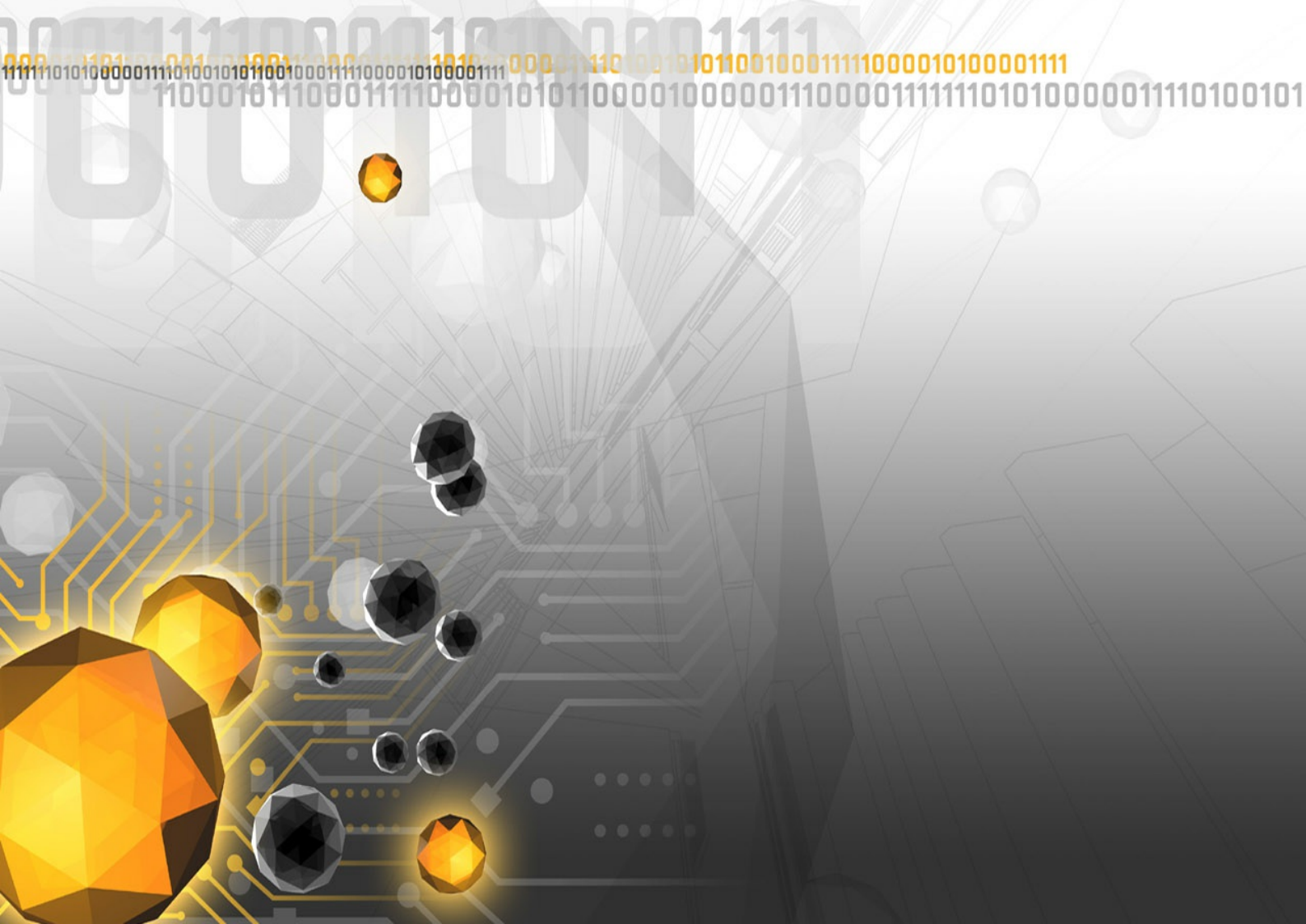
DeepSight™ INTELLIGENCE

CHINESE CYBER ESPIONAGE ACTOR COLD WIND AND THE ALPHA LABORATORY

MANAGED ADVERSARY AND THREAT INTELLIGENCE

DEEPSIGHT™ INTELLIGENCE | INTELLIGENCE REPORT | SYMC - 300243 | V.1
31 JUL 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: 29 Jul 2015 GMT

Chinese Cyber Espionage Actor Cold Wind and the Alpha Laboratory

DeepSight™ Intelligence | Intelligence Report | SYMC - 300243 | V.1 | 31 Jul 2015 GMT

KEY FINDINGS

Beijing Topsec Science and Technology Corporation's Alpha Laboratory (阿尔法实验室) provides computer network exploitation (CNE) support to the People's Republic of China (PRC) military and government.

An Alpha Laboratory employee with screen name Cold Wind (冷风) developed the newly identified IceGale cyber espionage RAT over the period of 2013–2015.

EXECUTIVE SUMMARY

DeepSight Intelligence assesses with high confidence that the Beijing Topsec Science and Technology Corporation's (北京天融信科技有限公司) Attack and Defense Research Center (天融信攻防研究中心), also known as the Alpha Laboratory (阿尔法实验室), provides computer network exploitation (CNE) support to the PRC military and government. The Alpha Laboratory was established in the second half of 2013 likely indicating Topsec's commitment to fulfilling an increasing demand for offensive and defensive cyber operation services. Topsec and Venus-tech, a second Beijing-based information security firm, likely compete with each other in providing these services.

DeepSight Intelligence further assesses with high confidence that an Alpha Laboratory employee with screen name Cold Wind (冷风) developed the IceGale cyber espionage RAT over the period 2013–2015 and has ten years of experience in RAT design and network exploitation. DeepSight Intelligence has previously reported on the use of the IceGale RAT against a top five ranked US university.

DETAILS

DeepSight Intelligence assesses with high confidence that an individual with the account name Cold Wind (a.k.a. 冷风,chinafe) on the CSDN forum[1] and EvilOctal platform[2] developed the IceGale RAT over the 2013–2015 period. DeepSight Intelligence has previously reported on the use of the IceGale RAT against a top five ranked US university (university #1)[3]. Cold Wind is but one member of a large network of linked PRC-based personas that participate on these Mandarin-language web forums and platforms. Several of these personas have previously been associated with network exploitation operations.

Cold Wind has been publishing information on RAT development and network exploitation on these platforms for at least ten years. His most recent writing, in 2015, discusses tools and techniques of intranet (internal network) penetration including post-breach network reconnaissance and credential harvesting.

According to CSDN information reviewed 30 July 2015, the blog of account holder Cold Wind contains approximately 500 posts from September 2005 to July 2015 on RAT development, network exploitation, programming, and other topics. Included are 87 posts under the category Trojan writing (October 2006 to December 2014) and 17 on intranet (internal network) penetration (May 2013 to July 2015).

- Within the set of posts on RAT development, DeepSight Intelligence has identified the six posts shown in Table 1 as containing code fragments and descriptions related to IceGale development.

Posting Date	Description of Post
28 September 2014	Gives sample code for 4K buffer-masking functions within the context of AV detection evasion.
13 January 2014	Discusses finding a bug relating to the use of the UDT protocol that involves the string UDPUDP.
21 November 2013	Describes four components of a RAT: generator, installer, hijack DLL, and server (named server.db). Mentions an INI config file, that the hijack DLL loads the server, and that the server accepts plug-ins.
7 November 2013	Describes placing shellcode within a DLL that allows the DLL to unload itself.
29 March 2013	Gives a code example for loading a program at startup by setting a "software\\XXZH" registry key.
16 January 2013	Discusses using a UDP-based Data Transfer Protocol (UDT) library with a RAT and includes Microsoft Visual Studio 2008 screen shots.

Table 1. Blog posts under CSDN account Cold Wind that relate to IceGale development

The posts contain very specific fragments of information, but neither the full source code nor a binary RAT package has been found in publicly accessible web media. This indicates the RAT has likely not been released publicly.

- The internal network penetration posts discuss topics including phishing email techniques, the use of Procdump and Mimikatz to extract Windows account credentials, one-statement VBS download scripts, and post-breach network reconnaissance tools/commands.

According to DeepSight Intelligence analysis, the most recently observed IceGale sample (MD5: 98cee79f1d0b57650ccfe675c999b98f) was compiled 20 May 2015 and observed 19 June 2015. The earliest known sample (MD5: 1eebd6ab4e84fc8e7097d1f13cd93f24) was observed 23 September 2014 (compile date unknown).

According to CSDN and EvilOctal forum information reviewed 29 July 2015, a 13 May 2007 CSDN blog post under account Cold Wind lists a link to an EvilOctal forum post as a place where a Cold Wind-developed RAT could be downloaded. (This linked EvilOctal account uses account names Cold Wind and chinafe.) The EvilOctal account includes 26 detailed articles on RAT development and network exploitation posted over the period June 2007 to November 2009. According to EvilOctal forum information, the account was last active March 2015 and was created in October 2005.

According to CSDN information reviewed 28 July 2015, the CSDN blog under account Cold Wind lists 25 side-bar links to social media accounts, forums, and websites under categories including Pandora, K brothers, masters, friends, Trojan writing, and recommended websites.

- Analysis of this network identified distance two links[4] to web media associated with personas Sincoder and Sunshine. The e-mail address root[@]cmdshell.com was associated with Sunshine and network infrastructure linked to the April–June intrusion at university #1[5]. According to a 29 July 2014 blog post by Dell SecureWorks, persona Sincoder was associated with advanced network exploitation operations against computer game firms.
- The side-bar list also includes a link to PRC-based Mandarin-language forum Whitecell[6] (now offline) and the home page of Poison Ivy.

DeepSight Intelligence assesses with high confidence that between April 2014 and December 2014, actor Cold Wind was a security researcher at the Beijing Topsec Science and Technology Alpha Laboratory. It is likely that he continues in this position at the time of this publication.

According to a reliable 27 August 2014 Mandarin-language article reporting on the 2014 KCon conference, held 22 August 2014 in Beijing, and its presenters by the CSDN news bureau titled, “Approaching the world of hackers you can sense the heartbeat of cyberspace,” an individual with screen name Cold Wind was a security researcher within the Alpha Laboratory of Beijing Topsec and a CSDN expert with the blog identified in the previous assessment. His conference presentation was on “APT special trojan technology.” This description was accompanied by the image shown in Figure 1.

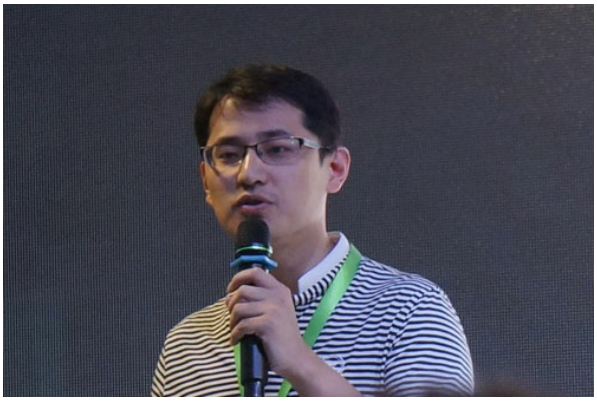


Figure 1. Cold Wind speaking at the 2014 Kcon conference held August 2014 in Beijing.

According to the Mandarin-language 2014 Kcon conference website, an individual with screen name Cold Wind was a conference presenter and gave a presentation on “APT special trojan technology.”

According to the Beijing Topsec Alpha Laboratory's corporate website, on 17 April 2014, an employee with screen name Cold Wind posted a Mandarin-language article on APT attack and defense and the Poison Ivy RAT.

According to EvilOctal forum information, on 31 December 2014, a Mandarin-language post under account name Cold Wind contained a recruitment notice for six security researcher positions at the Topsec Alpha Laboratory. These positions included a Windows/Linux vulnerability discovery and exploitation researcher as well as a network penetration test researcher.

DeepSight Intelligence assesses with high confidence that the Beijing Topsec Alpha Laboratory provides offensive network operations services to the PRC military and government and is also known as the Attack and Defense Research Center (天融信攻防研究中心, adlab). In the analysis above and in prior DeepSight Intelligence reporting, it has been identified that Cold Wind, while working at the center, was developing a RAT that has since been observed in cyber espionage operations. The company's own description of the center's functions includes support to the military as well as network attack and defense services. In addition, prior public reporting from 2015 provides further associations between the company and 2014 cyber espionage operations against US-based health insurance firms.

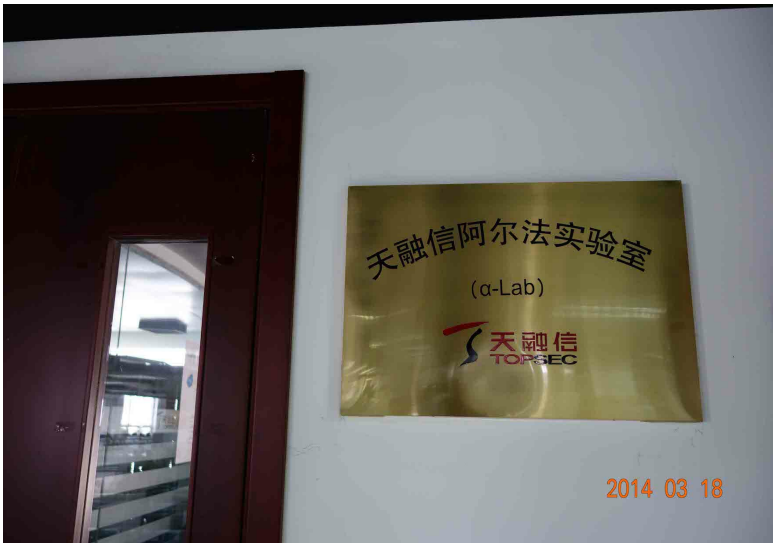


Figure 2. The entrance to the Beijing Topsec Corporation's Alpha Laboratory. Obtained from publicly available Topsec publicity material, the image is dated 18 March 2014.

According to reliable, publicly available, late-2013, Mandarin-language material by the Topsec company, the Topsec attack and defense research center was established during the second half of 2013 and is also known as the Alpha Laboratory or adlab. According to this material, the purpose of the center is to provide a range of services to the military and other government departments including "network attack, defense and penetration services," attack/defense simulation exercises under realistic conditions, and support to network defense. To provide these services, the center conducts research on advanced network attack and defense tools and techniques.

According to a 29 July 2015 paper by Symantec Security Response, the domain topsec2014[.]com was one of a few domains hosted on IP address 192[.]199.254.126. This IP address was associated

with 2014 cyber espionage operations against US-based health insurance firms. According to the paper, this domain's registrant email address was also associated with Beijing Topsec and a 2014 information security competition known as the Topsec Cup.

According to a 6 December 2010 article in Computerworld, the Topsec firm's founder and chairman, He Weidong, stated that the firm was partially funded by the PRC government.

---

[1] The Chinese Software Development Network (CSDN) is a PRC-based, Mandarin-language code sharing, software development, IT news, and social media platform.

[2] EvilOctal is an influential PRC-based, Mandarin-language hacking forum associated with Guilin University. Other notable forum members include Tan Dailin (Withered Rose) and Hack520.

[3] See DeepSight Intelligence report *Introducing PRC Cyber Espionage RAT: IceGale* (SYMC-300236), 24 July 2015.

[4] If Blog A links to blog B, which links to blog C, then blogs A and C have a distance two-link relationship.

[5] See DeepSight Intelligence report *PRC-Based Cyber Espionage Activity at Leading US University Likely Targeted International Relations Scholars; New Tool Samples Identified* (SYMC-300227), 10 July 2015.

[6] Whitecell was an advanced network exploitation research forum that PlugX developer Whg was once a member of.

OUTLOOK

Beijing Venus Information Technology Corporation (北京启明星辰信息技术有限公司), another leading Beijing-based information security firm, also runs an offensive and defensive network operations research laboratory named the Active Defense Laboratory (积极防御实验室). DeepSight Intelligence assesses that these two firms compete in providing offensive and defensive operations support to the PRC military and government. The 2013 investment by Topsec in the creation of a new research center likely shows increasing demands for such services.

TECHNICAL DETAILS

See the ***Metadata*** tab for the technical details and indicators of compromise related to this report.

METADATA

EXTRACTED INDICATORS

Indicator	Indicator Related CVE	Indicator Type
488a0a11f893ef86ed9a7757b160fd24		file_md5
ada9dd9781d70a50fe8e29025065fe36f7b60ba46e138174dba631d04b99e34f		file_sha256
02ad8e25d6e9e7716c207efb9dfaa36c		file_md5
421ea8a7748fa3f1877566420547044b207f2229b24d96d84f522e254366a67e		file_sha256
d6e51b2ca21886bf4287d264c55ad017		file_md5
ea31f3a9275f43fc0ff6594b4f76597a4693c81e035160a462a35fb4b135603c		file_sha256
76c14ffc03630ca8108b98acfb374237		file_md5
1c3ef7c81bf1e06d45fec3f52365bfa4576125a770bcdbe94cc43526ca2f159a		file_sha256
db43626ba0195da4e2db8f58de3630f2		file_md5
1231779eb66ca932a29464cf0f73de5472a94ec59734d2d61dd4abdbf2fbc123		file_sha256
flash.exe		file_name
0f647fc0aba78ab6173ef2998a750b54		file_md5
fb432fdfa29e8d339f31712e9b787fbee70dafe3c88b7a6b5b7a143e7e86616a		file_sha256
firefox.exe		file_name
9af9c671c83a311fc880d9a3b6e10227		file_md5
a9495e674d93eb5491075cef5281b6256c9e66f4e78911482d0e5fc6037bb6f6		file_sha256
nspr4.dll		file_name
75c5aa830b199f698d7cf66af28be845		file_md5
0c0c295ed89ea0fb3167c1e3eb00c6c34a428f7409953de90fbbd510ef3965e6		file_sha256
server.db		file_name
afb924318bf157882f17ee559d27f9c2		file_md5
79434cfb9617bf116897f6976d34f2467441fb0359131c0d83bd9e92452f72e5		file_sha256
sleep.db		file_name
b015cc36fe449fb592d6ca279e49c2c8		file_md5
af5b4d99e1165626af0c8a15e5ec046687cfa969876b61ca5b737332da9a55c7		file_sha256
1eebd6ab4e84fc8e7097d1f13cd93f24		file_md5
setup.zip		file_name
e02e45ca62ab8998d42923ab255fb776		file_md5
45aec9abb961beb4f0e73883a922d8cba618f6848c97a79c10e22133ec12d142		file_sha256
dfbb3da9a0f42080ad2f3292b33964f6		file_md5
67588248121fb5ed830bc0acb3d061aeee77c5c6e733b42ea9ce7e0f10082222		file_sha256

Indicator	Indicator Related CVE	Indicator Type
McUtil.dll		file_name
260a22e03bde4a1c2f01a6b591b07bf9		file_md5
670a033cd926e4e1a5d0c2a246c4316204e24200f219a096f8acf683d1868fbc		file_sha256
server.db		file_name
c24ecf1dfef4c3d195b58c185e31de12		file_md5
setup.exe		file_name
f38dd1c66c99ee817426a53b33329806		file_md5
4f8905c6e60ff76041603401ddb1e10dd137ed1755828c6ed93b1b65f033c7eb		file_sha256
McUtil.dll		file_name
c75b9940bddd9172d249df98c579dfa4		file_md5
1b5849be515d68c655fab654f76eced81b17a0ddcfddf358607b09aab0bd28b8		file_sha256
server.db		file_name
79c579d96e77e5e97911be443f1373e8		file_md5
b47e300069cb25df69d209746977ed0a915dba4161fad462a8751665d370281e		file_sha256
eb7b32feabc4e89d91a79e28253b45f8		file_md5
a8927cb1a3162485b77d8aa0d3b6bf189822e4c635755f2d98b1e990dc20ce36		file_sha256
7dcca4efe130a4b2ea1866c5add4f0a3		file_md5
fa546ff8105322834d5c3a74457b32656973bc847e5a723d903b2d9e1892d151		file_sha256
752729d7f2b40049304495f2b0ad554c		file_md5
237c81e91774b1cb463d4d7801df74a9005bbf305dfdbd033831febfcd7d3754		file_sha256
be9e45017a804d987d81c67466f4830d		file_md5
4ea260ecf2aed08c4c16c811a079e5f2252c753fc445431071f95f66491cf853		file_sha256
d306f20806818035be0f93571b27e1f7		file_md5
b83ffd77099be2b5309f9dceb564151d3111627905884eece30a3472f5d8f11e		file_sha256
server.db		file_name
d3e728d07cd2f2a6e5e31095131d26c9		file_md5
686c77b492ef127e5aec27974c5226162918702685a7c5dde1c003228d3219b8		file_sha256
default.govnb.com		domain
heritage.govnb.com		domain
fuckchina.govnb.com		domain
gameofthrones.ddns.net		domain
mail.vip53.cn		domain
sl.vip53.cn		domain
jakisdog.ddns.net		domain
ns1.symantec-inc.com		domain
ns3.symantec-inc.com		domain
yk.vip53.cn		domain

Indicator	Indicator Related CVE	Indicator Type
ashex.eicp.net		domain
update.mcafee-update.com		domain
lh.huanke8.net		domain
lhok.newsbs.net		domain
chrome.https443.net		domain
yandextech.trickip.org		domain
checkup.mrbasic.com		domain
blackout.organiccrap.com		domain
192.225.226.132		ip_address
123.30.127.133		ip_address
174.37.172.71		ip_address
122.10.88.26		ip_address
122.10.116.52		ip_address
103.24.245.5		ip_address
174.128.255.231		ip_address
153.121.53.115		ip_address
101.55.33.116		ip_address

FILES

Detection Name	Name	MD5	SHA 256	Malicious
		488a0a11f893ef86ed9a7757b160fd24	ada9dd9781d70a50fe8e29025065fe36f7b60ba46e138174dba631d04b99e34f	y
WS.Reputation.1		02ad8e25d6e9e7716c207efb9dfaa36c	421ea8a7748fa3f1877566420547044b207f2229b24d96d84f522e254366a67e	y
WS.Reputation.1		d6e51b2ca21886bf4287d264c55ad017	ea31f3a9275f43fc0ff6594b4f76597a4693c81e035160a462a35fb4b135603c	y
WS.Reputation.1		76c14ffc03630ca8108b98acfb374237	1c3ef7c81bf1e06d45fec3f52365bfa4576125a770bcdbe94cc43526ca2f159a	y
Trojan.Gen.2		db43626ba0195da4e2db8f58de3630f2	1231779eb66ca932a29464cf0f73de5472a94ec59734d2d61dd4abdbf2fbc123	y
Trojan.Gen.2	flash.exe	0f647fc0aba78ab6173ef2998a750b54	fb432fdfa29e8d339f31712e9b787fbee70dafe3c88b7a6b5b7a143e7e86616a	y
	firefox.exe	9af9c671c83a311fc880d9a3b6e10227	a9495e674d93eb5491075cef5281b6256c9e66f4e78911482d0e5fc6037bb6f6	y
	nspr4.dll	75c5aa830b199f698d7cf66af28be845	0c0c295ed89ea0fb3167c1e3eb00c6c34a428f7409953de90fbbd510ef3965e6	y
	nss3.dll	8a0abb851f919b6ee942c507dfb6b7c2	8185216e84ca319e27f3e989ae92d597d80be6643a9af0fb591d32a9ef8ca86e	n
	server.db	afb924318bf157882f17ee559d27f9c2	79434cfb9617bf116897f6976d34f2467441fb0359131c0d83bd9e92452f72e5	y

Detection Name	Name	MD5	SHA 256	Malicious
	sleep.db	b015cc36fe449fb592d6ca279e49c2c8	af5b4d99e1165626af0c8a15e5ec046687cfa969876b61ca5b737332da9a55c7	y
		1eebd6ab4e84fc8e7097d1f13cd93f24		y
WS.Reputation.1	setup.zip	e02e45ca62ab8998d42923ab255fb776	45aec9abb961beb4f0e73883a922d8cba618f6848c97a79c10e22133ec12d142	y
Backdoor.Trojan		dfbb3da9a0f42080ad2f3292b33964f6	67588248121fb5ed830bc0acb3d061aeee77c5c6e733b42ea9ce7e0f10082222	y
	AdobeTray.exe	324fc68be8b6a43ec46bca634f899747	d64ecd5db9ef68428c1a024274af360d565435ff9c5b92ef2cf5d9e03d4f063d	n
Backdoor.Trojan	McUtil.dll	260a22e03bde4a1c2f01a6b591b07bf9	670a033cd926e4e1a5d0c2a246c4316204e24200f219a096f8acf683d1868fbc	y
	server.db	c24ecf1dfef4c3d195b58c185e31de12		y
WS.Reputation.1	setup.exe	f38dd1c66c99ee817426a53b33329806	4f8905c6e60ff76041603401ddb1e10dd137ed1755828c6ed93b1b65f033c7eb	y
	AdobeTray.exe	884d46c01c762ad6ddd2759fd921bf71	3124fcb79da0bdf9d0d1995e37b06f7929d83c1c4b60e38c104743be71170efe	n
	McUtil.dll	c75b9940bddd9172d249df98c579dfa4	1b5849be515d68c655fab654f76eced81b17a0ddcfddf358607b09aab0bd28b8	y
	server.db	79c579d96e77e5e97911be443f1373e8	b47e300069cb25df69d209746977ed0a915dba4161fad462a8751665d370281e	y
		eb7b32feabc4e89d91a79e28253b45f8	a8927cb1a3162485b77d8aa0d3b6bf189822e4c635755f2d98b1e990dc20ce36	y
Backdoor.Trojan		7dcca4efe130a4b2ea1866c5add4f0a3	fa546ff8105322834d5c3a74457b32656973bc847e5a723d903b2d9e1892d151	y
WS.Reputation.1		752729d7f2b40049304495f2b0ad554c	237c81e91774b1cb463d4d7801df74a9005bbf305dfdbd033831febfcd7d3754	y
Backdoor.Trojan		be9e45017a804d987d81c67466f4830d	4ea260ecf2aed08c4c16c811a079e5f2252c753fc445431071f95f66491cf853	y
WS.Reputation.1		d306f20806818035be0f93571b27e1f7	b83ffd77099be2b5309f9dceb564151d3111627905884eece30a3472f5d8f11e	y
	server.db	d3e728d07cd2f2a6e5e31095131d26c9	686c77b492ef127e5aec27974c5226162918702685a7c5dde1c003228d3219b8	y

TARGET INDUSTRIES

NAICS Code	Name
51	Information

SOURCE REGIONS

Region	Asia
Subregion	Eastern Asia
Countries	China

TARGET REGIONS

Region	Americas
Subregion	North America
Countries	United States

THREAT DOMAINS

Cyber Espionage