CYBER
THREAT
ANALYSIS

CHINA

Recorded Future®

By Insikt Group®

June 16, 2021

Threat Activity Group RedFoxtrot Linked to China’s PLA Unit 69010; Targets Bordering Asian Countries

This report profiles a suspected Chinese state-sponsored threat activity group, RedFoxtrot, with links to PLA Unit 69010. The activity was identified through a combination of large-scale automated network traffic analytics and expert analysis. Data sources include the Recorded Future Platform, SecurityTrails, DomainTools, PolySwarm, Farsight, and common open-source tools and techniques. The report will be of most interest to individuals engaged in strategic and operational intelligence relating to the activities of Chinese military intelligence units in cyberspace and network defenders with a presence in Central or South Asia. Analysis cut-off date: June 1, 2021.

Executive Summary

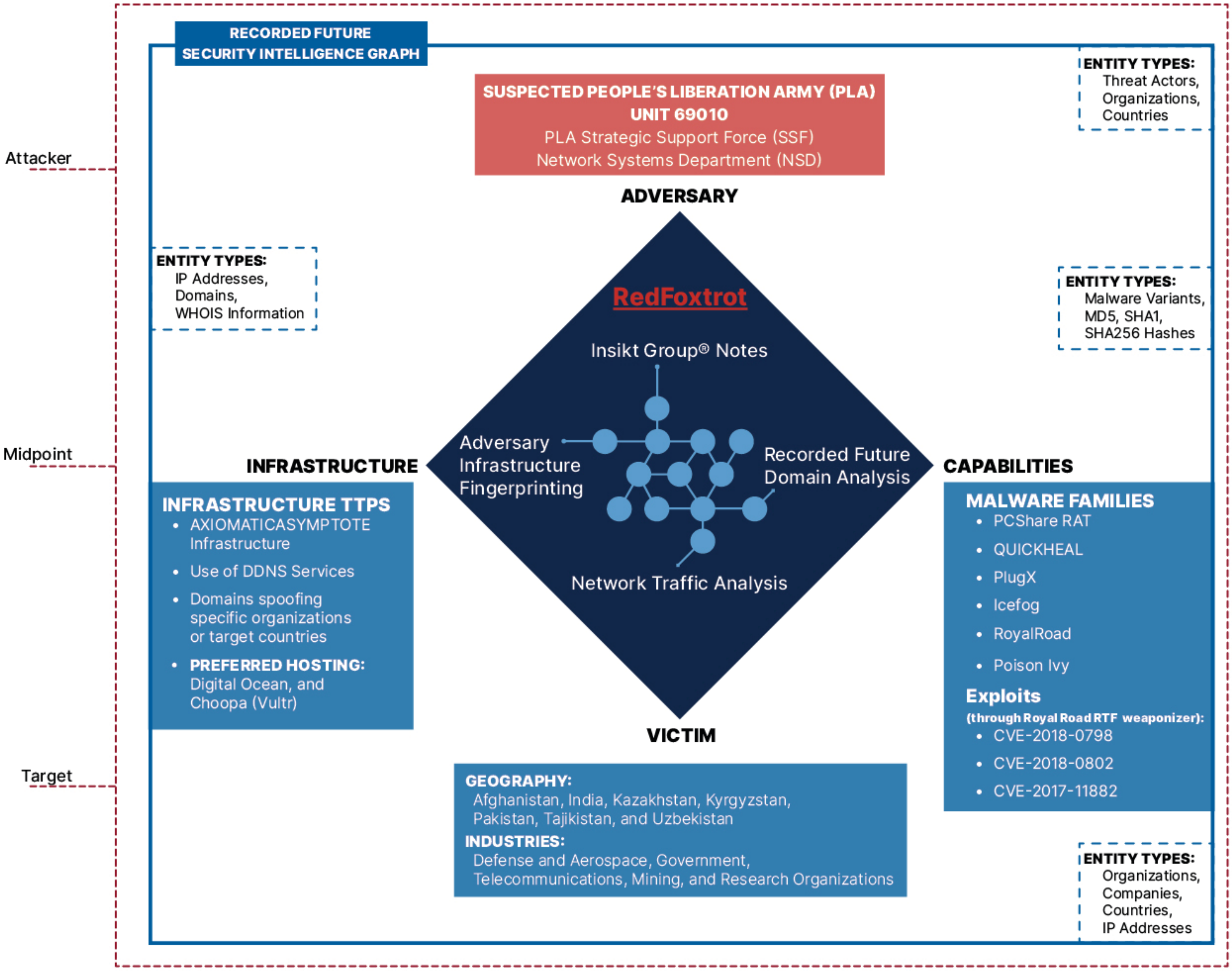
Recorded Future's Insikt Group has identified ties between a suspected Chinese state-sponsored threat activity group we track as RedFoxtrot and the Chinese military intelligence apparatus, specifically People's Liberation Army (PLA) Unit 69010 located in Ürümqi, Xinjiang. This activity offers a glimpse into PLA operations following a major organizational restructure beginning in 2015 and follows a period where public reporting has largely concentrated on groups affiliated with China's Ministry of State Security (MSS).

Unit 69010 is likely the Military Unit Cover Designator (MUCD) for a Technical Reconnaissance Bureau (TRB) within the PLA Strategic Support Force (SSF) Network Systems Department (NSD), an information and cyber warfare branch of the PLA. Due to lax operational security measures employed by a suspected RedFoxtrot operator, Insikt Group linked the threat group to the physical address of Unit 69010's headquarters. Publicly available procurement and court documents further tied Unit 69010 both to this address and to the SSF. Multiple academic publications also support the hypothesis that this unit has a cyber mission.

RedFoxtrot has been active since at least 2014 and predominantly targets government, defense, and telecommunications sectors across Central Asia, India, and Pakistan, aligning with the likely operational remit of Unit 69010. Of particular note, within the past 6 months, Insikt Group detected RedFoxtrot network intrusions targeting 3 Indian aerospace and defense contractors; major telecommunications providers in Afghanistan, India, Kazakhstan, and Pakistan; and multiple government agencies across the region. RedFoxtrot maintains large amounts of operational infrastructure and has likely employed both bespoke and publicly available malware families commonly used by Chinese cyber espionage groups, including Icefog, PlugX, Royal Road, Poison Ivy, ShadowPad, and PCShare. RedFoxtrot activity overlaps with threat groups tracked by other security vendors as Temp.Trident and Nomad Panda.

Key Judgments

- Formerly known as the Lanzhou Military Region's Second Technical Reconnaissance Bureau, PLA Unit 69010 has very likely been incorporated into the Network Systems Department of the PLA-SSF following a 2015 restructure.
- We believe that RedFoxtrot is a Chinese state-sponsored threat activity group based on identified links to a specific PLA unit and the use of shared custom capabilities considered unique to Chinese cyber espionage groups.
- In 2020, RedFoxtrot, alongside multiple other PLA and MSS-affiliated threat groups, likely gained access to the ShadowPad backdoor.
- In the aftermath of the 2015 restructuring, activity linked to previously tracked PLA-affiliated cyber espionage groups has declined, likely due to old activity groups disbanding or merging to form new clusters. With continued activity from suspected PLA groups such as Tonto Team, Tick, Naikon, and RedFoxtrot, and the emergence of new Chinese threat activity groups with suspected PLA links, Insikt Group believes that PLA-affiliated groups remain prominent within the Chinese cyber espionage sphere despite increased attention on their MSS counterparts.



SUSPECTED PEOPLE'S LIBERATION ARMY (PLA) UNIT 69010
PLA Strategic Support Force (SSF)
Network Systems Department (NSD)

ENTITY TYPES:
Threat Actors,
Organizations,
Countries

ENTITY TYPES:
IP Addresses,
Domains,
WHOIS Information

ENTITY TYPES:
Malware Variants,
MD5, SHA1,
SHA256 Hashes

INFRASTRUCTURE TTPS

- AXIOMATICASYMPTOTE Infrastructure
- Use of DDNS Services
- Domains spoofing specific organizations or target countries
- **PREFERRED HOSTING:** Digital Ocean, and Choopa (Vultr)

MALWARE FAMILIES

- PCShare RAT
- QUICKHEAL
- PlugX
- Icefog
- RoyalRoad
- Poison Ivy

Exploits
(through Royal Road RTF weaponizer):

- CVE-2018-0798
- CVE-2018-0802
- CVE-2017-11882

GEOGRAPHY:
Afghanistan, India, Kazakhstan, Kyrgyzstan, Pakistan, Tajikistan, and Uzbekistan

INDUSTRIES:
Defense and Aerospace, Government, Telecommunications, Mining, and Research Organizations

ENTITY TYPES:
Organizations,
Companies,
Countries,
IP Addresses

Figure 1: High-level RedFoxtrot TTPs and Recorded Future data sourcing graphic (Source: Recorded Future)

Threat Analysis

RedFoxtrot has primarily targeted aerospace and defense, government, telecommunications, mining, and research organizations in Afghanistan, India, Kazakhstan, Kyrgyzstan, Pakistan, Tajikistan, and Uzbekistan. These targets suggest the group is likely interested in gathering intelligence on military technology and defense. RedFoxtrot has historically employed multiple open- and closed-source tooling commonly shared across Chinese cyber espionage groups, including PlugX, Poison Ivy, Royal Road, PCShare, and IceFog. Insikt Group also identified multiple links to suspected ShadowPad command and control (C2) infrastructure, tracked by Recorded Future as AXIOMATICASYMPTOTE, providing evidence of yet another Chinese group with access to the custom backdoor. Notable RedFoxtrot victims over the past 6 months include multiple Indian aerospace and defense contractors; telecommunications companies in Afghanistan, India, Kazakhstan, and Pakistan; and several national and state institutions in the region. Activity over this period showed a particular focus on Indian targets, which occurred at a time of heightened border tensions between India and the People's Republic of China (PRC).

RedFoxtrot's Connection to PLA Unit 69010

Insikt Group identified links between RedFoxtrot's operational infrastructure and PLA Unit 69010 through the online persona of a suspected RedFoxtrot threat actor. Due to lax operational security measures employed by this individual, we uncovered a connection to the likely physical address of the headquarters of PLA Unit 69010, No. 553, Wenquan East Road, Shuimogou District, Ürümqi, Xinjiang (新疆乌鲁木齐市水磨沟区温泉东路553号). Insikt Group is not publicly disclosing the identity of this individual; however, an extensive online presence provided corroborating evidence indicating that this individual is located in Ürümqi, has an interest in hacking, and also has a suspected historical affiliation with the PLA's former Communications Command Academy[1] (通信指挥学院) located in Wuhan.

[1] Also formerly known as the Communications Command College, the Communications Command Academy has previously been noted for its role in training former 3PLA personnel in information and cyber warfare and military communications systems. It has now been likely incorporated into the College of Information and Communication at the National University of Defense Technology (国防科技大学信息通信学院).

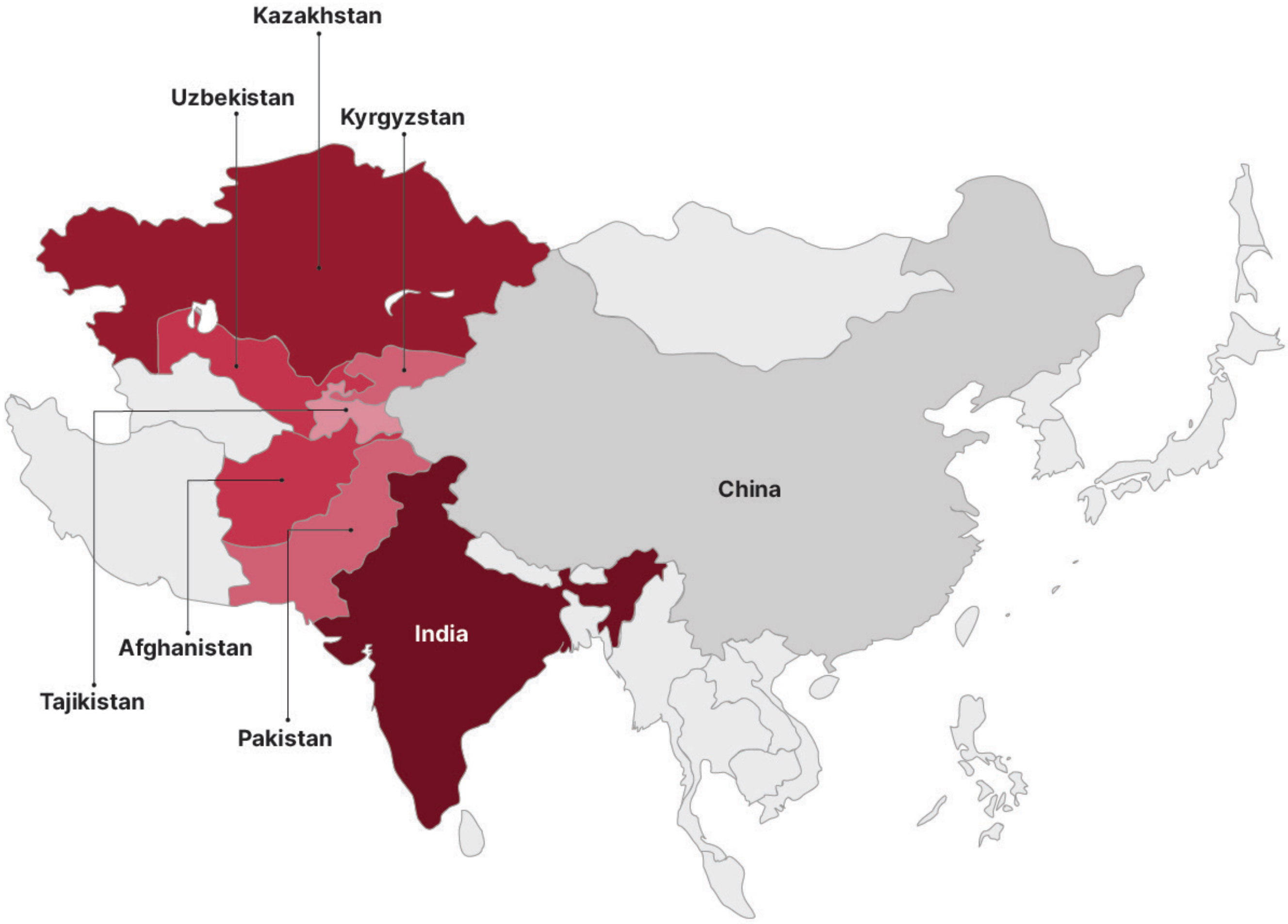


Figure 2: Heatmap of RedFoxtrot activity targeting Central and South Asia

What is Unit 69010?

Unit 69010 is likely the MUCD for a bureau within the PLA-SSF headquartered in Ürümqi, Xinjiang. Formerly known as the Lanzhou Military Region's Second TRB according to research published in 2011 from the Project 2049 Institute, signals intelligence (SIGINT) has long been considered to be within Unit 69010's area of responsibility. The unit also likely has multiple subordinate offices primarily responsible for monitoring military activity along China's western border. An analysis of academic output attributed to the unit also provides evidence that Unit 69010 likely has a cyber mission as late as 2015 (example publications [2],[3]). Prior to a restructure beginning in 2015, much of China's cyber espionage efforts were linked to TRBs and bureaus of the PLA General Staff Department's (GSD) Third Department (3PLA). 3PLA was broadly responsible for defensive SIGINT, including monitoring Chinese communication networks, protecting the security of Chinese domestic computer networks, and conducting cyber espionage-oriented computer network exploitation. Beginning in 2015, the capabilities and tasking of the TRBs and 3PLA were reorganized and largely moved into the newly formed SSF NSD. Evidence explored in the following section indicates that Unit 69010 was likely moved under the SSF NSD as part of China's military reforms.

The former Lanzhou Military Region was incorporated within the new Western Theater Command of the PLA following the 2015 restructure. The Western Theater Command is one of 5 theater commands of the PLA, and is almost certainly tasked with monitoring India, Pakistan, and Central Asia. This orientation directly aligns with observed RedFoxtrot activity. Similarly, intelligence gathering on defense, military, telecommunications, and government targets also aligns with the expected operational scope of a PLA unit and fits the target profile of other PLA-linked groups (1,2,3).

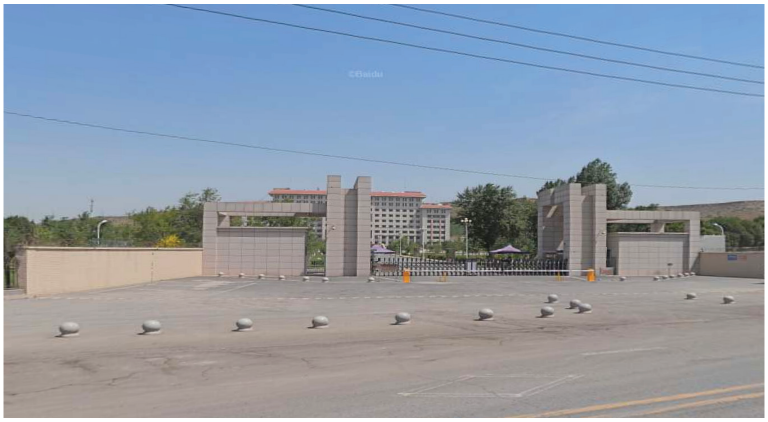
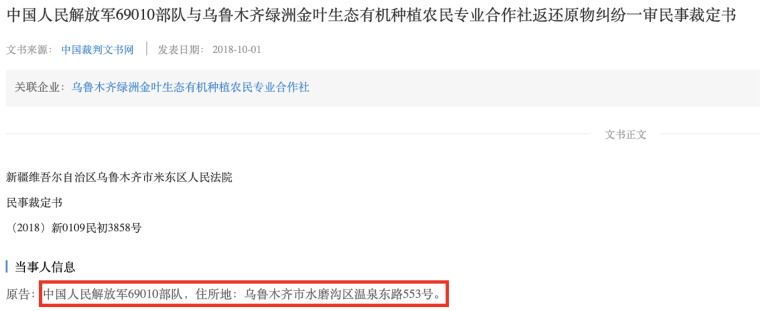


Figure 3: Entrance to suspected Unit 69010 compound located at No. 553 Wenquan East Road, Ürümqi (Source: Baidu Maps)

No. 553, Wenquan East Road

Public reporting has indicated that Unit 69010 is headquartered in Ürümqi's Shuimogou [水磨沟] district. We identified that the No. 553 Wenquan East Road address, which is situated within Shuimogou, has appeared on multiple Xinjiang provincial court documents directly linking PLA Unit 69010 to this location. Furthermore, this address is featured on 5 SSF-issued tenders for a variety of equipment over the past several years, indicating that Unit 69010 was likely moved to the SSF following PLA reforms.



中国人民解放军69010部队与乌鲁木齐绿洲金叶生态有机种植农民专业合作社返还原物纠纷一审民事裁定书

文书来源：中国裁判文书网 | 发表日期：2018-10-01

关联企业：乌鲁木齐绿洲金叶生态有机种植农民专业合作社

文书正文

新疆维吾尔自治区乌鲁木齐市米东区人民法院

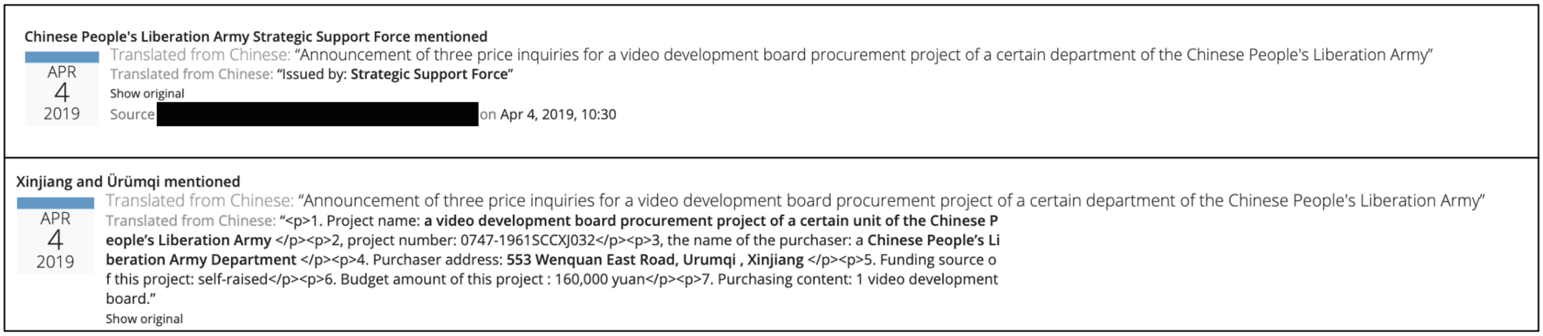
民事裁定书

（2018）新0109民初3858号

当事人信息

原告：中国人民解放军69010部队，住所地：乌鲁木齐市水磨沟区温泉东路553号。

Figure 4: Court document linking Unit 69010 to No. 553 Wenquan East Road address [4]



Chinese People's Liberation Army Strategic Support Force mentioned

APR 4 2019

Translated from Chinese: "Announcement of three price inquiries for a video development board procurement project of a certain department of the Chinese People's Liberation Army"

Translated from Chinese: "Issued by: **Strategic Support Force**"

Show original

Source [redacted] on Apr 4, 2019, 10:30

Xinjiang and Ürümqi mentioned

APR 4 2019

Translated from Chinese: "Announcement of three price inquiries for a video development board procurement project of a certain department of the Chinese People's Liberation Army"

Translated from Chinese: "<p>1. Project name: **a video development board procurement project of a certain unit of the Chinese People's Liberation Army** </p><p>2, project number: 0747-1961SCCXJ032</p><p>3, the name of the purchaser: a **Chinese People's Liberation Army Department** </p><p>4. Purchaser address: **553 Wenquan East Road, Urumqi , Xinjiang** </p><p>5. Funding source of this project: self-raised</p><p>6. Budget amount of this project : 160,000 yuan</p><p>7. Purchasing content: 1 video development board."

Show original

Figure 5: Recorded Future Event for SSF-issued military procurement documents for 553 Wenquan East Road address (Source: Recorded Future)

[2] Yang Ping 杨萍 and Liang Guangming 梁广明, "物联网安全问题及对策分析" [Security Problems and Solutions for the Internet of Things], 无线互联科技 Wireless Internet Technology 6, (2013): 13.

[3] Yang Ping 杨萍 and Tian Jianchun 田建春, "Wireshark网络安全风险评估关键技术研究" [Research on Key Technologies of Wireshark Network Security Risk Assessment], 网络安全技术与应用 Network Security Technology and Application 9 (2015): 54.

[4] https://m.qcc[.]com/wenshuDetail/b218bb9ef2c2e2b282f8c88e098001b7.html

Baidu Maps shows that this address corresponds to a large compound facility comprising multiple buildings and a residential area. As evident from satellite and street-level imagery, multiple satellites are visible on the roof of the unit's main building as well as the hill behind the compound, while other attributes commonly seen at PLA bases are also present, such as a parade area, a running track and sports fields, and a large gated entrance.

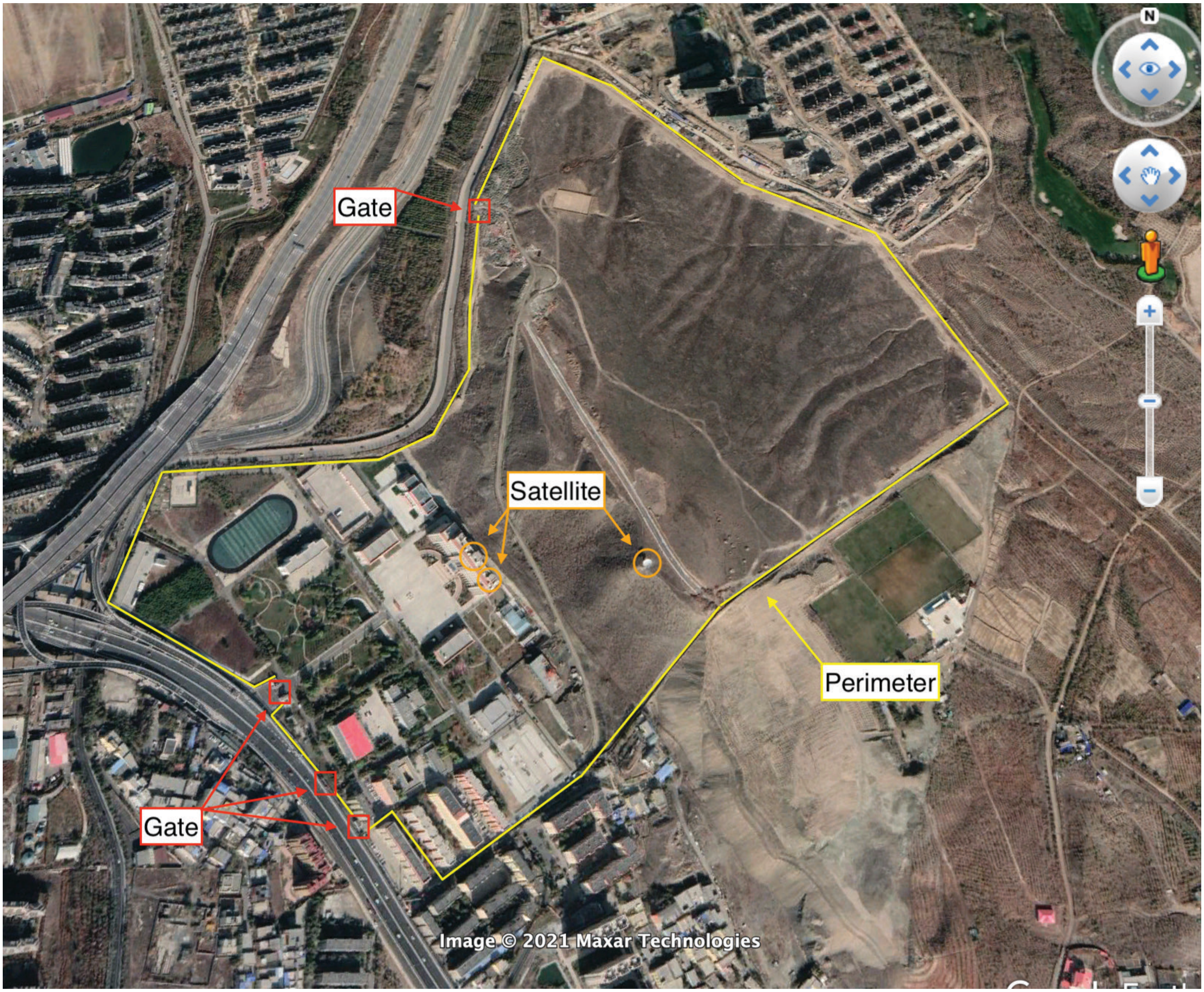
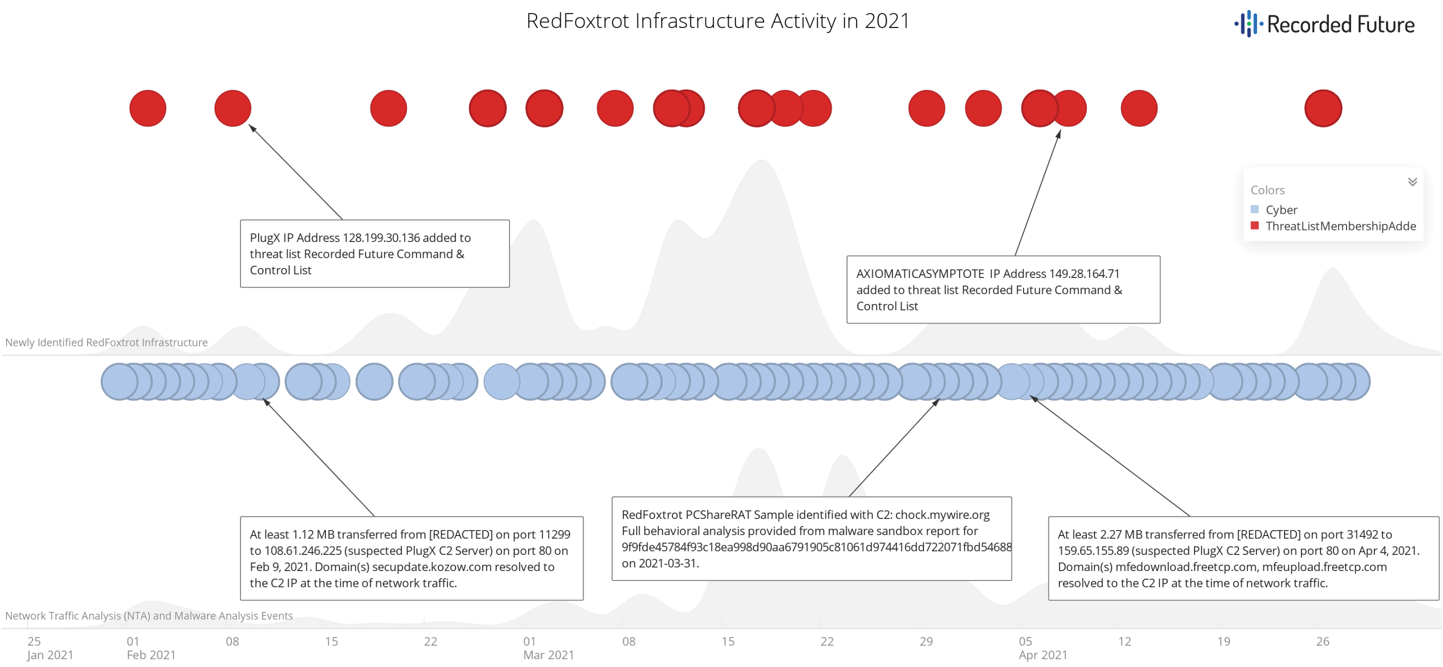


Figure 6: Aerial images of suspected Unit 69010 compound located on Wenquan East Road [5]

[5] Two other properties share the same address as Unit 69010: an apartment complex across the street, which we were unable to confirm is affiliated with the base, and an electronics store directly beside the base. It is very unlikely that the RedFoxtrot persona and related cyber espionage activity is linked to either of these 2 properties and the address almost certainly refers to Unit 69010 in the context of our investigation.



PlugX IP Address 128.199.30.136 added to threat list Recorded Future Command & Control List

AXIOMATICASYMPTOTE IP Address 149.28.164.71 added to threat list Recorded Future Command & Control List

At least 1.12 MB transferred from [REDACTED] on port 11299 to 108.61.246.225 (suspected PlugX C2 Server) on port 80 on Feb 9, 2021. Domain(s) secupdate.kozow.com resolved to the C2 IP at the time of network traffic.

RedFoxtrot PCShareRAT Sample identified with C2: chock.mywire.org Full behavioral analysis provided from malware sandbox report for 9f9fde45784f93c18ea998d90aa6791905c81061d974416dd722071fbd54688 on 2021-03-31.

At least 2.27 MB transferred from [REDACTED] on port 31492 to 159.65.155.89 (suspected PlugX C2 Server) on port 80 on Apr 4, 2021. Domain(s) mfedownload.freetcp.com, mfeupload.freetcp.com resolved to the C2 IP at the time of network traffic.

Figure 7: Timeline of RedFoxtrot infrastructure detection, malware detections, and NTA events in 2021 (Source: Recorded Future)

Mapping RedFoxtrot's Sprawling Infrastructure

Using Recorded Future Network Traffic Analysis (NTA), adversary infrastructure detection, and other common analytical techniques, we have tracked a large cluster of RedFoxtrot infrastructure and associated malware samples used in active intrusions over the past 6 months. There are strong ties between this activity and publicly reported campaigns dating back to at least 2014. We identified clear and consistent hosting overlaps for domains linked to the identified infrastructure cluster, as well as common targeting and overlapping malware use. Notably, we identified the following high-level trends in the group's infrastructure tactics, techniques, and procedures (TTPs):

- Use of a large number of Dynamic DNS (DDNS) domains which form part of overlapping infrastructure clusters
- DDNS domains often contain hints regarding geographical targeting or spoof specific organizations (for example, "inbsnl.ddns[.]info", "adtl.mywire[.]org", and "indianmail.zyns[.]com")
- Strong preference for DigitalOcean and Choopa (Vultr) hosting providers in recent times
- Use of AXIOMATICASYMPTOTE infrastructure, indicative of the group's likely access to the ShadowPad backdoor

As previously referenced in our reporting on the China-linked group RedEcho, network infrastructure used in ShadowPad infections is tracked by Insikt Group as AXIOMATICASYMPTOTE.

AXIOMATICASYMPTOTE and PlugX Clusters

Using Recorded Future adversary infrastructure detection methods, we identified that a large proportion of the RedFoxtrot domains are linked to AXIOMATICASYMPTOTE and PlugX C2 infrastructure. Many of these were also used as C2s for different malware families, such as PCShare. Commonly, the group used single servers to host a swath of DDNS domains, which were moved around in bulk over time.

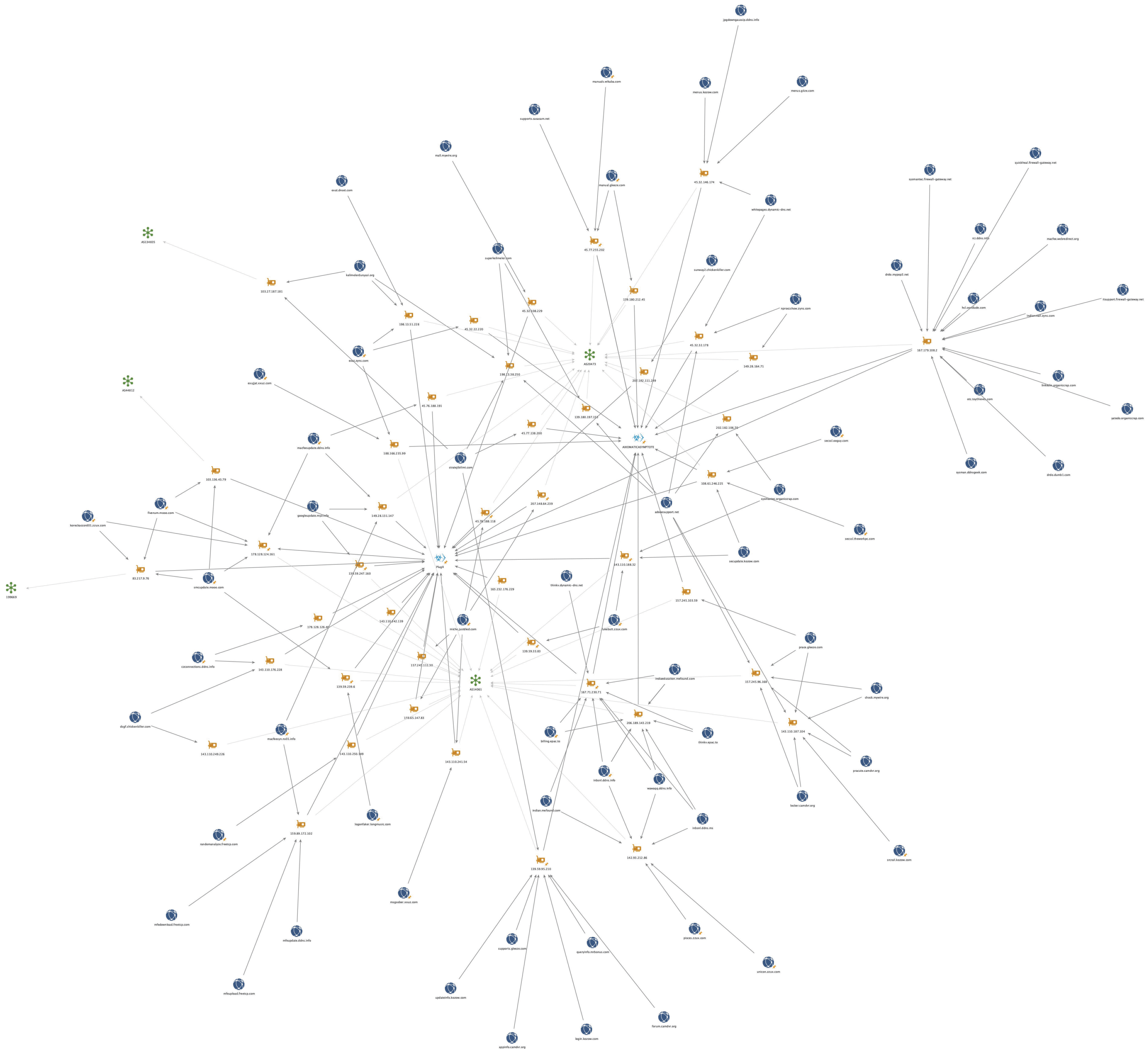


Figure 8: Partial Maltego chart of RedFoxtrot PlugX and AXIOMATICASYMPTOTE Infrastructure

Links to Historical Campaign Targeting Turkish Language Speakers

4 domains linked to RedFoxtrot activity registered in mid-2019 (kelimelerdunyasi[.]org, stratejibilimi[.]com, adobesupport[.]net, and superkelimeler[.]com) were all used by the group to mirror a legitimate Turkish language website for learning English, ingilizcem[.]org. In addition to consistent hosting overlaps and the shared spoofing of ingilizcem[.]org, 3 out of the 4 domains are linked to the same privacy protection registration email address, stratejibilimi.com@protectdomain[.]org. While these websites no longer resolve, open-source reporting indicates that adobesupport[.]net was used to serve the Poison Ivy SKYLINE variant masquerading as an Adobe Flash installer in mid-2019 (shortly after the registration of these 4 domains). We believe that these domains were likely used by RedFoxtrot to target Turkish-language speakers. Since this time, there have been consistent hosting overlaps between these 4 domains and multiple additional RedFoxtrot domains. Notably, the Poison Ivy variant served from adobesupport[.]net closely overlaps with additional suspected RedFoxtrot activity:

Poison Ivy SKYLINE Variant	C2 Domain
acb11d9d0652c95b16db17fda918ff5b6ee66815 6a30fe6276b0fa66f74c9720	skylineqaz.crabdance[.]com
c1e3a5e171d0de6054f4a1aeb9a46ff176ef5ba6 464304b2f2660a23396e91f4	coreldraw.kozow[.]com
379af30d508cdbae7eb201041d8eb815b239e18 1dd8106145d4263753df3acd9	hostmail1[.]com
367718fd58c658dce22c995f3e10bc3a5425814 ddf221686e166e3129a53e897	capture.kozow[.]com

In addition to characteristics previously highlighted regarding this Poison Ivy variant, there are also direct historical hosting overlaps between the kelimelerdunyasi[.]org domain and hostmail1[.]com (45.251.241[.]13) as well as hostmail1[.]com and skylineqaz.crabdance[.]com (206.189.153[.]132).

Overlaps With Publicly Reported Activity

RedFoxtrot activity overlaps with groups tracked by other security vendors as Temp.Trident/Nomad Panda. A multitude of infrastructure, targeting, and malware overlaps were discovered between RedFoxtrot activity and 2018 to 2019 campaigns tracked by FireEye as WATERFIGHT and SKYLINE, which targeted countries in Central Asia (1,2). Additionally, elements of the group's historical use of the Royal Road (also known as 8.t) rich text format (RTF) weaponizer to deliver Icefog and Poison Ivy payloads have been previously documented. Some notable overlaps with publicly reported activity include the following non-exhaustive examples:

1. The domain skylineqaz.crabdance[.]com has been previously referenced in public reporting in relation to activity targeting Turkey and Kazakhstan, and was hosted on DigitalOcean IP address 206.189.153[.]132 in September 2019. This domain features additional temporal hosting overlaps with multiple RedFoxtrot DDNS domains:
   - redhatboy.dynamic-dns[.]net
   - scorpio.dns04[.]com
   - koreckaccord01.zzux[.]com
   - exat.dnset[.]com
   - macfeesyn.ns01[.]info
   - gulistan.wikaba[.]com
   - macfeeupdate.ddns[.]info
   - lexuz.dns05[.]com
   - lexuz.x24hr[.]com
2. The Poison Ivy C2 capture.kozow[.]com was historically hosted on DigitalOcean IP address 45.76.197[.]157 from mid-to-late 2020, overlapping with the RedFoxtrot PCShare C2 domain locker.camdvr[.]org. As noted in previous reporting, the Poison Ivy sample linked to the capture.kozow[.]com C2 is the same SKYLINE variant used in the previously referenced campaign targeting Turkey and Kazakhstan.
3. In mid-2020, the domain pisces.zzux[.]com was concurrently hosted on the DigitalOcean IP address 142.93.212[.]86 alongside a cluster of RedFoxtrot India-themed DDNS domains:
   - inbsnl.ddns[.]info
   - inbsnl.ddns[.]ms
   - indian.mefound[.]com

4. Additional links between the pisces.zzux[.]com domain and RedFoxtrot infrastructure have also been previously documented. Furthermore, one of the above RedFoxtrot DDNS domains, inbsnl.ddns[.]info, is linked to a QUICKHEAL sample (f45c6f8695fbc6e537cea15142f062a0d21c4a556c5fc1f7a2f3ee661b036ffc), a shared custom malware family previously used in RedFoxtrot activity.

The Maltego chart below outlines additional overlaps with previously publicly reported RedFoxtrot activity.

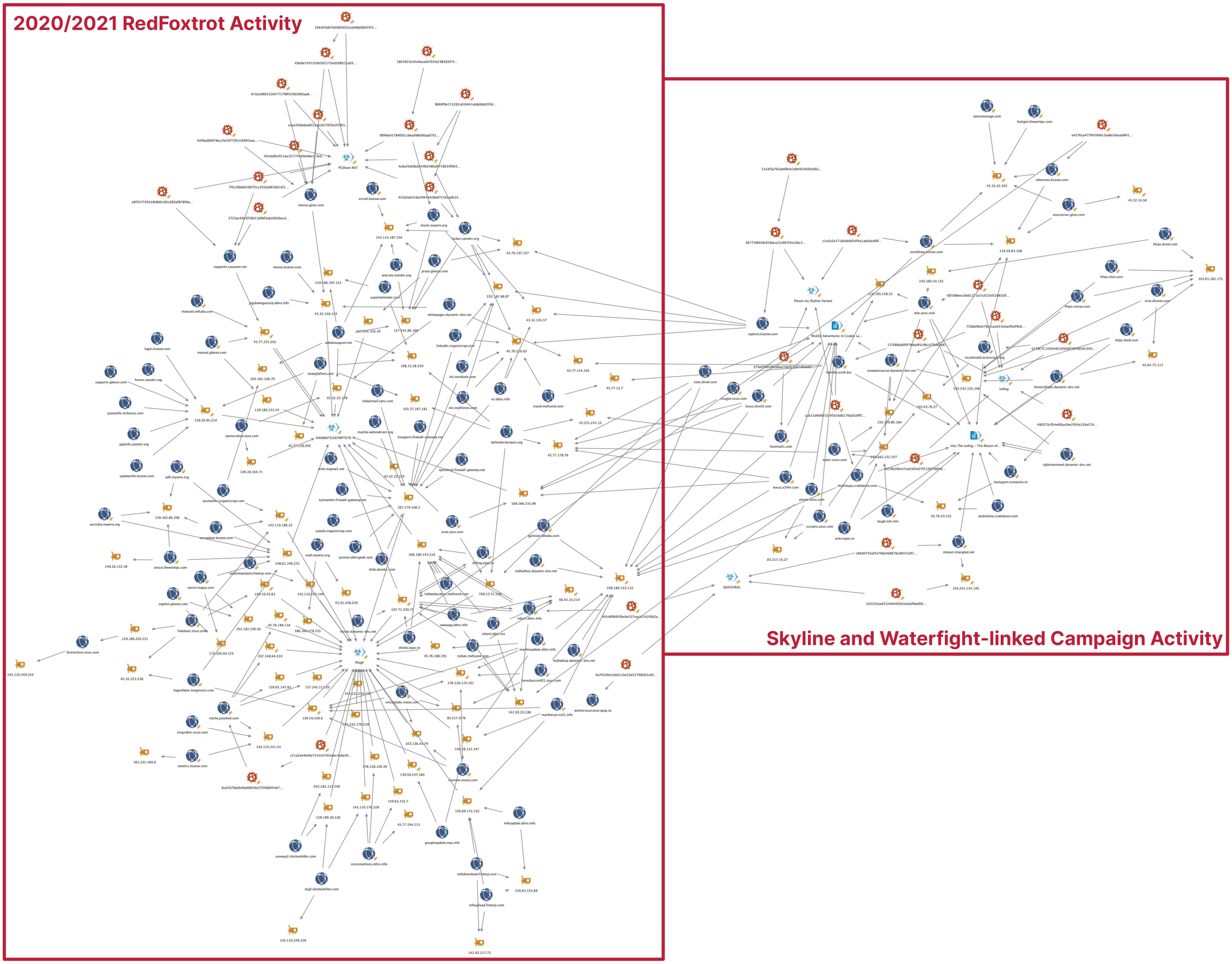

2020/2021 RedFoxtrot Activity
Skyline and Waterfight-linked Campaign Activity
PCShare RAT
PlugX
QUICKHEAL
Poison Ivy Skyline Variant

Figure 9: Overlap between 2020/2021 RedFoxtrot activity and publicly reported SKYLINE and WATERFIGHT campaigns

Mitigations

We recommend that users conduct the following measures to detect and mitigate activity associated with RedFoxtrot activity:

- Configure your intrusion detection systems (IDS), intrusion prevention systems (IPS), or any network defense mechanisms in place to alert on — and upon review, consider blocking connection attempts to and from — the external IP addresses and domains listed in Appendix A.
- Multiple state-sponsored and financially motivated threat activity groups continue to use DDNS domains in network intrusion activity. All TCP/UDP network traffic involving DDNS subdomains should be blocked and logged (using DNS RPZ or similar).
- Recorded Future Threat Intelligence, Third-Party Intelligence, and SecOps Intelligence module users can monitor real-time output from NTA and Malware Analysis analytics to identify suspected targeted intrusion activity involving your organization or key vendors and partners.
- Ensure Microsoft Office and Windows software are up to date with the latest software updates to protect against malicious documents that attempt to exploit known vulnerabilities for code execution, such as those created using the Royal Road RTF weaponizer.

Outlook

Our research uncovered cyber espionage activity attributed to RedFoxtrot, a group linked to Unit 69010 of the PLA-SSF. Of particular note: from 2020 to 2021, the group heavily targeted Indian defense contractors, telecommunications providers, and government organizations at a time of heightened tension between China and India. We also recently revealed a campaign targeting critical infrastructure within India that we attributed to a group called RedEcho. While the RedEcho campaign posed pre-positioning concerns within India's electricity system, RedFoxtrot's activity is more aligned with traditional PLA-linked activity in gathering military intelligence. These differing strands of activity exemplify Beijing's multi-pronged approach within cyberspace, using it as a tool for gathering intelligence on military technology and national security issues as well as political developments and foreign relations; for monitoring ethnic and religious minorities such as Uyghurs, Tibetans, and Catholics, and to further goals set out within strategic policy such as the Belt and Road Initiative and Made in China 2025.

Recent years have marked an apparent downturn in reported activity linked to previously tracked PLA-affiliated cyber espionage groups in the aftermath of the 2015 restructuring, likely due to old activity groups disbanding or merging to form new clusters. In this period, Chinese cyber espionage efforts have been widely characterized by activity linked to the Ministry of State Security (MSS), China's principal civilian foreign intelligence service. The MSS has been frequently identified employing a private contractor model for cyber espionage activity, according to US government indictments and the anonymous Chinese APT doxxing persona Intrusion Truth. However, with continued activity from PLA-linked groups such as Tonto Team, Tick, Naikon, and RedFoxtrot, we believe that PLA-affiliated groups remain prominent within the Chinese cyber espionage sphere despite increased attention on their MSS counterparts.

Appendix A — Indicators of Compromise

Readers can access the indicators listed below in our public Insikt Group Github repository: https://github.com/Insikt-Group/Research (RedFoxtrot - June 2021).

Network Indicators:

Domains:

```
adobesupport[.]net
adtl.mywire[.]org
appinfo.camdvr[.]org
aries.epac[.]to
billing.epac[.]to
capture.kozow[.]com
chock.mywire[.]org
coreldraw.kozow[.]com
czconnections.ddns[.]info
drdo.dumb1[.]com
drdo.mypop3[.]net
dsgf.chickenkiller[.]com
elienceso.kozow[.]com
exat.dnset[.]com
exat.zyns[.]com
execserver.giize[.]com
exujjat.xxuz[.]com
fashget.theworkpc[.]com
fivenum.mooo[.]com
foreverlove.zzux[.]com
forum.camdvr[.]org
fukebutt.zzux[.]com
googleupdate.myz[.]info
gulistan.wikaba[.]com
hcl.sexidude[.]com
honoroftajik.dynamic-dns[.]net
hostmail1[.]com
https.dnset[.]com
https.ikwb[.]com
https.otzo[.]com
https.vizvaz[.]com
inbsnl.ddns[.]info
inbsnl.ddns[.]ms
indiaeducation.mefound[.]com
indian.mefound[.]com
indianmail.zyns[.]com
itsupport.firewall-gateway[.]net
jpgdowngaussip.ddns[.]info
kastygost.compress[.]to
kelimelerdunyasi[.]org
koreckaccord01.zzux[.]com
laugh.toh[.]info
lexuz.dns05[.]com
lexuz.x24hr[.]com
linkedin[.]organiccrap[.]com
locker.camdvr[.]org
login.kozow[.]com
logonfaker.longmusic[.]com
macfee.webredirect[.]org
macfeesyn.ns01[.]info
macfeeupdate.ddns[.]info
mall.mywire[.]org
manual.gleeze[.]com
manuals.wikaba[.]com
menus.giize[.]com
menus.kozow[.]com
mfedownload.freetcp[.]com
mfeupdate.ddns[.]info
mfeupload.freetcp[.]com
miche.justdied[.]com
msgsober.xxuz[.]com
msn.dnsnet[.]com
nicodonald.accesscam[.]org
niteast.strangled[.]net
notice.theworkpc[.]com
nproccshow.zyns[.]com
otc[.]toythieves[.]com
pisces.zzux[.]com
prace.gleeze[.]com
pracute.camdvr[.]org
queryinfo.mrbonus[.]com
quickheal.firewall-gateway[.]net
randomanalyze.freetcp[.]com
rastelcs.kozow[.]com
rci.ddns[.]info
redhatboy.dynamic-dns[.]net
scorpio.zzux[.]com
secindia.mywire[.]org
secssl.ooguy[.]com
secssl.theworkpc[.]com
secupdate.kozow[.]com
skylineline.crabdance[.]com
skylineqaz.crabdance[.]com
smcupdate.mooo[.]com
srcrail.kozow[.]com
stratejibilimi[.]com
sunway2.chickenkiller[.]com
superkelimeler[.]com
supports.casacam[.]net
supports.gleeze[.]com
sysman.ddnsgeek[.]com
sysmantec.firewall-gateway[.]net
sysmantec[.]organiccrap[.]com
tajikstantravel.dynamic-dns[.]net
tele.zyns[.]com
thinkv.dynamic-dns[.]net
thinkv.epac[.]to
trand.mefound[.]com
trendiis.sixth[.]biz
updateinfo.kozow[.]com
uzwatersource.dynamic-dns[.]net
water.xxuz[.]com
wawaqq.ddns[.]info
whitepages.dynamic-dns[.]net
wsliversourcecor.epac[.]to
yatedo.organiccrap[.]com
```

IP Addresses (May 2021):

```
206.189.153[.]132
45.77.178[.]76
45.32.22[.]220
66.42.33[.]214
45.76.216[.]62
142.93.217[.]73
143.110.241[.]54
141.164.43[.]124
149.28.131[.]147
143.110.187[.]104
165.232.180[.]8
143.110.249[.]226
178.128.124[.]161
159.89.172[.]102
188.166.235[.]99
172.104.64[.]123
198.13.51[.]228
188.166.178[.]133
206.189.143[.]219
198.13.42[.]157
45.32.146[.]174
202.182.111[.]249
```

Malware Samples:

PCShare

```
2723ac49d3f59b51d96f3ab3605becdef1987242ef3d9d5b8490b0c9abe45049
425d2a6416a59943428e8727d2ad6247eb8342c35c4bd1d5b80df25d6fbcae94
4c6a45d08cb649b5486d9719634f903b3561e7820eda31bd50d811a01bd3481b
b668f9e213282cd1b941ab8d6dd5f3dd3266011ae16c0795ca86d12a57c095cc
69a9e5545103b582173ed268fc5ca0014c4d2e17337a953752b0157a76cc0bcb
7f3c26b8d3087f1cc345da965bb7af1a58488c6e260f12e72d8274d949a857bd
556d34db7e60b0d25eca0d8e6b9297cd9f2174c0d2ca013c0036a067457a2d01
e8f347745b1808db185c682af87896a941b4042f5de919e2010749152bda48ad
a7a3cd98252047717f8f429d2060aa84c6ee4ed8ae60ee15ad0b2b5807158c70
e1ca30bbdea8523aec6570f1b2f59012d0899875325a9ac88f09e09c14734ecc
f0c0a9b2911ee1f1774e69e0be313eda2054d744fa547f1c64ba0f078db3fcd9
9f9fde45784f93c18ea998d90aa6791905c81061d974416dd722071fbd54688e
69a9e5545103b582173ed268fc5ca0014c4d2e17337a953752b0157a76cc0bcb
8afcc6a25320a28833334a413a0f395a73bacf033fe0e84fea7ed4fec7945ca4
eeef1439b17280dfd7ce821752551aee57f3d1b7f385fe9cf331f69abd35cd96
8afcc6a25320a28833334a413a0f395a73bacf033fe0e84fea7ed4fec7945ca4
```

QUICKHEAL

```
4a7910fe2c0e611be52d15798563c007aa632d47eae1f020be95fde27d963da9
f45c6f8695fbc6e537cea15142f062a0d21c4a556c5fc1f7a2f3ee661b036ffc
851010b875a2ae5c68e85c7d549082539e427b0e9f0c5efef92e1396c6d8a0ae
```

PlugX

```
c21a3a44b46e7242c0762c8ec5e8a394ddc74b747244c5b83678620ae141e59c
6cd5079a69d9a68029e37f2680f44b7ba71c2b1eecf4894c2a8b293d5f768f10
45c944889a482ae2e0e0a8e260c3be737cb612c8804164badef61e8a8713b92f
```

Icefog

```
0c596299c47ce6305e07f55397fd69d49c8cab4f4b34a617bb6670dcaac9d9f2
11f38b6a69978dad95c9b1479db9a8729ca57329855998bd41befc364657d654
D096EECD60710CCF7F1658A52D54CAEF9CB26B3857B3A3DBEFA688C769E07339
087d8bee1db61273a7cd533d52b63265d3a8a8b897526d7849c48bcdba4b22ec
73bbb96e078a2ca3d55e0acffe0f9c80edf6ff0459a25c34edb4c14bb88783c1
e149E7C145D440193A0E3BF4B54C44DE00BBC3872EF18D6DA3C12F1E7ADD3053
```

PoisonIvy

```
acb11d9d0652c95b16db17fda918ff5b6ee668156a30fe6276b0fa66f74c9720
c1e3a5e171d0de6054f4a1aeb9a46ff176ef5ba6464304b2f2660a23396e91f4
379af30d508cdbae7eb201041d8eb815b239e181dd8106145d4263753df3acd9
367718fd58c658dce22c995f3e10bc3a5425814ddf221686e166e3129a53e897
```

Royal Road

```
51e3f3a762ab6fb0c3db4819560c6b1607cdcd257ce375e68fdf1a17ff5c2cb5
597c0c6f397eefb06155abdf5aa9a7476c977c44ef8bd9575b01359e96273486
4e1a2f731688f9aab80b1f55d9101bb1cddec08214d4379621c434899a01efbf
a95bbc1f067783c1107566ed7897549f6504d5367b8282efe6f06dc31414c314
9d239ddd4c925d14e00b5a95827e9191bfda7d59858f141f6f5dcc52329838f0
f5365387320ae6e6907fd2700f340ba8712cb08f7e52b2ec4dccfe99b3d648ef
ecdf806bb7ac876bac8250a1f0ff40395faf7a6738df6e0f62553c4164fdf16d
5238f8d8c3d16b52d39aa722daff663a5e6307c4b46e360969d84bf409a2690f
```

Appendix B — Detailed Malware Analysis

Chinese Cyber Espionage Groups Continue to Employ Shared Capabilities

RedFoxtrot's infrastructure is linked to an assortment of PlugX, Poison Ivy, Royal Road, PCShare, and IceFog samples used by the group. Furthermore, the use of AXIOMATICASYMPTOTE infrastructure has historically been linked to the use of the ShadowPad malware. 2 of these tools, IceFog and ShadowPad, are shared capabilities considered unique to Chinese cyber espionage groups. While Royal Road, PCShare, PlugX, and Poison Ivy are available more widely, their use is also strongly linked to multiple China-nexus threat activity groups. In recent times, RedFoxtrot has increasingly favored the use of PCShare, PlugX, and ShadowPad, with the group's use of IceFog, Poison Ivy, and Royal Road declining.

PCShare RAT

The Chinese open-source remote access trojan (RAT) PCShare is thought to have roots within the Chinese cybercriminal underground, with versions of the tool now freely available via GitHub. In recent years, variants of PCShare have been used in suspected Chinese cyber espionage activity targeting South East Asia governments and in campaigns attributed to the Chinese group Cycldek (also known as Goblin Panda). We identified multiple PCShare samples communicating with infrastructure within the identified RedFoxtrot infrastructure cluster. This consisted of a dropper and loader component which ultimately injects the PCShare RAT payload into the legitimate rdpclip.exe process. We identified 3 different samples used to drop PCShareRAT loaders, as listed below:

File Name	SHA256 Hash
Sophos System Protection Service.exe	556d34db7e60b0d25eca0d8e6b9297cd9f2174c0d2ca013c0036a067457a2d01
osloader.exe	B668f9e213282cd1b941ab8d6dd5f3dd3266011ae16c0795ca86d12a57c095cc
security_audit_template_final.doc	5802823e50e9aca0d765fa198383f74ca18859b1181cfc3f72f62667bca67dc2

The Sophos System Protection Service.exe sample is signed using a digital code signing certificate issued to 东莞信大融合创新研究院 (SHA1 thumbprint: 8E3991D623A7FFD86516224A0B6932785EF63F9E), which translates to Dongguan Xinda Integrated Innovation Research Institute. This organization is a Chinese military-civilian open innovation platform jointly established by the Dongguan Municipal People's Government and PLA-SSF Information Engineering University. We were unable to identify any additional files signed by this certificate, indicating it is not in widespread use. It is currently unclear how the threat activity group gained access to the code signing certificate, but it provides an additional nexus to a PLA-linked institution. In all cases, the dropper drops a PCShare loader to the following location and executes it using rundll32.exe:

```
C:\{user}\AppData\Local\Microsoft\Windows\Credentials\
Winload\halmacpi.slt
```

In each identified loader sample, the PCShare payload is injected by the loader into the legitimate process RDPclip.exe. Each identified PCShare payload also shares a common mutex (78de65b0701f3c9238a37).

One of the identified RedFoxtrot PCShare C2 domains (supports.casacam[.]net) is mentioned in a 2020 Bitdefender report detailing a Chinese activity group targeting Southeast Asia government institutions that details a similar PCShare dropper and loader component. However, the researchers note that this domain and other samples that inject into RDPclip.exe appear to be unrelated to the FunnyDream campaign analyzed within that report, which aligns with our findings that this is likely another case of shared tooling across Chinese activity groups.

PlugX

A RedFoxtrot PlugX sample named Sys.exe (SHA256: c21a3a44b46e7242c0762c8ec5e8a394ddc74b747244c5b83678620ae141e59c) was uploaded to a malware repository from India in September 2020. Sys.exe is a self-extracting RAR containing 3 files, RasTls.exe (a legitimate Symantec executable), RasTls.dll (malicious DLL used in DLL hijacking), and RasTls.dll.db (the PlugX payload), reflective of the ”triad” method of DLL hijacking employed by many Chinese activity groups.

Upon execution, RasTls.exe sideloads the malicious RasTls.dll (6cd5079a69d9a68029e37f2680f44b7ba71c2b1eecf4894c2a8b293d5f768f10), which in turn decrypts and loads the PlugX payload from RasTls.dll.db (fe18adaec076ffce63da6a2a024ce99b8a55bc40a1f06ed556e0997ba6b6d716). Once loaded, the payload contacts the C2 domain miche.justdied[.]com over TCP port 80. This same legitimate Symantec executable has been abused by multiple activity groups to load PlugX, and has also previously been used by RedFoxtrot to load both IceFog and QuickHeal. The PlugX samples used by RedFoxtrot all use an export function called MSCORE, which uses similar methods for decoding.

QUICKHEAL

We also identified multiple samples related to the identified adversary infrastructure cluster that appear to overlap with the malware variant tracked by FireEye as QUICKHEAL. All samples share an unusual export "GetOfficeDatatal" and feature multiple overlaps with 2 QUICKHEAL samples reported by FireEye in relation to the WATERFIGHT and SKYLINE campaigns.

One of the notable code overlaps is a function that loads memory addresses for SQLite and NSS functions, which are then used to parse, decode, and decrypt username and password combinations from the victim's Mozilla profiles. QUICKHEAL has also continued to use code to check if the backdoor is running in a proxy, and shares a hardcoded User-Agent: `Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727; .NET CLR 3.0.04506.648; .NET CLR 3.5.210.`

Royal Road, IceFog, and Poison Ivy

Elements of RedFoxtrot's use of the Royal Road RTF weaponizer to load the IceFog and Poison Ivy backdoors throughout 2018 and 2019 have been previously documented; however, we have not observed the group load other malware families using Royal Road other than these 2. While wider use of the Royal Road weaponizer by some Chinese groups is ongoing, its use by RedFoxtrot and several other China-linked groups has dropped since early 2020, likely in response to extensive public reporting. In addition to public reporting detailing the group's use of these capabilities, further examples of RedFoxtrot's historical use of these tools to target Central Asia, Pakistan, and India include the following:

- A RedFoxtrot Royal Road sample (51e3f3a762ab6fb0c3db4819560c6b160 7cdcd257ce375e68fdf1a17ff5c2cb5) from 2019 is linked to the identified infrastructure cluster, with the C2 domain remaining active into late 2020. The RTF document title is "DYSL-QT_Slide_DMC_090719.doc", which likely corresponds to the "Defence Research and Development Organisation (DRDO) Young Scientist Laboratory for Quantum Technologies" (DYSL-QT) located in Hyderabad, India. Additionally, DMC is likely in reference to the DRDO Management Council (DMC), suggesting the group used this lure in activity targeting Indian defense research. The RTF document drops the same Poison Ivy SKYLINE variant payload referenced earlier in the report (367718fd58c658dce22c995f3e10 bc3a5425814ddf221686e166e3129a53e 897), which is configured to communicate with the C2 capture.kozow[.]com.
- Another RedFoxtrot domain, water.xxuz[.]com, is linked to a historical Icefog sample (ICEFOG-P version) (SHA256: 0c596299c47ce6305e07f5 5397fd69d49c8cab4f4b34a617bb6670dcaac9d9f2). This sample was likely used in the WATERFIGHT campaign.
- Notably, 2 Royal Road lures used by the group in 2018 and 2019 specifically reference 2 telecommunications providers in Pakistan and India. We subsequently identified 2021 intrusions targeting both of these organizations. While we cannot confirm whether these previous intrusion attempts using Royal Road were successful, it indicates that telecommunications providers are a long term target of the group.

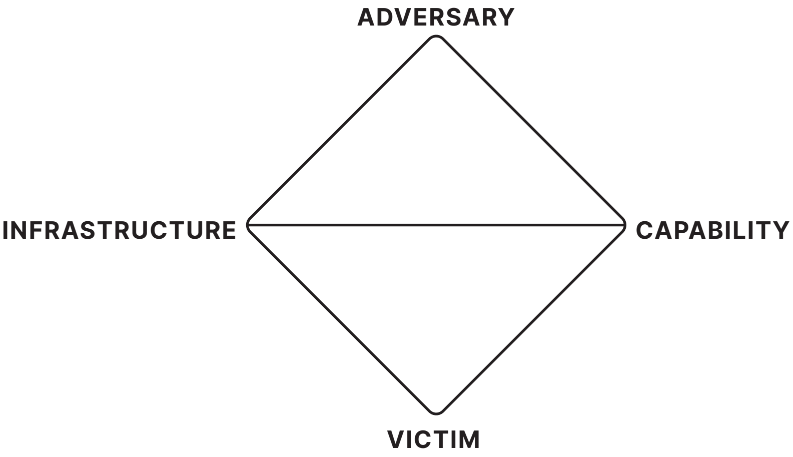
Recorded Future Threat Activity Group and Malware Taxonomy

Recorded Future's research group, Insikt, tracks threat actors and their activity, focusing on state actors from China, Iran, Russia, and North Korea, as well as cyber criminals - individuals and groups - from Russia, CIS states, China, Iran, and Brazil. We emphasize tracking activity groups and where possible, attributing them to nation state government, organizations, or affiliate institutions.

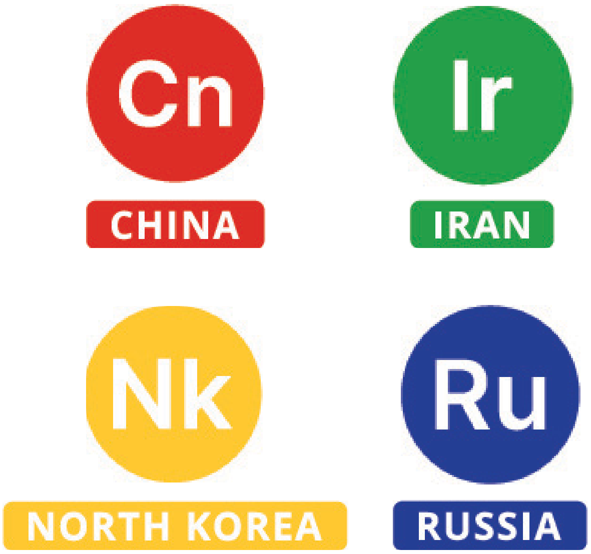
Our coverage includes:

- Government organizations and intelligence agencies, their associated laboratories, partners, industry collaborators, proxy entities, and individual threat actors.
- Recorded Future-identified, suspected nation state activity groups, such as RedAlpha, RedBravo, Red Delta, and BlueAlpha and many other industry established groups.
- Cybercriminal individuals and groups established and named by Recorded Future
- Newly emerging malware, as well as prolific,persistent commodity malware

Insikt Group names a new threat activity group or campaign when analysts have data corresponding to at least three points on the Diamond Model of Intrusion Analysis with at least medium confidence, derived from our Security Intelligence Graph. We can tie this to a threat actor only when we can point to a handle, persona, person, or organization responsible. We will write about the activity as a campaign in the absence of this level of adversary data. We use the most widely-utilized or recognized name for a particular group when the public body of empirical evidence is clear the activity corresponds to a known group.



Insikt Group utilizes a simple color and phonetic alphabet naming convention for new nation state threat actor groups or campaigns. The color corresponds to that nation's flag colors, currently represented below, with more color/nation pairings to be added as we identify and attribute new threat actor groups associated with new nations.



For newly identified cybercriminal groups, Insikt Group uses a naming convention corresponding to the Greek alphabet. Where we have identified a criminal entity connected to a particular country, we will use the appropriate country color, and where that group may be tied to a specific government organization, tie it to that entity specifically.

Insikt Group uses mathematical terms when naming newly identified malware.

About Recorded Future

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture.