Threat Hunter TeamSymantecTwitterLinkedInPosted: 5 Apr, 20225 Min ReadThreat IntelligenceFollowtwitterlinkedin

Cicada: Chinese APT Group Widens Targeting in Recent Espionage Activity

Government orgs and NGOs among victims in a wide-ranging and sustained campaign.

A Chinese state-backed advanced persistent threat (APT) group is attacking organizations around the globe in a likely espionage campaign that has been ongoing for several months.

Victims in this Cicada (aka APT10) campaign include government, legal, religious, and non-governmental organizations (NGOs) in multiple countries around the world, including in Europe, Asia, and North America. The wide number of sectors and geographies of the organizations targeted in this campaign is interesting. Cicada's initial activity several years ago was heavily focused on Japanese-linked companies, though in more recent times it has been linked to attacks on managed service providers (MSPs) with a more global footprint. However, this campaign does appear to indicate a further widening of Cicada's targeting.

The attribution of this activity to Cicada is based on the presence on victim networks of a custom loader and custom malware that are believed to be exclusively used by the APT group.

While Cicada has been linked to espionage-style operations dating back to 2009, the earliest activity in this current campaign occurred in mid-2021, with the most recent activity seen in February 2022, so this is a long-running attack campaign that may still be ongoing, researchers from Symantec, a division of Broadcom, have found.

Activity on infected networks

In several cases, the initial activity on victim networks is seen on Microsoft Exchange Servers, suggesting the possibility that a known, unpatched vulnerability in Microsoft Exchange may have been used to gain access to victim networks in some cases.

Once the attackers have successfully gained access to victim machines we observe them deploying various different tools, including a custom loader and the Sodamaster backdoor. The loader deployed in this campaign was also deployed in a previous Cicada attack.

Sodamaster is a known Cicada tool that is believed to be exclusively used by this group. It is a fileless malware that is capable of multiple functions, including evading detection in a sandbox by checking for a registry key or delaying execution; enumerating the username, hostname, and operating system of targeted systems; searching for running processes, and downloading and executing additional payloads. It is also capable of obfuscating and encrypting traffic that it sends back to its command-and-control (C&C) server. It is a powerful backdoor that Cicada has been using since at least 2020.

In this campaign, the attackers are also seen dumping credentials, including by using a custom Mimikatz loader. This version of Mimikatz drops mimilib.dll to obtain credentials in plain text for any user that is accessing the compromised host and provides persistence across reboots.

The attackers also exploit the legitimate VLC Media Player by launching a custom loader via the VLC Exports function, and use the WinVNC tool for remote control of victim machines.

Other tools utilized in this attack campaign include:

- RAR archiving tool - can be used to compress, encrypt, or archive files, likely for exfiltration.
- System/Network discovery - a way for attackers to determine what systems or services are connected to an infected machine.
- WMIExec - Microsoft command-line tool that can be used to execute commands on remote computers.
- NBTScan - an open-source tool that has been observed being used by APT groups to conduct internal reconnaissance within a compromised network.

Victims

The victims in this campaign appear to primarily be government-related institutions or NGOs, with some of these NGOs working in the fields of education and religion. There were also victims in the telecoms, legal, and pharmaceutical sectors.

The victims are spread through a wide number of regions including the U.S., Canada, Hong Kong, Turkey, Israel, India, Montenegro, and Italy. There is also just one victim in Japan, which is notable due to Cicada's previous strong focus on Japanese-linked companies.

The attackers spent as long as nine months on the networks of some victims.

The victims targeted, the various tools deployed in this campaign, and what we know of Cicada's past activity all indicate that the most likely goal of this campaign is espionage. Cicada activity was linked by U.S. government officials to the Chinese government in 2018.

Significance of this activity

This is a long-running campaign from a sophisticated and experienced nation-state-backed actor that may still be ongoing, as the most recent activity we saw in this campaign was in February 2022. The targeting of multiple large organizations in different geographies at the same time would require a lot of resources and skills that are generally only seen in nation-state backed groups, and shows that Cicada still has a lot of firepower behind it when it comes to its cyber activities.

Protection

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

Indicators of Compromise (IOCs)

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

01b610e8ffcb8fd85f2d682b8a364cad2033c8104014df83988bc3ddfac8e6ec

056c0628be2435f2b2031b3287726eac38c94d1e7f7aa986969baa09468043b1

062ce400f522f90909ed5c4783c5e9c60b63c09272e2ddde3d13e748a528fa88

0b452f7051a74a1d4a544c0004b121635c15f80122dc6be54db660ceb2264d6f

0ec48b297dd1b0d6c3ddd15ab63f405191d7a849049feedfa7e44096c6f9d42a

20fc3cf1afcad9e6f19e9abebfc9daf374909801d874c3d276b913f12d6230ec

2317d3e14ab214f06ae38a729524646971e21b398eda15cc9deb8b00b231abc3

2417da3adebd446b9fcb8b896adb14ea495a4d923e3655e5033f78d8e648fcc8

37f56127226ce96af501c8d805e76156ca6b87da1ba1bb5d227100912f6c52d9

3aa54e7d99b69a81c8b25ab57aeb971644ed0a206743c9e51a80ec1852f03663

3ff2d6954a6b62afb7499e1e317af64502570181fd49ac5a74e2f7947e2e89db

4f6a768841595293146ca04f879efa988e4e95ce0f2bc299cb669fea55e78b65

5269db6b19a1d758c75e58ee9bbf2f8fd684cfedbfe712d5b0182d7bbd3a1690

5bc68df582c86c884b563b15057cc223f2e9bc1022ebb297e32a9a7e3036228b

6b4692029f05489ecda10e11cfacfc3b19097856b88647d3695f3bdc7dd83ce9

7b581c0305c78f28bad60028c63e852dc34fc9e28f39e4b0af73d80c1d9680c9

83030f299a776114878bcd2ade585d97836ef4ddb6943cb796be2c88bcb83a83

90a03dabfc4e56a12cc3bac5cbe991db044b900a01ec341803c864506e467ffa

9917a2213f114e87745867e5fea6717efd727d7c08fdc851969224be2f0e019b

9b5f9ff82ed238bcbd83628ed3ec84988dc05f81cec9e45a512fbd2c8ac45c33

adfe177ade7d9bfe4df251a69678102aec1104a4ba9f73032dd90aba76d8bdd9

b76fde584f87c88bdd21fab613335ce7fc05788aa4bb3191d1517ec16ef4d11a

ce45af43dd2af52d6034e981515474147802efdfe036e00078fee29a01694fd6

d461347388ccf0c2008332a1674885a41f70b94b2263bddef44e796d3b1b43b5

df993dca434c3cd2da94b6a90b0ae1650d9c95ea1d5f6a5267aca640d8c6d00e

ee46e714660f7652502d5b3633fae0c08c8018f51cfb56a487afd58d04dd551a

fe33fdd5a63fee62362c9db329dde11080a0152e513ef0e6f680286a6a7b243f

88[.]198.101[.]58

168[.]100.8[.]38

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.

Want to comment on this post?

We encourage you to share your thoughts on your favorite social platform.

TwitterLinkedIn