Burning Umbrella

An Intelligence Report on the Winnti Umbrella and Associated State-Sponsored Attackers.

Tom Hegel

May 3, 2018

Table of Contents

Key Judgements

- We assess with high confidence that the Winnti umbrella is associated with the Chinese state intelligence apparatus, with at least some elements located in the Xicheng District of Beijing.
- A number of Chinese state intelligence operations from 2009 to 2018 that were previously unconnected publicly are in fact linked to the Winnti umbrella.
- We assess with high confidence that multiple publicly reported threat actors operate with some shared goals and resources as part of the Chinese state intelligence apparatus.
- Initial attack targets are commonly software and gaming organizations in United States, Japan, South Korea, and China. Later stage high profile targets tend to be politically motivated or high value technology organizations.
- The Winnti umbrella continues to operate highly successfully in 2018. Their tactics, techniques, and procedures (TTPs) remain consistent, though they experiment with new tooling and attack methodologies often.
- Operational security mistakes during attacks have allowed us to acquire metrics on the success of some Winnti umbrella spear phishing campaigns and identify attacker location with high confidence.
- The theft of code signing certificates is a primary objective of the Winnti umbrella's initial attacks, with potential secondary objectives based around financial gain.

Report Summary

The purpose of this report is to make public previously unreported links that exist between a number of Chinese state intelligence operations. These operations and the groups that perform them are all linked to the Winnti umbrella and operate under the Chinese state intelligence apparatus. Contained in this report are details about previously unknown attacks against organizations and how these attacks are linked to the evolution of the Chinese intelligence apparatus over the past decade. Based on our findings, attacks against smaller organizations operate with the objective of finding and exfiltrating code signing certificates to sign malware for use in attacks against higher value targets. Our primary telemetry consists of months to years of full fidelity network traffic captures. This dataset allowed us to investigate active compromises at multiple organizations and run detections against the historical dataset, allowing us to perform a large amount of external infrastructure analysis.

Background

The Winnti umbrella and closely associated entities has been active since at least 2009, with some reports of possible activity as early as 2007. The term "umbrella" is used in this report because current intelligence indicates that the overarching entity consists of multiple teams/actors whose tactics, techniques, and procedures align, and whose infrastructure and operations overlap. We assess that the different stages of associated attacks are operated by separate teams/actors, however in this report we will show that the lines between them are blurred and that they are all associated with the same greater entity. The Winnti and Axiom group names were created by Kaspersky Lab and Symantec, respectively, for their 2013/2014 reports on the original group. The name “Winnti” is now primarily used to refer to a custom backdoor used by groups under the umbrella. Multiple sources of public and private threat intelligence have their own names for individual teams. For example, LEAD is a common alias for the group targeting online gaming, telecom, and high tech organizations. Other aliases for groups related include BARIUM, Wicked Panda, GREF, PassCV, and others. This report details how these groups are linked together and serve a broader attacker mission. The many names associated with actors in the greater intelligence mission are due to the fact that they are built on telemetry of the intelligence provider which is typically unique and dependent on their specific dataset. This report focuses heavily on networking related telemetry.

We assess with high confidence that the attackers discussed here are associated with the Chinese state intelligence apparatus. This assessment is based on attacker TTPs, observed attack infrastructure, and links to previously published intelligence. Their operations against gaming and technology organizations are believed to be economically motivated in nature. However, based on the findings shared in this report we assess with high confidence that the actor's primary long-term mission is politically focused. It's important to note that not all publicly reported operations related to Chinese intelligence are tracked or linked to this group of actors. However, TTPs, infrastructure, and tooling show some overlap with other Chinese-speaking threat actors, suggesting that the Chinese intelligence community shares human and technological resources across organizations. We assess with medium to high confidence that the various operations described in this report are the work of individual teams, including contractors external to the Chinese government, with varying levels of expertise, cooperating on a specific agenda.

In 2015 the People's Liberation Army of China (PLA) began a major reorganization which included the creation of the Strategic Support Force (SSF / PLASSF). SSF is responsible for space, cyber, and electronic warfare missions. Some of the overlap we observed from groups could potentially be related to this reorganization. Notably, key incident details below include attacker mistakes that likely reveal the true location of some attackers as the Xicheng District of Beijing.

Tactics, Techniques, and Procedures (TTPs):

Though the TTPs of the attacking teams vary depending on the operation, their use of overlapping resources presents a common actor profile. Key interests during attacks often include the theft of code signing certificates, source code, and internal technology documentation. They also may attempt to manipulate virtual economies for financial gain. While unconfirmed, the financial secondary objective may be related to personal interests of the individuals behind the attacks.

Initial attack methods include phishing to gain entry into target organization networks. The group then follows with custom malware or publicly available offensive tooling (Metasploit/Cobalt Strike), and may use a number of methods to minimize their risk of being detected. Such techniques include a particular focus on "living off the land" by using a victim's own software products, approved remote access systems, or system administration tools for spreading and maintaining unauthorized access to the network.

We have observed incidents where the attacker used other victim organizations as a proxy for unauthorized remote access. In these cases, organization 1 had been compromised for a long period of time, and the attacker accessed victim organization 2 via the organization 1 network.

Delivery and C2 domains routinely have subdomains which resemble target organizations. Additionally, their C2 domains are used across many targets, while subdomains tend to be created and removed quickly and are unique to a particular target or campaign. Also noteworthy is that the actors set their domains to resolve to 127.0.0.1 when not in use, similar to what was originally reported on by Kaspersky Lab (see below).

The actor often uses TLS encryption for varying aspects of C2 and malware delivery. As noted in the “Infrastructure Analysis” section of this report, the actor primarily abuses Let’s Encrypt to sign SSL certificates. We also observed many cases in which self-signed certificates were used in attacks.

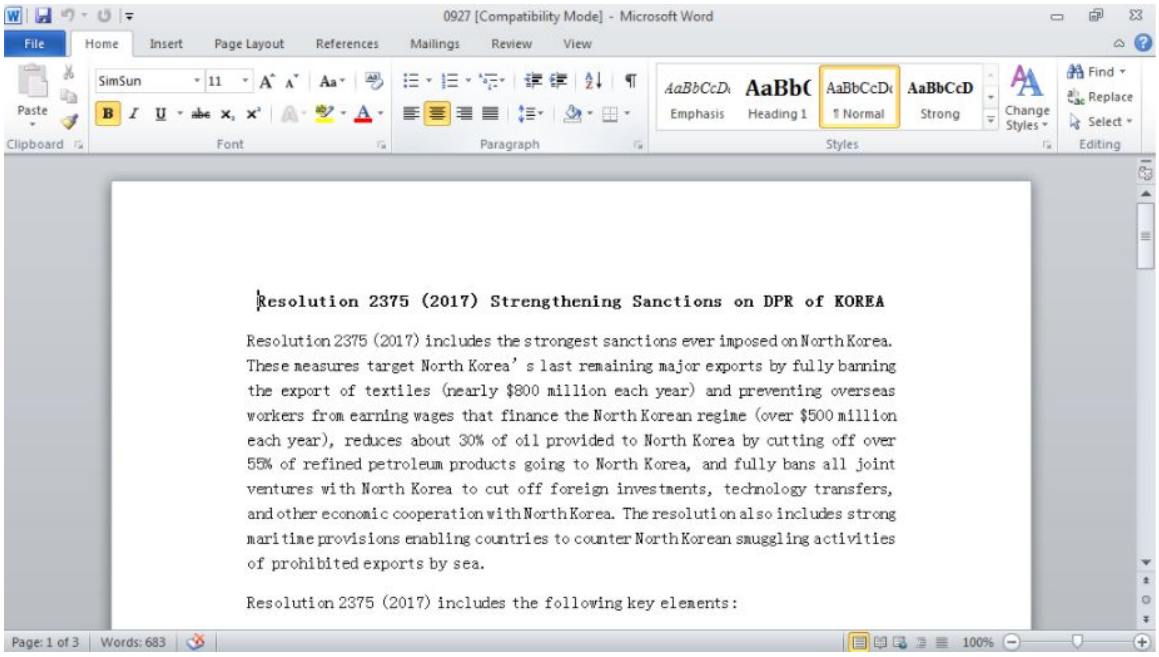
Overall, the Winnti umbrella and linked groups are lacking when it comes to operational security. However, some activities linked to these groups follow better operational security and infrastructure management approaches. This may be a clue to the division of responsibilities by team and skill level within the broader organization.

Targets:

The Winnti umbrella and linked groups’ initial targets are gaming studios and high tech businesses. They primarily seek code signing certificates and software manipulation, with potential financially motivated secondary objectives. These targets have been identified in the United States, Japan, South Korea, and China.

Based on the infrastructure, links to previous reporting, and recently observed attacks, the broader organization’s main targets are political. Historically this has included Tibetan and Chinese journalists, Uyghur and Tibetan activists, the government of Thailand, and prominent international technology organizations.

One example of a politically focused lure by the Winnti umbrella and linked groups is an end of 2017 document titled “Resolution 2375 (2017) Strengthening Sanctions on DPR of KOREA” which is a malicious file associated with the C2 infrastructure described here - see MD5: 3b58e122d9e17121416b146daab4db9d.



Some Key Public Reports:

2013:

Kaspersky Lab publicly reported on the original Winnti group, technical details around the Winnti samples, and various honeypot analysis methods. Most noteworthy is the Winnti umbrella's targeting of gaming organizations in search of code signing certificates, virtual currencies, and updating mechanisms which could potentially be used to attack victims' clients. Interestingly, this was the first identified trojan for the 64-bit Microsoft Windows operating system with a valid digital signature as noted by the author. The abuse of signed applications is a very effective attack approach that the entity continues to use.

2014:

Novetta released an outstanding report detailing "Operation SMN," in which they collaborated with a number of private organizations on a large scale malware eradication operation which is linked to the original Winnti group by the malware being delivered. In the report, the actor is named Axiom. Novetta reported links to publications from as far back as 2009 that also link the group to the Chinese state intelligence apparatus with high confidence. Links exist to various known attacks and actor groups, such as "Operation Aurora," Elderwood Group's successful 2010 attack against Google and many other organizations. Another link exists to the successful compromise of the security organization Bit9 in 2013, where their own product was used to sign and spread malware to their customers. In addition, FireEye's "Operation DeputyDog" detailed attacks on Japanese targets from the same attack infrastructure. Many other incidents are detailed in the Operation SMN report. Following all of these details back in time, we can see an overlap in TTPs and

targets from the APT1 report by Mandiant, which serves as a great historical example of Chinese intelligence cyber operations in their most basic form.

2016:
Cylance released a blog post reporting on digitally signed malware used in targeted attacks against gaming organizations in China, Taiwan, South Korea, Europe, Russia, and the United States. Cylance refers to the attacking entity as “PassCV” in their reporting. Cylance successfully identified a large quantity of malware binaries which were signed with valid certificates stolen from a number of gaming studios in East Asia. In addition to detailing the individual certificates and signed malware, they identified a significant amount of network infrastructure which contain various interesting links to our own findings.

2017 - March/April:
Trend Micro reported on attacks that abused GitHub for use in malware command and control, which they attributed to the original Winnti group. Amusingly, Trend Micro later reported on an individual linked to the group and the attacks who happens to be a fan of pigs.

2017 - July 5th:
Citizen Lab reported on attacks against journalists by an actor mimicking China-focused news organizations HK01, Epoch Times, Mingjing News, and Bowen Press. As Citizen Lab noted, these news organizations are blocked in China for their political views. The report notes that malware used in these attacks was linked to a stolen code signing certificate mentioned in the Cylance PassCV post. That overlap, in addition to infrastructure links from a Palo Alto Unit 42 blog post, strongly links this attack to the previously mentioned reports as well as to our own. As Unit 42 reports, the attacks against entities in the government of Thailand used the “bookworm” trojan.

2017 - July/October:
ProtectWise 401TRG published our own findings and an update on LEAD using open source and public tooling in attacks against Japanese gaming organizations. These attacks are linked with high confidence to ongoing operations in the United States and East Asia.

Other Noteworthy Events:
In 2017, multiple supply-chain attacks occurred which had some similarities to the Winnti umbrella and associated entities. For example, Kaspersky reported on ShadowPad, a large-scale compromise of NetSarang, which resembles the Winnti and PlugX malware. In addition, Kaspersky and Intezer identified notable code similarities to the Winnti umbrella and APT17 in the compromise of Piriform, which

allowed attackers to sign and spread altered versions of the CCleaner software to a large customer base.

Analysis of Attacks on Initial Targets

Throughout 2017 and 2018, ProtectWise 401TRG was involved in a number of detection and incident response engagements with our customers that linked back to the Winnti umbrella and other closely associated entities. Through the analysis of public and private intelligence, we have successfully identified similar attacks, which allow us to assess with high confidence that the details below follow a global attack trend as the Chinese intelligence operations have evolved over time.

2017 Operations:
One of the most common tactics used by the Winnti umbrella and related entities is phishing users whose credentials may provide elevated access to a target network. We have observed spear-phishing campaigns that target human resources and hiring managers, IT staff, and internal information security staff, which are generally very effective.

In 2017 the entity focused most of its efforts around technical job applicant email submissions to software engineering, IT, and recruiting staff, which we originally reported on at our 401trg.pw blog. The phishing lures used multiple languages, including Japanese as in the below example:


From:
Date: 2017/7/
Subject: OSとAndroid アプリの開発担当を応募します~

貴社の募集内容を拝見しました、 主な言語: Object-C,JAVA,Swift,此方はRubyを利用7年,PHPを利用6年
くらいのIOS APP開発経験があります、Android APPの開発は5年、またAWS, Jenkins,Microsoft Azure,ZendFramework環境における開発とスマートフォンアプリ決済処理に関する開発経験もあります、MSSQL,Mysql,Oracle,PostgreSQLも5年利用しています
是非ご覧になってください: http://job./?session=201707

The approximate translation is as follows:

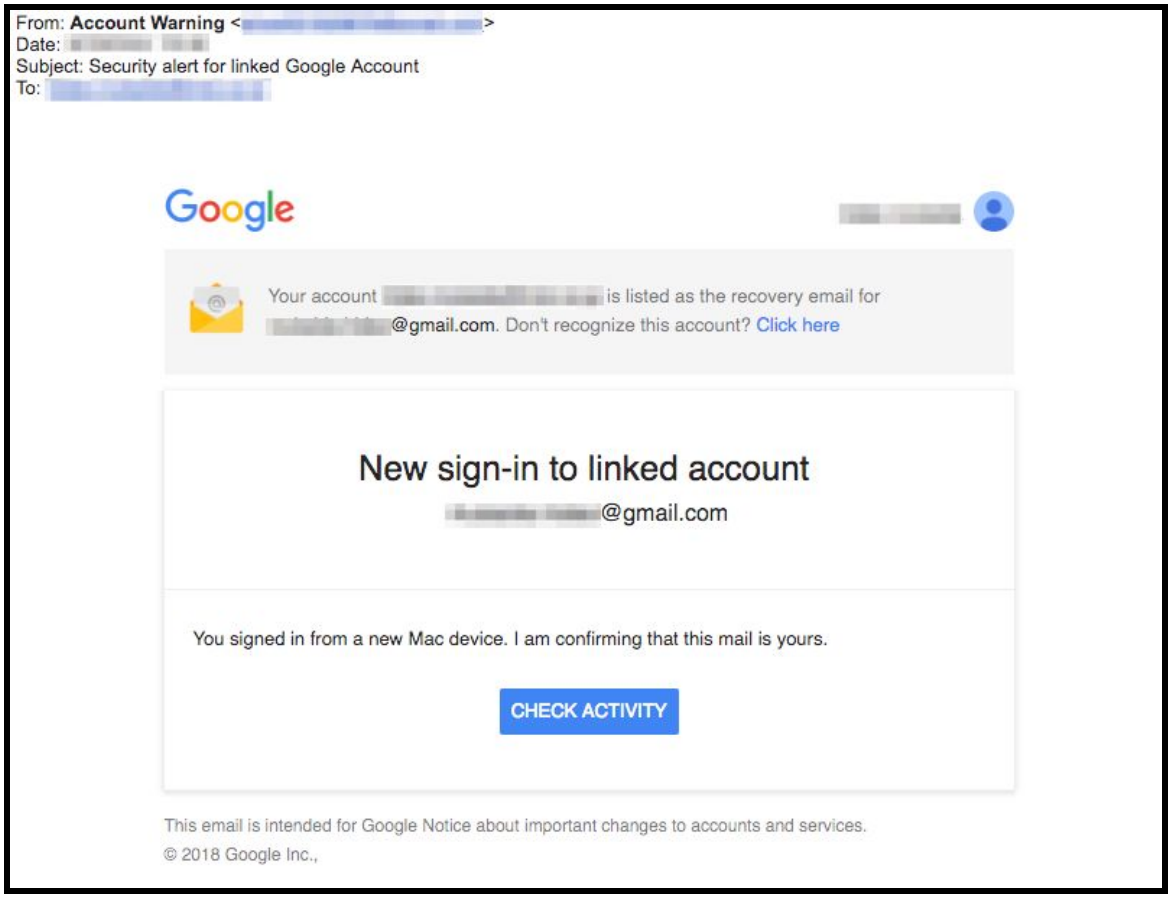
> *I saw your job posting. My main languages are Object-C, JAVA, and Swift, and I have 7 years experience with Ruby and 6 years experience with PHP. I have 5 years experience developing iOS apps, as well as Android apps, AWS, Jenkins, Microsoft Azure, ZendFramework, and smartphone application payment processing. I also have 5 years experience with MSSQL, Mysql, Oracle, and PostgreSQL. Please see here: [malicious link]*

The process that followed a target clicking the malicious link evolved as the attacker progressed through the campaigns. The links consistently sent the victim to a fake resume, but the exact format of that resume changed over time; we have observed resumes being delivered as DOC, XLS, PDF, and HTML files. Once opened, the fake resumes performed various actions in an effort to download malware onto the victim host. During the same time period, we also observed the actor using the Browser Exploitation Framework (BeEF) to compromise victim hosts and download Cobalt Strike. In this campaign, the attackers experimented with publicly available tooling for attack operations. During this infection process, the actor was known to check the target operating system and deliver malware, signed by a previously stolen key, for the appropriate host environment. In some cases, valid Apple certificates stolen from victims were used in this process, which linked the attack to additional victim organizations.

Post-compromise actions by the attacker followed a common pattern. First they attempted to spread laterally in the network using stolen credentials and various reconnaissance efforts, such as manually examining shares and local files. The primary goal of these attacks was likely to find code-signing certificates for signing future malware. The secondary goals of the attackers depended on the type of victim organization, but were often financial. For example, gaming organizations tended to fall victim to manipulation or theft of in-game virtual currencies. Non-gaming victims may have experienced theft of intellectual property such as user or technology data.

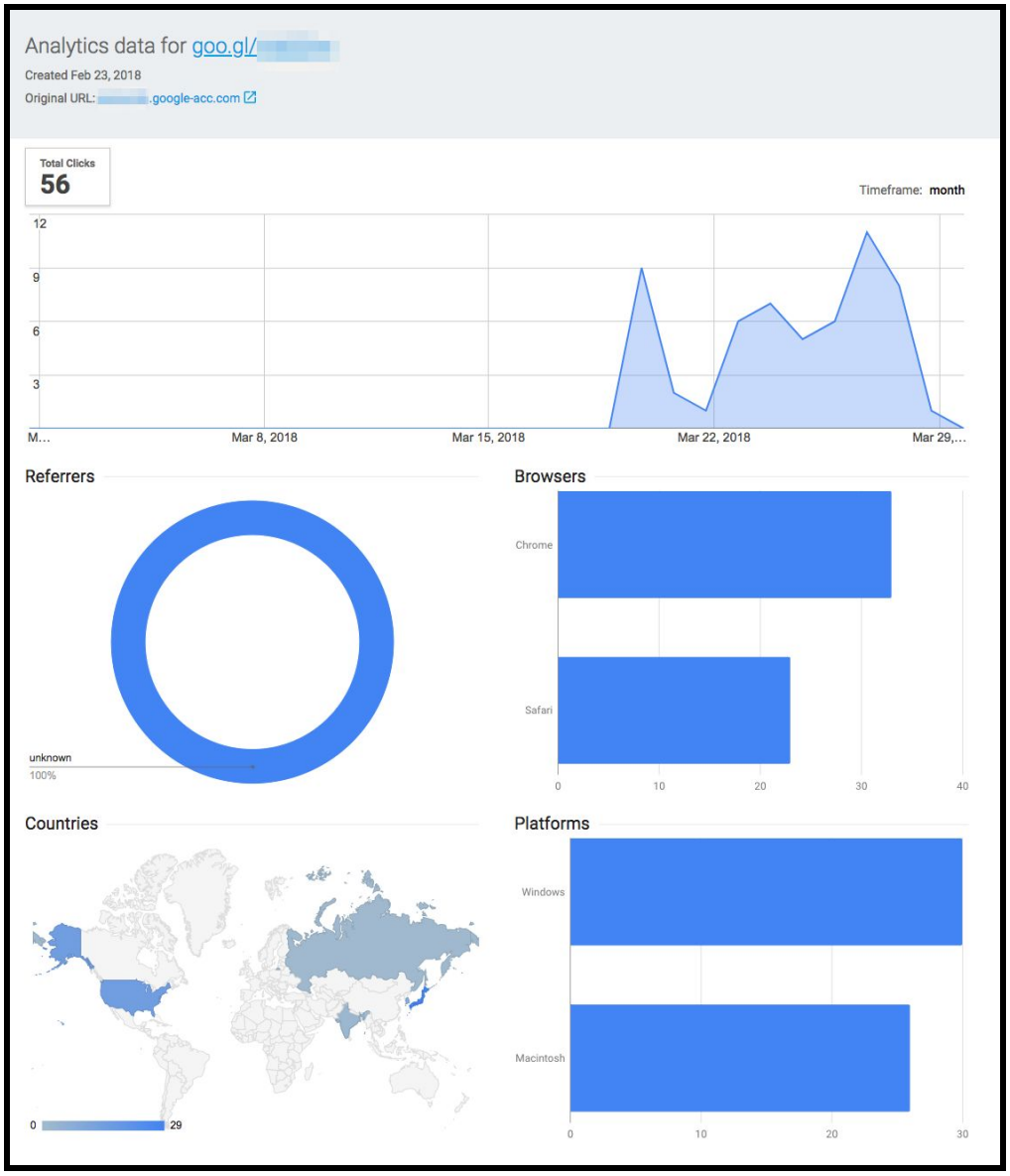
2018 Operations:

More recently, various attack campaigns from the Winnti umbrella and associated groups have been very successful without the use of any exploits or malware. Phishing remains the initial infection vector but the campaign themes have matured. In 2018, the campaigns have largely been focused on common services such as Office 365 and Gmail.



It is important to note that attackers likely have additional information on their target organizations' preferred email solutions based on previous incidents or open source intelligence.

In more recent phishing campaigns conducted by the Winnti umbrella and associated groups, URL shortening services have been used. For example, Google's URL shortening service goo.gl was used over the past weeks, allowing us to gain insight into the scale of this campaign using publicly available analytics.



As you can see from the above screenshot, this particular phishing campaign ran from March 20th to March 28th, 2018. Notably, the link was created on February 23rd, 2018, indicating roughly three weeks of preparation for the attacks. These metrics allow us to gain insight into who clicked the link in a phishing email and was directed to a phishing or malware delivery landing page. According to Google analytics, there were a total of 56 clicks. 29 were from Japan, 15 from the United States, 2 from India, and 1 from Russia. 33 of the clicks were from Google Chrome, and 23 were from Safari. 30 were from Windows OS hosts, and 26 were macOS hosts.

In general, the attackers phish for credentials to a user's cloud storage, and would be expected to later attempt malware delivery in the cases of a failed credential phish or valueless cloud storage.

In cases where the victim uses O365 and/or G-suite for enterprise file storage, the attackers manually review the contents for data of value. If code signing certificates are stored here, the primary mission has been accomplished, as they may be easily downloaded. In other cases, the attackers attempt to use other files and documentation in the cloud storage to help them traverse or gain privileges on the network. The targets in 2018 include IT staff, and commonly sought out files include internal network documentation and tooling such as corporate remote access software.

Once the attackers gain remote access to the network via malware or stolen remote access tooling and credentials, the operation continues as we've seen, though their post-compromise actions have become more efficient and automated. Internal reconnaissance is performed by scanning the internal network for open ports 80, 139, 445, 6379, 8080, 10022, and 30304. The choice of ports by the attacker indicates a strong interest in internal web and file storage services. An interesting addition is the use of 30304, which is the peer discovery port for Ethereum clients.

In the attackers' ideal situation, all remote access occurs through their own C2 infrastructure, which acts as a proxy and obscures their true location. However, we have observed a few cases of the attackers mistakenly accessing victim machines without a proxy, potentially identifying the true location of the individual running the session. In all of these cases, the net block was 221.216.0.0/13, the China Unicom Beijing Network, Xicheng District.

Visualizing Attacker Infrastructure

Based on the various incidents we have been involved in, in addition to past public reporting and open-source intelligence, we can construct a map representing the infrastructure most closely associated with the Winnti umbrella and closely related entities. For the sake of producing an accurate representation of the infrastructure, we are excluding any shared infrastructure (such as hosting provider IPs used for many unrelated domains) and low confidence indicators. Please note this is not an exhaustive list of all active infrastructure in use by the group.

As detailed below, this infrastructure spans at least eight years of activity by the Winnti umbrella and related groups. Please note, as this section heavily references the "Some Key Public Reports" section, above, we recommend reading that first. Indicators are provided in Appendix A.

1. The area of the map labeled #1 is the phishing, malware delivery, fake resume, and C2 infrastructure. This includes domains, IPs, malware hashes, SSL certificates, and WHOIS information. In this section of the infrastructure, we primarily observe the network and file indicators which would be used

against targets valued for code signing certificates, software manipulation, and potential financial manipulation. The indicators detailed in the 2017 & 2018 Initial Target section of this report are located in #1. Infrastructure in this area is currently in use and not entirely historical.

2. This area is a network that we assess is associated with the umbrella with low confidence. The most interesting findings here are the large number of Let's Encrypt SSL certificates in use and the overlap with attacker exclusive infrastructure. This proposed relationship is generated by infrastructure links alone, as no malicious activity has been confirmed to or from region #2. Infrastructure in this area is currently in use and not historical.

3. Area #3 is linked to the initial attack infrastructure (#1) by domain WHOIS details, likely from operational security mistakes. We assess with high confidence that these infrastructures are linked. Based on the lax structure and naming of this section, it is highly probable that it is used for attacker experimenting and development. Some examples include domains such as "nobody.will.know.whoami[.]la", "secret.whoami[.]la", and "no.ip.detect.if.using.ipv6[.]la". Infrastructure in this area is currently in use and not historical.

4. This area has various links to #3 in which an individual software developer is identified. We asses this connection with low to medium confidence and will refrain from publicly sharing details in this report. This area contains many personally operated domains and SSL certificates. Infrastructure in this area is currently in use and not historical.

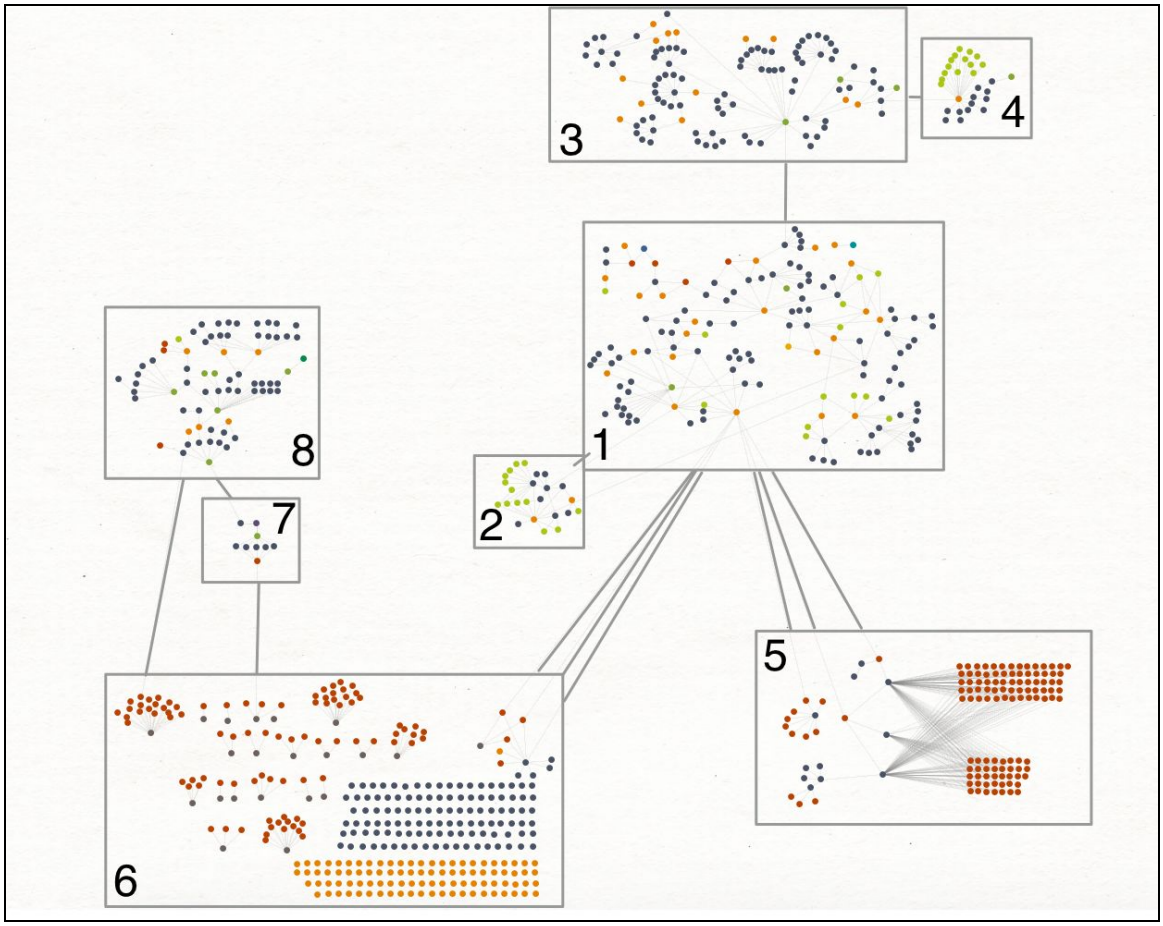
5. Area #5 of the map is part of what Novetta reported on as Operation SMN in 2014. Infrastructure in this area is purely historical and based on Novetta's reporting, which we can link to area #1 via known umbrella infrastructure. The vast majority of indicators in this area are the many associated hashes, combined with their C2 destination domains and IPs.

6. This area of the map is what Cylance reported on as PassCV in 2016. The vast majority of infrastructure and indicators here are stolen code signing certificates, malware signed with the certificates, and C2 domains. This area contains information on many victims of campaigns related to area #1. Infrastructure in this area is historical. We assess that this area is linked to the Winnti umbrella with high confidence.

7. This section represents infrastructure identified by Citizen Lab in their July 5th 2017 reporting on attacks against journalists. As they originally identified, one of the NetWire binaries was signed with a stolen certificate linked to #6,

the Cylance PassCV report. We were able to further expand this section by pivoting off of additional domain WHOIS information.

8. Lastly is area #8, which links back with high confidence to #7 (Citizen Lab reporting) and #6 (PassCV). This area consists of domains, IPs, MD5 file hashes, and further WHOIS operational security mistakes. This area is similar in functionality to #1 and #3, serving as infrastructure for both high-value politically focused attacks and developer personal use. This section links to the online identities of an individual we asses to be associated with the Winnti umbrella or a closely related group at a medium to high confidence. Infrastructure in this area is currently in use and not historical. One example of malicious activity in this area was the document detailing the strengthening of sanctions against North Korea, above. These activities are similar to the type of politically motivated targeted attacks Citizen Lab reported on. Some infrastructure in this area is currently in use and is not completely historical.



Investigative Findings

Based on incident response engagements, research into the associated attacker infrastructure, and previously reported research, we can summarize our findings as follows:

1. The Chinese intelligence apparatus has been reported on under many names, including Winnti, PassCV, APT17, Axiom, LEAD, BARIUM, Wicked Panda, and GREF.

2. The overlap of TTPs and infrastructure between the Winnti umbrella and other groups indicates the use of shared human and technology resources working towards an overarching goal. Operational security mistakes allow the linking of attacks on lower value targets to higher value campaigns. Reuse of older attack infrastructure, links to personal networks, and observed TTPs play a role in this overlap.

3. The attackers behind observed activity in 2018 operate from the Xicheng District of Beijing via the net block 221.216.0.0/13.

4. Initial attack targets are commonly software organizations in the United States, Japan, South Korea, and China. Later stage high profile targets tend to be political organizations or high-value technology companies.

5. The attackers grow and learn to evade detection when possible, but lack operational security when it comes to the reuse of some tooling. Living off the land and adaptability to individual target networks allow them to operate with high rates of success.

Conclusion

We hope the information we've shared in this report will help potential targets and known victims in addition to the greater information security community. Though they have at times been sloppy, the Winnti umbrella and its associated entities remain an advanced and potent threat. We hope that the information contained within this report will help defenders thwart this group in the future.

We'd like to extend a special thank you to all the victims, targets, researchers, and security vendors who have shared their own findings over the years.

Appendix A: Associated Indicators

If you are interested in automating the intake of public 401TRG indicators, we recommend using our github detections repository.

Area #1:

Type	Indicator
IP Address	106.184.5.252
IP Address	106.185.31.128
IP Address	106.186.122.96
IP Address	13.115.93.210
IP Address	133.242.145.137
IP Address	139.162.106.19
IP Address	139.162.119.48
IP Address	139.162.17.161
IP Address	139.162.79.40
IP Address	139.162.95.39
IP Address	159.65.71.30
IP Address	172.104.101.131
IP Address	172.104.115.124
IP Address	198.199.78.207
IP Address	207.126.114.154
IP Address	45.32.18.187
IP Address	45.77.179.192
IP Address	52.199.202.13
IP Address	61.78.62.102
IP Address	61.78.62.21
IP Address	61.78.62.61

Domain	11116[.]intra[.]applestunes[.]com
Domain	24287[.]intra[.]applestunes[.]com
Domain	26707[.]intra[.]applestunes[.]com
Domain	33604[.]intra[.]applestunes[.]com
Domain	account[.]microsoftssonline[.]com
Domain	account[.]micrrosoftsonline[.]com
Domain	account[.]outlook-s[.]com
Domain	accounts[.]gmail[.]sa[.]com
Domain	accounts[.]google-acc[.]com
Domain	accounts[.]google-caches[.]com
Domain	alienlol[.]com
Domain	app[.]appaffect[.]com
Domain	appaffect[.]com
Domain	applestunes[.]com
Domain	applevswin[.]com
Domain	asmc[.]best
Domain	atliassian[.]com
Domain	awsprocduction[.]immigrantlol[.]com
Domain	awsstatics[.]com
Domain	css[.]google-statics[.]com
Domain	dnslog[.]mobi
Domain	eggagent[.]info
Domain	exoticlol[.]com
Domain	ftp[.]appaffect[.]com
Domain	ftp[.]eggagent[.]info
Domain	ftp[.]ssrsec[.]com
Domain	ftp[.]winter[.]tokyo
Domain	gmail[.]sa[.]com
Domain	google-acc[.]com

Domain	google-caches[.]com
Domain	google-searching[.]com
Domain	google-statics[.]com
Domain	googlecloud[.]center
Domain	gstatic[.]guide
Domain	helpdesk[.]access[.]ly
Domain	id[.]atliassian[.]com
Domain	immigrantlol[.]com
Domain	intra2015[.]awsstatics[.]com
Domain	job[.]yoyakuweb[.]technology
Domain	jobcenters[.]com
Domain	jobscenters[.]org
Domain	k0oo[.]co
Domain	login[.]gmail[.]sa[.]com
Domain	login[.]microsoftssonline[.]com
Domain	login[.]micrrosoftsonline[.]com
Domain	macos[.]exoticlol[.]com
Domain	mail[.]appaffect[.]com
Domain	mail[.]atliassian[.]com
Domain	mail[.]awsstatics[.]com
Domain	mail[.]google-acc[.]com
Domain	mail[.]google-caches[.]com
Domain	mail[.]microsoftssonline[.]com
Domain	mail[.]micrrosoftsonline[.]com
Domain	mail[.]mondoor[.]tv
Domain	mail[.]outlook-s[.]com
Domain	mail[.]ssrsec[.]com
Domain	mail[.]winter[.]tokyo
Domain	martianlol[.]com

Domain	microsoftsec[.]com
Domain	microsoftssonline[.]com
Domain	mondoor[.]tv
Domain	ns1[.]google-searching[.]com
Domain	ns2[.]googlecloud[.]center
Domain	outerlol[.]com
Domain	outlook-s[.]com
Domain	proappcs[.]com
Domain	rabbit[.]awsstatics[.]com
Domain	resume[.]immigrantlol[.]com
Domain	snow[.]winter[.]tokyo
Domain	sqlmapff[.]com
Domain	sshsocks[.]google-searching[.]com
Domain	ssl[.]gmail[.]sa[.]com
Domain	ssl[.]google-acc[.]com
Domain	ssl[.]google-caches[.]com
Domain	ssrsec[.]com
Domain	strangelol[.]com
Domain	summer[.]winter[.]tokyo
Domain	support[.]theonelogin[.]com
Domain	theonelogin[.]com
Domain	vmxesxi[.]google-searching[.]com
Domain	vps2java[.]securitytactics[.]com
Domain	winter[.]tokyo
Domain	www5363uj[.]sakura[.]ne[.]jp
Domain	yoyakuweb[.]technology
SSL Cert SHA1	512509787e4da7aaf71b89d25698a9e9d43501fd
SSL Cert SHA1	bd3abf19f065d102503e9186c152e529d3e33143
SSL Cert SHA1	df7826303b98004afd1102f597f6c7b067086a00

SSL Cert SHA1	1217cbb57fb26bd52d976f34571bd6c6514265e9
SSL Cert SHA1	e6a3b45b062d509b3382282d196efe97d5956ccb
SSL Cert SHA1	8e400380e376b9fb03612967940bb8e07175ab6a
SSL Cert SHA1	263babc25c177e0e6bd87c687bad8316240f971e
SSL Cert SHA1	58e1a9c1dae311fabdfa065955216a46eecb5816
SSL Cert SHA1	bae30b15dbb1544cf194d076b75b7bb9e3d6b760
SSL Cert SHA1	0e34141846e7423d37f20dc0ab06c9bbd843dc24
SSL Cert SHA1	23d57a493a5bfe1801b9d6e0894555242661a27b
SSL Cert SHA1	8e11362a487a744fd21682cd86ad053e8bd5b9ce
File MD5 Hash	b676ec7b387de8795833b691a367d3d1
File MD5 Hash	e798cfe49e6afb61f58d79a53f06d785
File MD5 Hash	371acda8d719426b6a8867767260b9ce
Cookie	_phishing-framework_session
WHOIS Email	haveip2015@gmail[.]com
WHOIS Email	iisexit@gmail[.]com

Area #2:

Type	**Indicator**
IP Address	52.199.171.117
IP Address	118.243.177.54
Domain	y177054.ppp.asahi-net.or[.]jp
Domain	newsite.parakaro.co[.]jp
Domain	www.hyper.parakaro.co[.]jp
Domain	office.parakaro.co[.]jp
Domain	hyper.parakaro.co[.]jp
Domain	peq.parakaro.co[.]jp
Domain	next.parakaro.co[.]jp
Domain	ftp.parakaro.co[.]jp

Domain	parakaro.co[.]jp
SSL Cert SHA1	12eb8a9f1a7cd1cc10e57847dd5476c6062b9e58
SSL Cert SHA1	8df0b63fbdd9616d581bdb101929eb17f80f9e99
SSL Cert SHA1	92a1c7e1fd5afccd957e7fcbcdd2431eb9bf3d50
SSL Cert SHA1	a22d97e4ede82ae8375522aca59db575d08c5c35
SSL Cert SHA1	ddf115821717dabb5e69c753d27460242204031e
SSL Cert SHA1	5e0fa58bf1c4c1b63144052063dc2bb9129aa1f3
SSL Cert SHA1	c3e55bd6fe0205fe7dc1ad53ed03db269ba5da71
SSL Cert SHA1	1cc87c7c900d584400c5c82073672888fefb145e
SSL Cert SHA1	ca2854658dff72da77bf82c1fe5899d09f9f559d
SSL Cert SHA1	93caf237baa37cd42dfc4653ffc1792fcbad4642
SSL Cert SHA1	aff17a2e1969e4bf81dbaa3591778887546570cb
SSL Cert SHA1	3f3da327ca330396f1ab0a543be284f85d9d414a

Area #3:

Type	Indicator
IP Address	119.29.157.220
IP Address	207.126.114.133
IP Address	207.126.114.136
IP Address	207.126.114.158
IP Address	207.126.114.161
IP Address	207.126.114.163
IP Address	208.185.83.234
IP Address	208.185.83.241
IP Address	208.185.83.248
IP Address	208.185.92.31
IP Address	208.185.92.62
IP Address	42.51.17.180

IP Address	64.125.185.106
Domain	117[.]89[.]65[.]117[.]ipv6[.]la
Domain	address[.]ipv6[.]la
Domain	anonymous[.]ipv6[.]red
Domain	be[.]loved[.]tokyo
Domain	bless[.]christmas
Domain	blessed[.]loved[.]tokyo
Domain	channel-w[.]in
Domain	cisco[.]ipv6[.]la
Domain	colour[.]of[.]girls[.]is[.]violet[.]la
Domain	cute[.]devil[.]tokyo
Domain	devil[.]tokyo
Domain	diamond[.]violet[.]la
Domain	didin[.]asia
Domain	doyan[.]party
Domain	enjoy[.]and[.]loved[.]tokyo
Domain	ertiga[.]org
Domain	freak[.]pictures
Domain	ftp[.]devil[.]tokyo
Domain	ftp[.]ipv6[.]red
Domain	ftp[.]loved[.]tokyo
Domain	ftp[.]newbie[.]red
Domain	gadget[.]newbie[.]red
Domain	happy[.]bless[.]christmas
Domain	hidden[.]ipv6[.]red
Domain	huhaifan[.]com
Domain	i[.]loved[.]tokyo
Domain	ipv4[.]ipv6[.]la
Domain	ipv6[.]la

Domain	ipv6[.]red
Domain	irc[.]devil[.]tokyo
Domain	joy[.]full[.]bless[.]christmas
Domain	just[.]a[.]newbie[.]red
Domain	katanya[.]rame[.]yah[.]di[.]channel[.]violet[.]la
Domain	like[.]violet[.]la
Domain	loved[.]tokyo
Domain	loved[.]tokyo
Domain	loving[.]and[.]being[.]loved[.]tokyo
Domain	loving[.]and[.]being[.]loved[.]tokyo
Domain	ludicrous[.]lol
Domain	mail[.]bless[.]christmas
Domain	mail[.]devil[.]tokyo
Domain	mail[.]ipv6[.]la
Domain	mail[.]ipv6[.]red
Domain	mail[.]loved[.]tokyo
Domain	mail[.]multicons[.]net
Domain	mail[.]newbie[.]red
Domain	mail[.]nteng[.]xyz
Domain	mail[.]violet[.]la
Domain	mail[.]whoami[.]la
Domain	multicons[.]net
Domain	my[.]pal[.]violet[.]la
Domain	naoteng[.]top
Domain	naotengml[.]xyz
Domain	newbie[.]red
Domain	no[.]ip[.]detect[.]if[.]using[.]ipv6[.]la
Domain	nobody[.]will[.]know[.]whoami[.]la
Domain	nteng[.]xyz

Domain	on-line[.]connection[.]violet[.]la
Domain	packet[.]ipv6[.]la
Domain	people[.]do[.]not[.]need[.]to[.]be[.]fixed[.]they[.]need[.]to[.]be[.]loved[.]tokyo
Domain	percuma[.]berteman[.]sama[.]newbie[.]red
Domain	psycho[.]red
Domain	pure[.]newbie[.]red
Domain	pv6[.]red
Domain	rosemarry[.]asia
Domain	secret[.]whoami[.]la
Domain	sekarang[.]waktunya[.]pake[.]ipv6[.]red
Domain	silent[.]whoami[.]la
Domain	sky[.]violet[.]la
Domain	teng123[.]top
Domain	ti[.]vengo[.]sul[.]perizoma[.]ipv6[.]la
Domain	top106[.]top
Domain	uhh[.]yeah[.]whoami[.]la
Domain	ultra[.]violet[.]la
Domain	using[.]ipv6[.]la
Domain	violet[.]la
Domain	whoami[.]la
Domain	xops[.]violet[.]la
WHOIS Email	18277225531@163[.]com
WHOIS Email	253125567@qq[.]com
WHOIS Email	ykcrewz@yahoo[.]com

Area #5:

Type	Indicator
Domain	toya[.]co[.]kr
Domain	war[.]eatuo[.]com
Domain	war[.]geekgalaxy[.]com
Domain	war[.]webok[.]net
Domain	war[.]winxps[.]com
Domain	winxps[.]com
Domain	mail[.]winxps[.]com
Domain	ad1[.]winxps[.]com
Domain	69f319a6-10c4-4792-9caf-ec3b3c4b5314[.]winxps[.]com
MD5 File Hash	013cd79973f9e26cd86719a988227c0c
MD5 File Hash	031cb00db70f12ba917cd5675658f2c7
MD5 File Hash	07f33ec44f655fe5386b342a10ae48a6
MD5 File Hash	0810959693b40e9b61046f594f86bdb4
MD5 File Hash	095cd159b460d9232123cadfa3670158
MD5 File Hash	0ae61e7f2dd01e6293b9df2e2787caca
MD5 File Hash	0b6019cb7d872112837e3459266e1337
MD5 File Hash	0c5861504dd9156b601c0db63eebaf52
MD5 File Hash	0e7c4616c04c1a200a95b908ecd70027
MD5 File Hash	0f8a8eaf95c7b3b5d9b60a73140fc2bb
MD5 File Hash	108137d380650c99a682077255e95418
MD5 File Hash	12c8dfe94914c793c8a72b024d9334f6
MD5 File Hash	14a9d379d3b16146ac58bc1fd0f3561a
MD5 File Hash	15c700bc1e4ec53af996f5628e97a541
MD5 File Hash	15d909f3761b4ed5b85428bea971fc3b
MD5 File Hash	16406aeff6ded69b102b7442324bcd37
MD5 File Hash	1670b57851c73813cb17479b302f84c0

MD5 File Hash	171ffa1fb15a298bcca8d8108fe913a9
MD5 File Hash	18b2e353c4628013c27aa1528cd7bd9c
MD5 File Hash	1c1157f3fbd1587527e5ade92f8f2f7f
MD5 File Hash	1caa2b7cc66d901994a0893baecd2e06
MD5 File Hash	1ec70a07ec2aa63ba568160d22a78611
MD5 File Hash	270bba9ad5d6a8cf7e828870e4ae323f
MD5 File Hash	28c3fa62b1f6a9baf71e18d78d0b97ca
MD5 File Hash	2a312a7fcd5fd20e4a50e73b6b9c93de
MD5 File Hash	33d385520a2677cb4232d25fdd49407f
MD5 File Hash	3af5259a62cd4fd5ff0df1a54478997e
MD5 File Hash	3b56e91ed28d1bef96ee80ebb7ec90a3
MD5 File Hash	3beaa003e5e1eaf60fe18c7a5b039a62
MD5 File Hash	3f0649854d60a43ef8bea236a0eecee2
MD5 File Hash	3f3f0205a6526fc87a23a4e123e55d55
MD5 File Hash	41b0e32592c9f846915d2452d1cab758
MD5 File Hash	43fec0660c9e28ac046c0ffa8c987ed9
MD5 File Hash	44c4afc43c0be6b8710226e64d3b58f9
MD5 File Hash	459323ec0efc8d4e0f7c4908e08035fd
MD5 File Hash	4617b5821d3d378addf68450ca6db761
MD5 File Hash	49984ae27318351a541fae53522d3bef
MD5 File Hash	49b1ca0752d166c2cc5e04cbab8b71ee
MD5 File Hash	5042398cd279b93c2b76a3d0e78b5887
MD5 File Hash	5048a96b8a0abb9dc9c068e16373598b
MD5 File Hash	54a0136213c408a489b9a158d1dcc5de
MD5 File Hash	5620be18199c15296f3b23ba5831e2d4
MD5 File Hash	5747b40d886fb05e5e05298549c9caa5
MD5 File Hash	5a44818722a4f61602c9490012a8658e
MD5 File Hash	5ad07321baed16a6d1187169c3160df4
MD5 File Hash	5c7828e1f193ef222b083c6ef8c888f6

MD5 File Hash	5ed62492675e5577f5df02b349339195
MD5 File Hash	603854698d11963ae116bc735a8b40ca
MD5 File Hash	6275219b8a353f7e093c7dd2e9301567
MD5 File Hash	6513d8c68a32d6989b637d1e827f2c11
MD5 File Hash	65e4bd4dddd164e3f331d677922ee288
MD5 File Hash	68af93fd6d813c4110ad7850ed027b69
MD5 File Hash	6eefa1529bcf192f7ccea1f5aeefe707
MD5 File Hash	6f4ce475c83bbb9890c3180973a2f75b
MD5 File Hash	71f0e9068a8d3f9a81aecccad7571535
MD5 File Hash	73497bb006c082008a49c09fbcdc7787
MD5 File Hash	740249492922bf531821692b4c23498e
MD5 File Hash	74ec010ca8ff895b1ab801a03e6282bb
MD5 File Hash	75c775cbfaf9bd40c504c3737e93fafd
MD5 File Hash	7b218f72c4baf98673340cf4789ec012
MD5 File Hash	7b6ca860c3e6bdc75b0be26db70a603a
MD5 File Hash	8674e3c77e8051cfdf1c4d321a7188bf
MD5 File Hash	86fd00eb911c241c9367bf0d4c079300
MD5 File Hash	8b2db1c9d8ba805d5a310910fd6aff7d
MD5 File Hash	8e3e4b006af3c1835ef3b7b4dcd3f1de
MD5 File Hash	8e4a973b7440e8bb3f6d272660d6c06d
MD5 File Hash	92274d90c221b0aad382f816026a4781
MD5 File Hash	953c183445b67059e2a2378f8d1b6709
MD5 File Hash	97734c735b031143a3347fb89915f477
MD5 File Hash	98a073e1e545075aa0030995cc07745a
MD5 File Hash	9d77a9318c53affe7c170710644491fe
MD5 File Hash	9e3b5b7988c0307a60b9a2c15161c1ff
MD5 File Hash	9ec4bc6990635c847d95271bf8c77794
MD5 File Hash	a0aaf3c9d5f30645453953cb2bb87f3f
MD5 File Hash	a16bb004efb227cb1686d7051c409e42

MD5 File Hash	a22af4fc7fe011069704a15296634ca6
MD5 File Hash	ad48e2b0520b1deb70e0ecd32ffca96a
MD5 File Hash	af30fca836142d6a0b8672f1e8f53acf
MD5 File Hash	b07cf2bb96ccebfe563c6c8f7046143a
MD5 File Hash	b38b2eae598ee1f5204ef5198d16dcdf
MD5 File Hash	b68cab0a6da7244532c051073c8ba2f3
MD5 File Hash	b6e2518f9c9028e9bf452551637ed2ae
MD5 File Hash	b714e63b420932b63ec4db269fba8689
MD5 File Hash	b745534a50459b4950ef8cefd9f0a078
MD5 File Hash	b9c4386e1b32283598c1630be5a12503
MD5 File Hash	bb775b77c3a546fa432264a142c24a3d
MD5 File Hash	bea51d525ee6ea6d4272c7adc23dfb7d
MD5 File Hash	bffc195107e60a7ea58e44125df33dc6
MD5 File Hash	c202654790c1e7321fdcb9604d5d5221
MD5 File Hash	c3f45d748021f8a9acbf00fdc3cfcd6b
MD5 File Hash	c8bc4425a6953c09f23a7e5d4333988c
MD5 File Hash	ce96cb57fde2ec600f9549f73acfd6bb
MD5 File Hash	cfb08ee3399604d37470797d49c01f72
MD5 File Hash	d0e6ddf740f811d823193ccc67afccb0
MD5 File Hash	d1cdff47853aae8fd697e569a0897d5e
MD5 File Hash	d31e57fcb728a4f36e21764b164a9e57
MD5 File Hash	d661dc2ad44bd056f7ca292727007693
MD5 File Hash	db01783710e0c5aff92156a0e76deade
MD5 File Hash	db68a610468969288cea1b845b38789f
MD5 File Hash	dc38409bb31c27f90a780c0546139cbb
MD5 File Hash	de82407423aadb8009e378e406515c92
MD5 File Hash	e244f2d62ae2b0b0db324e4586dc860d
MD5 File Hash	e49a27232b010e51124d98926122503f
MD5 File Hash	e5d73a4ed51e05968869ebb9506b3338

MD5 File Hash	e64ce6079f46bf98c213d967f1994d43
MD5 File Hash	e64d1b662f98aa977e0dbb424b2c344d
MD5 File Hash	ea4babbd8f7c614f51c2bec44c8267a3
MD5 File Hash	eb272fe923ccf3e66fde1bf309cbc464
MD5 File Hash	eb94043d9fe8cf170b016e243f1188b1
MD5 File Hash	ec2be7eeb812d87e9c995542dbd8f064
MD5 File Hash	ef1b7fd90b274d872ee15a3f2ca35193
MD5 File Hash	efac2baa9941d9a066256bdbbf20e080
MD5 File Hash	F11b3dc0c2818931e0bfe5c0b9fafe05
MD5 File Hash	F34567a507b8d531c31be32f354e234e
MD5 File Hash	F765686eed32f57071762fadd32b8b6d
MD5 File Hash	Feea14f4bba2326a8d9b0baca0ee5a5e
MD5 File Hash	F8a3b026f90a3b33f11fe850c870b063

Area #6:

Type	Indicator
IP Address	101.55.33.106
IP Address	101.55.64.183
IP Address	101.55.64.209
IP Address	101.55.64.246
IP Address	101.55.64.248
IP Address	101.79.124.251
IP Address	101.79.124.254
IP Address	103.24.152.18
IP Address	103.25.9.191
IP Address	103.25.9.193
IP Address	103.25.9.194
IP Address	103.25.9.195

IP Address	103.25.9.200
IP Address	103.25.9.202
IP Address	103.25.9.240
IP Address	103.25.9.241
IP Address	103.25.9.242
IP Address	103.25.9.244
IP Address	103.28.46.79
IP Address	103.56.102.9
IP Address	104.199.139.211
IP Address	106.10.64.250
IP Address	113.10.168.162
IP Address	113.30.103.103
IP Address	113.30.123.254
IP Address	113.30.70.209
IP Address	113.30.70.216
IP Address	113.30.70.238
IP Address	113.30.70.254
IP Address	115.23.172.113
IP Address	116.31.99.65
IP Address	118.123.19.9
IP Address	118.123.229.22
IP Address	118.130.152.246
IP Address	119.63.38.210
IP Address	121.156.56.114
IP Address	121.54.169.39
IP Address	122.226.186.28
IP Address	122.49.105.16
IP Address	123.1.178.39
IP Address	123.249.7.226

IP Address	123.249.81.202
IP Address	14.29.50.66
IP Address	150.242.210.149
IP Address	150.242.210.15
IP Address	150.242.210.160
IP Address	150.242.210.161
IP Address	150.242.210.187
IP Address	150.242.210.195
IP Address	175.126.40.21
IP Address	180.210.43.134
IP Address	182.161.100.3
IP Address	182.237.3.60
IP Address	182.252.230.254
IP Address	183.60.106.205
IP Address	183.86.194.10
IP Address	183.86.194.16
IP Address	183.86.194.42
IP Address	183.86.194.92
IP Address	183.86.211.134
IP Address	183.86.218.167
IP Address	183.86.218.169
IP Address	183.86.218.170
IP Address	184.168.221.40
IP Address	184.168.221.64
IP Address	184.168.221.86
IP Address	192.225.226.74
IP Address	192.74.232.8
IP Address	192.74.237.164
IP Address	199.15.116.59

IP Address	199.15.116.61
IP Address	199.83.51.25
IP Address	202.153.193.90
IP Address	210.209.116.62
IP Address	210.4.223.134
IP Address	211.39.141.23
IP Address	211.44.42.53
IP Address	218.234.76.75
IP Address	19.135.56.175
IP Address	222.186.58.117
IP Address	23.252.164.156
IP Address	23.252.164.238
IP Address	27.255.64.94
IP Address	42.121.131.17
IP Address	45.114.9.206
IP Address	45.125.13.227
IP Address	45.125.13.247
IP Address	58.64.203.13
IP Address	61.111.3.101
IP Address	61.36.11.112
IP Address	69.56.214.232
IP Address	98.126.107.249
IP Address	98.126.193.223
IP Address	98.126.91.205
Domain	115game[.]com
Domain	1songjiang[.]info
Domain	3389[.]hk
Domain	360[.]0pengl[.]com
Domain	360antivirus[.]net

Domain	64[.]3389[.]hk
Domain	amd-support[.]com
Domain	auth[.]ncsoft[.]to
Domain	baidusecurity[.]net
Domain	bak[.]timewalk[.]me
Domain	blog[.]unitys3d[.]com
Domain	bot[.]1songjiang[.]info
Domain	bot[.]360antivirus[.]org
Domain	bot[.]duola123[.]com
Domain	bot[.]eggdomain[.]net
Domain	bot[.]fbi123[.]com
Domain	bot[.]fengzigame[.]net
Domain	bot[.]godaddydns[.]net
Domain	bot[.]ibmsupport[.]net
Domain	bot[.]itunesupdate[.]net
Domain	bot[.]jjevil[.]com
Domain	by[.]dns-syn[.]com
Domain	cloud[.]0pendns[.]org
Domain	cloud[.]amd-support[.]com
Domain	cloud[.]dellassist[.]com
Domain	dark[.]anonshell[.]com
Domain	dns-syn[.]com
Domain	dns[.]0pengl[.]com
Domain	dns[.]360antivirus[.]org
Domain	dns[.]eggdomain[.]net
Domain	dns[.]godaddydns[.]net
Domain	down[.]fengzigame[.]net
Domain	eggdomain[.]net
Domain	fengzigame[.]net

Domain	fk[.]duola123[.]com
Domain	free[.]amd-support[.]com
Domain	global[.]ncsoft[.]to
Domain	godaddydns[.]com
Domain	gzw[.]3389[.]hk
Domain	help[.]0pengl[.]com
Domain	hijack[.]css2[.]com
Domain	home[.]ibmsupports[.]com
Domain	images[.]iphone-android-mobile[.]com
Domain	intelrescue[.]com
Domain	ios[.]0pengl[.]com
Domain	iphone-android-mobile[.]com
Domain	itunesupdate[.]net
Domain	jj[.]aresgame[.]info
Domain	jj[.]duola123[.]com
Domain	jj[.]fbi123[.]com
Domain	kasperskyantivirus[.]net
Domain	kp[.]css2[.]com
Domain	kuizq[.]ddns[.]info
Domain	lin[.]0pengl[.]com
Domain	lin[.]0penssl[.]com
Domain	linux[.]cocoss2d[.]com
Domain	linux[.]css2[.]com
Domain	linux[.]unitys3d[.]com
Domain	ls[.]0pendns[.]org
Domain	m[.]css2[.]com
Domain	m[.]unitys3d[.]com
Domain	mail[.]iphone-android-mobile[.]com
Domain	mzx[.]jjevil[.]com

Domain	new[.]dns-syn[.]com
Domain	news[.]0pengl[.]com
Domain	news[.]eggdomain[.]net
Domain	nokiadns[.]com
Domain	ns1[.]0pendns[.]org
Domain	ns1[.]amd-support[.]com
Domain	ns1[.]appledai1y[.]com
Domain	ns1[.]dellassist[.]com
Domain	ns1[.]nokiadns[.]com
Domain	ns2[.]0pendns[.]org
Domain	ns8[.]0pendns[.]org
Domain	ns9[.]amd-support[.]com
Domain	ns9[.]nokiadns[.]com
Domain	nss[.]aresgame[.]info
Domain	qqantivirus[.]com
Domain	rk[.]mtrue[.]com
Domain	rk[.]mtrue[.]net
Domain	roboscan[.]net
Domain	root[.]godaddydns[.]net
Domain	rus[.]css2[.]com
Domain	sale[.]ibmsupport[.]cc
Domain	sc[.]0pengl[.]com
Domain	sc[.]0penssl[.]com
Domain	sc[.]dellrescue[.]com
Domain	sc[.]dns-syn[.]com
Domain	sdfsd[.]iphone-android-mobile[.]com
Domain	smtp[.]iphone-android-mobile[.]com
Domain	ssl[.]0pengl[.]com
Domain	ssl[.]0penssl[.]com

Domain	support[.]godaddydns[.]cc
Domain	support[.]godaddydns[.]net
Domain	task[.]dns-syn[.]com
Domain	test[.]dellassist[.]com
Domain	udp[.]jjevil[.]com
Domain	udp[.]timewalk[.]me
Domain	up[.]roboscan[.]net
Domain	update[.]0pengl[.]com
Domain	update[.]360antivirus[.]net
Domain	update[.]css2[.]com
Domain	update[.]fengzigame[.]net
Domain	update[.]nortonantivir[.]us
Domain	update[.]qqantivirus[.]com
Domain	w[.]cocoss2d[.]com
Domain	waw[.]cocoss2d[.]com
Domain	waw[.]css2[.]com
Domain	waw[.]unitys3d[.]com
Domain	wsus[.]kasperskyantivirus[.]net
Domain	www[.]eggdns[.]com
Domain	www[.]iantivirus[.]us
Domain	yang[.]0pendns[.]org
Domain	zx[.]3389[.]hk
Domain	zx[.]css2[.]com
Domain	zx[.]duola123[.]com
MD5 File Hash	011858556ad3a5ef1a6bbc6ad9eaae09
MD5 File Hash	027eb2cda9f1c8df00e26641ce4ef12d
MD5 File Hash	045fd6e98a51a3c4e55a99bb6696f4de
MD5 File Hash	04dc04a1a61769f33b234ad0f19fdc53
MD5 File Hash	11898306703dcbeb1ca2cd7746384829

MD5 File Hash	15ce067a4d370afae742db91646d26ee
MD5 File Hash	175c7694d32191091334e20509a7b2c0
MD5 File Hash	1826efb7b1a4f135785ccfc8b0e79094
MD5 File Hash	19e137dc5974cfad5db62f96e3ba9fd1
MD5 File Hash	1fee79f50848493f08c5e5736594dab2
MD5 File Hash	218b1cd127a95a107dbaf4abe001d364
MD5 File Hash	22de97c025f3cc9ad3f835d97b0a7fab
MD5 File Hash	231257eb290ad0335ebf4556f156fc68
MD5 File Hash	254d87bdd1f358de19ec50a3203d771a
MD5 File Hash	276aaea14d125f69fe7e80e5a30180d7
MD5 File Hash	285a2e9216dbf83edf5ef12ba063a511
MD5 File Hash	28af0e2520713b81659c95430220d2b9
MD5 File Hash	2ea30517938dda8a084aa00e5ee921f6
MD5 File Hash	30498006ce28019ec4a879484d67a6b4
MD5 File Hash	37bb8eacc454aa619ef35e8d82ae85bd
MD5 File Hash	37c37e327a766a1b2db2fb9c934ff16e
MD5 File Hash	3a9503ce79a0ac3b6f2f38163d55554d
MD5 File Hash	47a69704566f37e8626bb8bb5fa784c8
MD5 File Hash	485ca8d140169ebbc8e5b3d7eaed544f
MD5 File Hash	48c21badebacdc9239416a9848b4855c
MD5 File Hash	494bedc21836a3323f88717066150abf
MD5 File Hash	50f7c822562c1213d244e1389d3895c8
MD5 File Hash	527bfd801206c4b382487320ce2a245e
MD5 File Hash	5919b59b61b3807b18be08a35d7c4633
MD5 File Hash	5a69a3d1520260bea2c34adf3cb92c03
MD5 File Hash	6103f34ec409f99762e9c3714dfa1262
MD5 File Hash	6255f40b4000abad8b9e795280fddfd1
MD5 File Hash	66f915ebdde2f98e2f802a52f1a4e85e
MD5 File Hash	6e4846b1029fed9118bbfaa0bd66f0a9

MD5 File Hash	70e41bc5daa6ff811317afef75498062
MD5 File Hash	71f8fb73be84e3d5045d4cfbf7ed4f53
MD5 File Hash	727dfef3918db48b9922ac75796aed55
MD5 File Hash	72b1bfaf65ad9ec596860c1ea3bfb4cc
MD5 File Hash	75b713b8d54403c51317679b4038a6ff
MD5 File Hash	76c9bce4beb37cc8c00a05f3efafe89a
MD5 File Hash	773afaa800f539ce195540e2f1882270
MD5 File Hash	7c086172be6d1eed7fd65a1a4a8df59f
MD5 File Hash	7d673e07393b45960e99b14bd2ebce77
MD5 File Hash	8349691b6c37d9e5fa75ee6365b40bf5
MD5 File Hash	840b05e6fefc3ce01bb181e0454c6bf5
MD5 File Hash	88d2b57c8bf755c886b1bf30a4be87eb
MD5 File Hash	8a8ee6f199438776f6842aab67fb953d
MD5 File Hash	8a8f14c3513b3e14bc57a7ac111341e3
MD5 File Hash	8cb10b202c47c41e1a2c11a721851654
MD5 File Hash	8d20017f576fbd58cce25637d29826ca
MD5 File Hash	8eabdff3d7d6bd826c109a37b10b218b
MD5 File Hash	905fd186adf773404041648fec09f13e
MD5 File Hash	9b06c85682f8486d665f481e56ad65c7
MD5 File Hash	a445d0bfafe5947492e4044cb49eda13
MD5 File Hash	a4c07dbaa8ce969fd0f347d01776d03b
MD5 File Hash	a765a20055059148af311023c95b9239
MD5 File Hash	a7b7b485c266605e219ea185292443c8
MD5 File Hash	a9f392eee93215109b2afc0c887128dc
MD5 File Hash	aaee989b391dea8163ce5a0d6f55b317
MD5 File Hash	ace2ace58cc68db21c38b43a0182fc8b
MD5 File Hash	b15f9a6a0d6a5e52abc7a8134f856949
MD5 File Hash	b5e7832464bff54896b1d42a76760dbc
MD5 File Hash	c176286e35c0629ea526e299c369dc6e

MD5 File Hash	c1d4b96374cfe485179b547ebacc1ee1
MD5 File Hash	c214dc7763e98f2744dd5e7a44e80bba
MD5 File Hash	c3869609968c97fd27e3dc71f26d98d3
MD5 File Hash	c4db0ac33c0676bd3633ac030111192c
MD5 File Hash	c91efaa99a5d9c51dfe86ea286fab519
MD5 File Hash	cbcff0eb404183902457332e72915d07
MD5 File Hash	cd82d1dc730eb9e7e19802500417e58a
MD5 File Hash	cf1d926f21bf93b958b55a43ee5317dc
MD5 File Hash	d1eac0815f7244e799cf0883aab8ec3d
MD5 File Hash	d3bf38bcf3a88e22eb6f5aad42f52846
MD5 File Hash	d4bc7b620ab9ee2ded2ac783ad77dd6d
MD5 File Hash	d73d232a9ae0e948c589148b061ccf03
MD5 File Hash	db60f645e5efcb872ff843a696c6fe04
MD5 File Hash	dc0fccad4972db4cf6cb85a4eabe8087
MD5 File Hash	de7d2d4a6b093365013e6acf3e1d5a41
MD5 File Hash	dee54d45b64fc48e35c80962fb44f73f
MD5 File Hash	dfee3a4e1a137eda06e90540f3604ecb
MD5 File Hash	e32dc66f1337cb8b1ed4f87a441e9457
MD5 File Hash	e4192340a54d73dca73685ce999dc561
MD5 File Hash	e61a40e9ddccc2412435d2f22b4227c2
MD5 File Hash	e72a55235a65811e4afe31b857c5294d
MD5 File Hash	eaaa0408c3cd686a30871fedf31ce241
MD5 File Hash	f1059405feaaae373c59860fdec66fd0
MD5 File Hash	f2449ecf637a370b6a0632a4b45cd554
MD5 File Hash	f2a0df6b2a8de26d2f6e86ec46683808
MD5 File Hash	f3917d618a37342eadfee90f8539b3b9
MD5 File Hash	fc650a1292ade32e41d3fdc2fb7dd3f3
MD5 File Hash	fcec72d588c1cdd03361a334f29c125b
MD5 File Hash	fe9971fe78f3bc22c8df0553dced52ed

MD5 File Hash	ff7611be7e3137708a68ea8523093419
Code Signing Cert Serial Num.	028E1DECCF93D38ECF396118DFE908B4
Code Signing Cert Serial Num.	0453F5E1437937
Code Signing Cert Serial Num.	0F66842B4F9C458B72136F0AE96924B7
Code Signing Cert Serial Num.	112127474DE010DA49D31D0EE8193EAC2D0E
Code Signing Cert Serial Num.	1121333A0B1EA5C37487BE5B034CE7E548C2
Code Signing Cert Serial Num.	1121A39E974748623CA6E3E49A8BAEB3ED3A
Code Signing Cert Serial Num.	1121B967F092CBF19234F4F18F730F4F767B
Code Signing Cert Serial Num.	1121BE355D779209D9115CAB4F639917EB72
Code Signing Cert Serial Num.	1121C4FE70E986B0A09CECA460359F98E5EE
Code Signing Cert Serial Num.	22CF7DA7B76FC5C4E77225CFA1BDA497
Code Signing Cert Serial Num.	27A433CA2FE767B65EB96E4304C92E53
Code Signing Cert Serial Num.	2B5A383157EFC7CD2617EF32F0A7ACB9
Code Signing Cert Serial Num.	2B6EF1471DFC04ED3CB642AC56F139E5
Code Signing Cert Serial Num.	2F046D1750F5F527BD6F57503A7CAA07
Code Signing Cert Serial Num.	3308CED5C19726541B196F805AC50CD0
Code Signing Cert Serial Num.	4505E9AC8D288D763A1088ED1E2C8A60
Code Signing Cert Serial Num.	57BE1A00D2E59BDBD19524AAA17ED93B
Code Signing Cert Serial Num.	597683B68EF6B0C8BE2D85A212B51910
Code Signing Cert Serial Num.	76311C06EB80095EB520D02BDE7FAC1F
Code Signing Cert Serial Num.	7A00ACB77008A72110110E0D6635B97F
Code Signing Cert Serial Num.	7E12573328ADF45B6F3EC341E646293A

Area #7:

Type	Indicator
Domain	chinadagitaltimes[.]net
Domain	datalink[.]one
Domain	bowenpress[.]org
Domain	bowenpress[.]net

Domain	bowenpross[.]com
Domain	tibetonline[.]info
WHOIS Phone	12126881188
WHOIS Email	aobama_5@yahoo[.]com

Area #8:

Type	Indicator
IP Address	103.82.52.111
IP Address	103.82.52.18
IP Address	118.184.85.135
IP Address	118.193.222.253
IP Address	205.209.149.144
IP Address	205.209.186.164
Domain	5tua[.]com
Domain	862283496@qq[.]com
Domain	aboluewang[.]com
Domain	airsportschina[.]net
Domain	bafangqudao[.]com
Domain	chongzhonglaw[.]com
Domain	duoxiantong[.]com
Domain	find-iphone-icloudcn[.]com
Domain	find-iphone-icloudids[.]com
Domain	find-iphone-iclouds[.]com
Domain	find-iphone-icloudss[.]com
Domain	find-iphone-idicloud[.]com
Domain	find-iphone7-icloud[.]com
Domain	find-iphoneid-itunes[.]com
Domain	freesss[.]net

Domain	gistal[.]com
Domain	guizuidc[.]com
Domain	huanjue123[.]zs[.]guizuidc[.]com
Domain	kuaiwenwang[.]com
Domain	laoa8[.]com
Domain	lycostal[.]com
Domain	mail[.]gistal[.]com
Domain	mail[.]lycostal[.]com
Domain	mail[.]openncheckmail[.]com
Domain	maozai huanjue
Domain	mianbeiankj[.]com
Domain	openmd5[.]com
Domain	openncheckmail[.]com
Domain	senvmeitu[.]com
Domain	shijihulian[.]com
Domain	shiyuesun[.]com
Domain	tjglmy[.]com
Domain	tqvps[.]com
Domain	ttidc[.]net
Domain	tyuweb[.]com
Domain	user[.]xiangyunvps[.]com
Domain	user[.]xiangyunvps[.]net
Domain	vpsgys[.]com
Domain	www[.]5tua[.]com
Domain	www[.]chongzhonglaw[.]com
Domain	www[.]duoxiantong[.]com
Domain	www[.]find-iphone-idicloud[.]com
Domain	www[.]find-iphone7-icloud[.]com
Domain	www[.]kuaiwenwang[.]com

Domain	www[.]laoa8[.]com
Domain	www[.]tqvps[.]com
Domain	www[.]ttidc[.]net
Domain	www[.]xiangyunhulian[.]com
Domain	www[.]xiangyunvps[.]com
Domain	www[.]xiangyunvps[.]net
Domain	www[.]xunsuhulian[.]com
Domain	xgyun[.]vip
Domain	xiangyunhulian[.]com
Domain	xiangyunvps[.]net
Domain	xunsuhulian[.]com
MD5 File Hash	3b58e122d9e17121416b146daab4db9d
MD5 File Hash	b6be3f0864354a2e68144d17c3884d3b
MD5 File Hash	d848d4ec24e678727b63251e54a0a5de
WHOIS Email	huajue1019@qq[.]com
WHOIS Email	huajue1019@vip.qq[.]com
WHOIS Email	huanjue1019@qq[.]com
WHOIS Email	rooterit@outlook[.]com
SSL Cert SHA1	5a1c6ae9e2633df29c01a2668538e0203de375b2

About 401TRG

401TRG (Threat Research Group) is the Threat Research & Analysis Team at ProtectWise. Using our experience and background in incident response and network forensics in both the public and private sectors, we study ProtectWise's extensive network-oriented datasets. This work is focused around network traffic analysis, reverse engineering malware, building behavioral detections, and much more. We are sharing our knowledge and intelligence discoveries with fellow network defenders and information security professionals to strengthen the community as a whole.

©2018 ProtectWise, Inc. All rights reserved.