MANDIANT ADVANTAGE

Event Coverage/Implication

Suspected TEMP[.]Zagros Infrastructure Identified

Cyber Espionage (CE) Fusion (FS)

February 21, 2023 09:05:55 PM, 23-00003340, Version: 1

Executive Summary

- Mandiant uncovered new infrastructure that we assess with moderate confidence is used by TEMP[.]Zagros potentially for scanning and command and control.
- Some identified servers are likely used in operations employing well-known remote control programs, which aligns with TEMP[.]Zagros tactics, techniques, and procedures.
- These findings represent a threat to organizations of interest to the Iranian Government.
- Please see the Technical Annex for related samples.

Threat Detail

Mandiant identified suspicious infrastructure that shares similar URI patterns and appears to be running on open-source software. Network communications and online submission data suggests this infrastructure has been used against government, media, telecommunications, and financial targets in the Middle East, North Africa, and South Asia since early 2022.

- The infrastructure (Table 1) shares similar URI patterns and appears to run on Werkzeug to create web servers:
  - http://<IP_address>/apiy7?<11_chars_ID>=<11_chars_ID>
  - http://<IP_address>/apiv4?<7_char_token>=<7_char_token>
  - hxxp://<IP_address>/getcb[.]aspx?<11_chars_ID>=<11_chars_ID>
  - hxxp://<IP_address>/main[.]aspx?<11_chars_ID>=<11_chars_ID>
- Netflow data suggests that network traffic occurred between some of the identified servers and the government and media sectors in Israel and Kuwait.
- Users believed to be associated with a financial solutions entity and the telecommunications industry in Egypt and Afghanistan also submitted related URLs to a public malware repository.

IPs		
137[.]74[.]131[.]30	85[.]239[.]55[.]147	51[.]254[.]25[.]39
159[.]69[.]45[.]212	141[.]95[.]177[.]141	157[.]90[.]153[.]60
45[.]86[.]22[.]23	65[.]21[.]183[.]238	157[.]90[.]152[.]26
45[.]86[.]228[.]23	91[.]121[.]240[.]104	178[.]32[.]30[.]3

Table 1: Suspected TEMP[.]Zagros infrastructure

Identified infrastructure can be found in Table 2, of which two servers are believed to be command and control (C&C) servers for SimpleHelp, 164[.]132[.]237[.]78 and 5[.]196[.]249[.]160[.]

IPs	
5[.]196[.]249[.]160	141[.]95[.]177[.]130
164[.]132[.]237[.]78	141[.]95[.]177[.]140

Table 2: Additional suspected TEMP[.]Zagros infrastructure

Suspected Ties to TEMP[.]Zagros

We assess with moderate confidence this infrastructure is used by TEMP[.]Zagros potentially for scanning and C&C operations based on the identification of servers believed to act as C&C servers for SimpleHelp-related payloads and targeting consistencies.

- At least three servers are believed to be SimpleHelp C&C servers: 164[.]132[.]237[.]78, 5[.]196[.]249[.]160, and 178[.]32[.]30[.]3[.] Suspected TEMP[.]Zagros activity has been associated with the use of legitimate remote access tools, including SimpleHelp (22-00027414), SYNCRO (22-00025782), RemoteUtilities, and ScreenConnect (22-00000674, 22-00015666), which allow full access to victims' computers.
- We attribute some of this infrastructure and related samples in the Technical Annex to UNC3313, an activity cluster with moderate confidence ties to TEMP[.]Zagros.
- The IPs 91[.]121[.]240[.]104 and 178[.]32[.]30[.]3 share the URI template noted above and have been publicly reported as being linked to TEMP[.]Zagros-associated activity.
  - hxxp://178[.]32[.]30[.]3/apiy7?znq08v2u9m6=znq08v2u9m6
  - hxxp://91[.]121[.]240[.]104:443/apiy7?BPT8JQR6TP0=BPT8JQR6TP0
- The assessed targeting, while not confirmed, is consistent with TEMP[.]Zagros operational interests.

Outlook and Implications

The findings associated with the discovery of related infrastructure is consistent with TEMP[.]Zagros' use of legitimate remote access software and ongoing interest in the Middle East region. We anticipate that TEMP[.]Zagros-related activity will continue to pose a threat to government and telecommunications entities within the Middle East region and the region's periphery in the long term.

Technical Annex

Related Samples

- Remote Work-linux64-online[.]tar (MD5: 6441d645ad73a076675b10fcf4dbfafd)
  - SimpleHelp Remote Work-linux64-online (MD5: aead7f21f77e80687e020dbfb1dee6b7)
  - Simple Help remote access tool
  - C&C: 178[.]32[.]30[.]3
- UNAVAILABLE (MD5: 5f71191ca2aff4738d9ca86e884e9afa)
  - VBA downloader
  - Downloads: hxxp://178[.]32[.]30[.]3:80/kz10n2f9d5c4pkz10n2f9s2vhkz10n2f9/gcwPu2KXdqEbDpJQ33/
  - Response content unavailable

Please rate this product by taking a short four question survey

First Version Publish Date

February 21, 2023 09:05:55 PM

Threat Intelligence Tags

Actors

- UNC3313
  Aliases
  - UNC 3313
  - UNC-3313
  - UNC3313

Intended Effects

- Military Advantage
- Political Advantage

Motivations

- Military/Security/Diplomatic

Source Geographies

- Iran

Tactics, Techniques And Procedures (TTPs)

- Enabling Infrastructures

Technical Indicators & Warnings

Identifier	Related
Network Type	network
IP	137[.]74[.]131[.]30

Identifier	Related
Network Type	network
IP	141[.]95[.]177[.]141

Identifier	Related
Network Type	network
IP	85[.]239[.]55[.]147

Identifier	Related
Network Type	network
IP	45[.]86[.]228[.]23

Identifier	Related
Network Type	network
IP	141[.]95[.]177[.]140

Identifier	Related
Network Type	network
IP	157[.]90[.]152[.]26

Identifier	Related
Network Type	network
IP	5[.]196[.]249[.]160

Identifier	Related
Network Type	network
IP	45[.]86[.]22[.]23

Identifier	Related
Network Type	network
IP	159[.]69[.]45[.]212

Identifier	Related
Network Type	network
IP	141[.]95[.]177[.]130

Identifier	Related
Network Type	network
IP	157[.]90[.]153[.]60

Identifier	Related
Network Type	network
IP	65[.]21[.]183[.]238

Identifier	Related
Network Type	network
IP	178[.]32[.]30[.]3

Identifier	Related
Network Type	network
IP	91[.]121[.]240[.]104

Identifier	Related
Network Type	network
IP	164[.]132[.]237[.]78

Identifier	Related
Network Type	network
IP	51[.]254[.]25[.]39

Identifier	Related
Actor	UNC3313
File Size	2365
File Name	mudwp1_edrvbs[.]vbs
MD5	5f71191ca2aff4738d9ca86e884e9afa
SHA1	fa73bee345b6f5d214917b5425bb2a6bd9b45de7
SHA256	fb69c821f14cb0d89d3df9eef2af2d87625f333535eb1552b0fcd1caba38281f
Type	text/plain

Identifier	Attacker
Actor	UNC3313
File Size	3194880
File Name	UNAVAILABLE
MD5	6441d645ad73a076675b10fcf4dbfafd
SHA1	f8b87549a03f00073944471f42c6719163ea8406
SHA256	94fce6c44814a087f02cab585c347f9b9564aad8ab09ac5d29fba721950833c5
Type	application/x-tar

Identifier	Related
Actor	UNC3313
File Size	3186519
File Name	SimpleHelp Remote Work-linux64-online
MD5	aead7f21f77e80687e020dbfb1dee6b7
SHA1	9f2ede235a7f205942c452f10ef6ee08cfc16296
SHA256	82b616b2c205b13fc0451a6fdbf51ec1be0e7317a46f5f1b3ad081e6d848258a
Type	application/x-executable

Version Information

Version:1, February 21, 2023 09:05:55 PM