Harvester: Nation-state-backed group uses new toolset to target victims in South Asia

symantec-enterprise-blogs.security.com/blogs/threat-intelligence/harvester-new-apt-attacks-asia

A previously unseen actor, likely nation-state-backed, is targeting organizations in South Asia, with a focus on Afghanistan, in what appears to be an information-stealing campaign using a new toolset.

The Harvester group uses both custom malware and publicly available tools in its attacks, which began in June 2021, with the most recent activity seen in October 2021. Sectors targeted include telecommunications, government, and information technology (IT). The capabilities of the tools, their custom development, and the victims targeted, all suggest that Harvester is a nation-state-backed actor.

New toolset deployed

The most notable thing about this campaign is the previously unseen toolset deployed by the attackers.

The attackers deployed a custom backdoor called Backdoor.Graphon on victim machines alongside other downloaders and screenshot tools that provided the attackers with remote access and allowed them to spy on user activities and exfiltrate information.

We do not know the initial infection vector that Harvester used to compromise victim networks, but the first evidence we found of Harvester activity on victim machines was a malicious URL. The group then started to deploy various tools, including its custom Graphon backdoor, to gain remote access to the network. The group also tried to blend its activity in with legitimate network traffic by leveraging legitimate CloudFront and Microsoft infrastructure for its command and control (C&C) activity.

Tools used:

- Backdoor.Graphon - custom backdoor that uses Microsoft infrastructure for its C&C activity
- Custom Downloader - uses Microsoft infrastructure for its C&C activity
- Custom Screenshotter - periodically logs screenshots to a file

- Cobalt Strike Beacon - uses CloudFront infrastructure for its C&C activity (Cobalt Strike is an off-the-shelf tool that can be used to execute commands, inject other processes, elevate current processes, or impersonate other processes, and upload and download files)

- Metasploit - an off-the-shelf modular framework that can be used for a variety of malicious purposes on victim machines, including privilege escalation, screen capture, to set up a persistent backdoor, and more.

The custom downloader used by the attackers leverages the Costura Assembly Loader. Once on a victim machine, it checks if the following file exists:

> [ARTEFACTS_FOLDER]\winser.dll

If the file does not exist it downloads a copy from the following URL:

> hxxps://outportal[.]azurewebsites.net/api/Values_V2/Getting3210

Next, the sample creates the following file if it does not exist:

> "[ARTEFACTS_FOLDER]\Microsoft Services[.]vbs"

Then it sets the following registry value to create a loadpoint:

> HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\"MicrosoftSystemServices" = "[ARTEFACTS_FOLDER]\Microsoft Services[.]vbs"

Finally it opens an embedded web browser within its own UI using the following URL:

> hxxps://usedust[.]com

While it initially appeared that this URL may have been a loadpoint for Backdoor.Graphon, upon further investigation it appears to be a decoy to confuse any affected users.

Backdoor.Graphon is compiled as a .NET PE DLL with export “Main” and the following PDB file name:

> D:\OfficeProjects\Updated Working Due to Submission\4.5\Outlook_4.5\Outlook 4.5.2 32 bit New without presistancy\NPServices\bin\x86\Debug\NPServices[.]pdb

When this is executed, it attempts to communicate with the attackers’ C&C servers, which are hosted on Microsoft infrastructure.

- hxxps://microsoftmsdn[.]azurewebsites.net/api/Values_V1/AuthAsyncComplete_V1?Identity=[INFECTION_ID]
- hxxps://microsoftsgraphapi[.]azurewebsites.net/api/Values_V1/AuthAsyncComplete_V1?Identity=[INFECTION_ID]
- hxxps://msdnmicrosoft.azurewebsites[.]net/api/Values_V1/AuthAsyncComplete_V1?Identity=[INFECTION_ID]

The attackers then run commands to control their input stream and capture the output and error streams. They also periodically send GET requests to the C&C server, with the content of any returned messages extracted and then deleted.

Data that cmd.exe pulled from the output and error streams is encrypted and sent back to the attackers’ servers.

The custom screenshot tool was also packed with the Costura Assembly Loader. The screenshot tool takes photos that it saves to a password-protected ZIP archive for exfiltration, with all archives older than a week deleted.

Ongoing activity

While we do not have enough evidence yet to attribute Harvester's activity to a specific nation state, the group's use of custom backdoors, the extensive steps taken to hide its malicious activity, and its targeting all point to it being a state-sponsored actor. Harvester's use of legitimate infrastructure to host its C&C servers in order to blend in with normal network traffic is one example of the stealthy steps taken by this actor.

The targeting of organizations in Afghanistan in this campaign is also interesting given the huge upheaval seen in that country recently. The activity carried out by Harvester makes it clear the purpose of this campaign is espionage, which is the typical motivation behind nation-state-backed activity.

That Harvester's most recent activity was seen earlier this month means that organizations in the sectors and geographies mentioned should be alert to the malicious activity outlined in this blog.

Protection

File based:

> Backdoor.Graphon

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

Indicators of Compromise

0740cc87a7d028ad45a3d54540b91c4d90b6fc54d83bb01842cf23348b25bc42

303f93cc47c58e64665f9e447ac11efe5b83f0cfe4253f3ff62dd7504ee935e0

3c34c23aef8934651937c31be7420d2fc8a22ca260f5afdda0f08f4d3730ae59

3c8fa5cc50eb678d9353c9f94430eeaa74b36270c13ba094dc5c124259f0dc31

470cd1645d1da5566eef36c6e0b2a8ed510383657c4030180eb0083358813cd3

691e170c5e42dd7d488b9d47396b633a981640f8ab890032246bf37704d4d865

a4935e31150a9d6cd00c5a69b40496fea0e6b49bf76f123ea34c3b7ea6f86ce6

c4b6d7e88a63945f3e0768657e299d2d3a4087266b4fc6b1498e2435e311f5d1

cb5e40c6702e8fe9aa64405afe462b76e6fe9479196bb58118ee42aba0641c04

d84a9f7b1d70d83bd3519c4f2c108af93b307e8f7457e72e61f3fa7eb03a5f0d

f4a77e9970d53fe7467bdd963e8d1ce44a2d74e3e4262cd55bb67e7b3001c989

URL

hxxps://perfect-couple.com/perfectcouple[.]exe – sample was downloaded from this address

BLOG UPDATED *2.45pm, October 18, 2021: Minor updates made for clarity*

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.