojan.Explod!g3		dab2cbb34ec587587bdf0418f7fb06b1	4de07466f24a26311fe011f92c8b04e7c2c3ef4df8f5853bde523404ac06c34f	y
Archive		2783cee3aac144175fef308fc768ea63	973fbccbc6d917883d502c88cb7fadfc1a5657adbec377c7a4ed77292ebaeda9	y
Archive		f58f03121eed899290ed70f4d19af307	ba168c69866ba2e370c9bfbfe06d5863af0e4b387ce05084928710af3c7c43ce	y
Trojan.Explod		5a2338dd7d0fa0478e34b4407daabbc9	26e64f95ee23a6ec3b9fb8f937bed8e6ea247379b1f0b2e95ef071dc113b420c	y
		96b1221ba725f1aaeaaa63f63cf04092		y

TARGET INDUSTRIES

NAICS Code	Name
92	Public Administration
61	Educational Services
51	Information

SOURCE REGIONS

Region	Asia
Subregion	Western Asia
Countries	Lebanon

TARGET REGIONS

Region	America; Europe; Asia
Subregion	North America; Northern Europe; Western Asia
Countries	Canada; United States; United Kingdom; Lebanon; Turkey; Israel

THREAT DOMAINS

Cyber Espionage