Espionage Campaign Targets Telecoms Organizations across Middle East and Asia

symantec-enterprise-blogs.security.com/blogs/threat-intelligence/espionage-campaign-telecoms-asia-middle-east

Threat Hunter TeamSymantec

Attackers most likely linked to Iran have attacked a string of telecoms operators in the Middle East and Asia over the past six months, in addition to a number of IT services organizations and a utility company.

Organizations in Israel, Jordan, Kuwait, Saudi Arabia, the United Arab Emirates, Pakistan, Thailand, and Laos were targeted in the campaign, which appears to have made no use of custom malware and instead relied on a mixture of legitimate tools, publicly available malware, and living-off-the-land tactics. While the identity of the attackers remains unconfirmed, there is some evidence to suggest a link to the Iranian Seedworm (aka MuddyWater) group. The targeting and tactics are consistent with Iranian-sponsored actors.

Attack outline

After breaching a targeted network, the attackers typically attempt to steal credentials and move laterally across the network. They appear to be particularly interested in Exchange Servers, deploying web shells onto them. In some cases, the attackers may be using compromised organizations as stepping stones to additional victims. Furthermore, some targets may have been compromised solely to perform supply-chain-type attacks on other organizations.

In most attacks, the infection vector is unknown. Evidence of a possible vector was found at only one target. A suspected ScreenConnect setup MSI appeared to have been delivered in a zipped file named “Special discount program.zip”, suggesting that it arrived in a spear-phishing email.

Telecoms attack

In one attack against a telecoms firm in the Middle East, which began in August 2021, the first evidence of compromise was the creation of a service to launch an unknown Windows Script File (WSF). Scripts were then used to issue various domain, user discovery, and remote service discovery commands.

The attackers used PowerShell to download another WSF and run it. Net group was used to query for the “exchange trusted subsystem” domain group.

The attackers used Certutil to download a suspected Ligolo tunneling tool and launch WMI, which was used to get remote machines to carry out the following tasks:

- Execute Certutil to download an unknown file
- Execute Certutil to download an unknown WSF file and execute Wscript to launch this script
- Execute PowerShell to download and execute content
- Execute PowerShell to download a suspected web shell to an Exchange Server

Based on process lineage data, attackers seemed to use scripts extensively. These may be automated scripts used for collecting information and downloading additional tools. However, in one instance, a command asks cURL for help, suggesting that there may have been at least some hands-on-keyboard activity on the part of the attackers.

The attackers then used a remote access tool, believed to be eHorus, to perform the following tasks:

- Deliver and run a suspected Local Security Authority Subsystem Service (LSASS) dumping tool
- Deliver what are believed to be Ligolo tunneling tools
- Execute Certutil to request a URL from Exchange Web Services (EWS) of what appears to be other targeted organizations

One feature of this attack against a telecoms organization is that the attackers may have attempted to pivot to other targets by connecting to the Exchange Web Services (EWS) of other organizations, another telecoms operator, and an electronic equipment company in the same region. The following commands were used:

- certutil.exe -urlcache –split [DASH]f hxxps://[REDACTED]/ews/exchange[.]asmx
- certutil.exe -urlcache -split [DASH]f hxxps://webmail.[REDACTED][.]com/ews

It is unclear what the intent of these requests is. It is possible the attackers were attempting to check connectivity to these organizations.

Possible supply chain attack

One target that appeared to be an outlier was a utility company in Laos. The infection vector may have been the exploit of a public-facing service since the first machine that appeared to be compromised was an IIS web server. Suspicious activity also had w3wp.exe in the process lineage.

The attackers then used PowerShell to:

- Download a suspected Ligolo tunneling tool
- Download an unknown PowerShell script
- Download an unknown XLS file

The attackers then used PowerShell to connect to a webmail server of an organization in Thailand. They also attempted to connect to IT-related servers belonging to another company in Thailand.

To facilitate credential theft, WMI was used to execute PowerShell to modify the registry to store passwords in plaintext in memory. In addition to this, an obfuscated version of the publicly available CrackMapExec tool appeared to be deployed.

Toolset

The attackers made heavy use of legitimate tools and publicly available hacking tools. These include:

- ScreenConnect: Legitimate remote administration tool
- RemoteUtilities: Legitimate remote administration tool

- eHorus: Legitimate remote administration tool
- Ligolo: Reverse tunneling tool
- Hidec: Command line tool for running a hidden window
- Nping: Packet generation tool
- LSASS Dumper: Tool that dumps credentials from Local Security Authority Subsystem Service (LSASS) process
- SharpChisel: Tunneling tool
- Password Dumper
- CrackMapExec: Publicly available tool that is used to automate security assessment of an Active Directory environment
- ProcDump: Microsoft Sysinternals tool for monitoring an application for CPU spikes and generating crash dumps, but which can also be used as a general process dump utility
- SOCKS5 proxy server: Tunneling tool
- Keylogger: Retrieves browser credentials
- Mimikatz: Publicly available credential dumping tool

Seedworm link?

There is some evidence to suggest that the Iranian Seedworm group was responsible for these attacks. Two IP addresses used in this campaign have been previously linked to Seedworm activity. However, Seedworm is known to regularly switch its infrastructure, meaning conclusive attribution cannot be made.

There is also some overlap in tools between this campaign and earlier Seedworm campaigns. ScreenConnect, RemoteUtilities, SharpChisel, Ligolo, ProcDump, and Password Dumper were all referenced by Trend Micro in a March 2021 blog on Seedworm activity.

In the case of two tools – SharpChisel and Password Dumper – identical versions were used in this campaign to those that were documented by Trend.

Focused campaign

If these attacks are linked to Iran, it will not be the first time an Iranian threat actor has targeted the telecoms sector. In 2018, Symantec revealed that the Chafer group had compromised of a major telecoms services provider in the Middle East.

While the ultimate end goal of the campaign remains unknown, the focus on telecoms operators suggests that the attackers are gathering intelligence on the sector and possibly attempting to pivot into spying on communications.

Protection/Mitigation

For the latest protection updates, please visit the Symantec Protection Bulletin.

Indicators of Compromise

ae5d0ad47328b85e4876706c95d785a3c1387a11f9336844c39e75c7504ba365 – Ligolo e0873e15c7fb848c1be8dc742481b40f9887f8152469908c9d65930e0641aa6b – Ligolo

22e7528e56dffaa26cfe722994655686c90824b13eb51184abfe44d4e95d473f – Hidec

b0b97c630c153bde90ffeefc4ab79e76aaf2f4fd73b8a242db56cc27920c5a27 – Nping

b15dcb62dee1a8499b8ac63064a282a06abf0f7d0302c5e356cdb0c7b78415a9 – LSASS Dumper

61f83466b512eb12fc82441259a5205f076254546a7726a2e3e983011898e4e2 – SharpChisel

ccdddd1ebf3c5de2e68b4dcb8fbc7d4ed32e8f39f6fdf71ac022a7b4d0aa4131 – Password Dumper

facb00c8dc1b7ed209507d7c56d18b2c542c4e0b2986b9bfaf1764d8e252576b – CrackMapExec

1a107c3ece1880cbbdc0a6c0817624b0dd033b02ebaf7fa366306aaca22c103d – ProcDump

916cc8d6bf2282ae0d2db587f4f96780af59e685a1f1a511e0b2b276669dc802 – ProcDump

e2a7a9a803c6a4d2d503bb78a73cd9951e901beb5fb450a2821eaf740fc48496 – ProcDump

f6600e5d5c91ed30d8203ef2bd173ed0bc431453a31c03bc363b89f77e50d4c5 - SOCKS5 proxy server

6d73c0bcdf1274aeb13e5ba85ab83ec00345d3b7f3bb861d1585be1f6ccda0c5 – Keylogger

912018ab3c6b16b39ee84f17745ff0c80a33cee241013ec35d0281e40c0658d9 – Mimikatz

96632f716df30af567da00d3624e245d162d0a05ac4b4e7cbadf63f04ca8d3da – Mimikatz

bee3d0ac0967389571ea8e3a8c0502306b3dbf009e8155f00a2829417ac079fc – Mimikatz

d9770865ea739a8f1702a2651538f4f4de2d92888d188d8ace2c79936f9c2688 - Mimikatz