Japan-Linked Organizations Targeted in Long-Running and Sophisticated Attack Campaign

symantec-enterprise-blogs.security.com/blogs/threat-intelligence/cicada-apt10-japan-espionage

Posted: 17 Nov, 20208 Min ReadThreat Intelligence

Evidence that advanced persistent threat group Cicada is behind attack campaign targeting companies in 17 regions and multiple sectors.

A large-scale attack campaign is targeting multiple Japanese companies, including subsidiaries located in as many as 17 regions around the globe in a likely intelligence-gathering operation.

Companies in multiple sectors are targeted in this campaign, including those operating in the automotive, pharmaceutical, and engineering sector, as well as managed service providers (MSPs).

The scale and sophistication of this attack campaign indicates that it is the work of a large and well-resourced group, with Symantec, a division of Broadcom (NASDAQ: AVGO), discovering enough evidence to attribute it toCicada (aka APT10, Stone Panda, Cloud Hopper).Cicada has been involved in espionage-type operations since 2009, and U.S. government officials have linked the activities of APT10, which we track as Cicada, to the Chinese government.

Cicada has historically been known to target Japan-linked organizations, and has also targeted MSPs in the past. The group is using living-off-the-land tools as well as custom malware in this attack campaign, including a custom malware - Backdoor.Hartip - that Symantec has not seen being used by the group before. Among the machines compromised during this attack campaign were domain controllers and file servers, and there was evidence of files being exfiltrated from some of the compromised machines.

The attackers extensively use DLL side-loading in this campaign, and were also seen leveraging the ZeroLogon vulnerability that was patched in August 2020.

How was this campaign discovered?

This campaign was first discovered by Symantec when suspicious DLL side-loading activity on one of our customer's networks triggered an alert in our Cloud Analytics technology, which is available in Symantec Endpoint Security Complete (SESC). This activity was then reviewed by our Threat Hunter analysts before being passed on to our investigations team for further analysis.

Cloud Analytics leverages artificial intelligence in order to comb through Symantec's vast data and spot patterns associated with targeted attacks. It is capable of automatically flagging incidents that would otherwise have taken thousands of hours of analyst time to identify. The initial Cloud Analytics alert allowed our threat hunting team to identify further victims of this activity, build a more complete picture of this campaign, and attribute this activity to Cicada. It also allowed us to update and create new protections to ensure our customers are protected from this activity.

Victims

This campaign has been ongoing since at least mid-October 2019, right up to the beginning of October 2020, with the attack group active on the networks of some of its victims for close to a year. The campaign is very wide-ranging, with victims in a large number of regions worldwide.

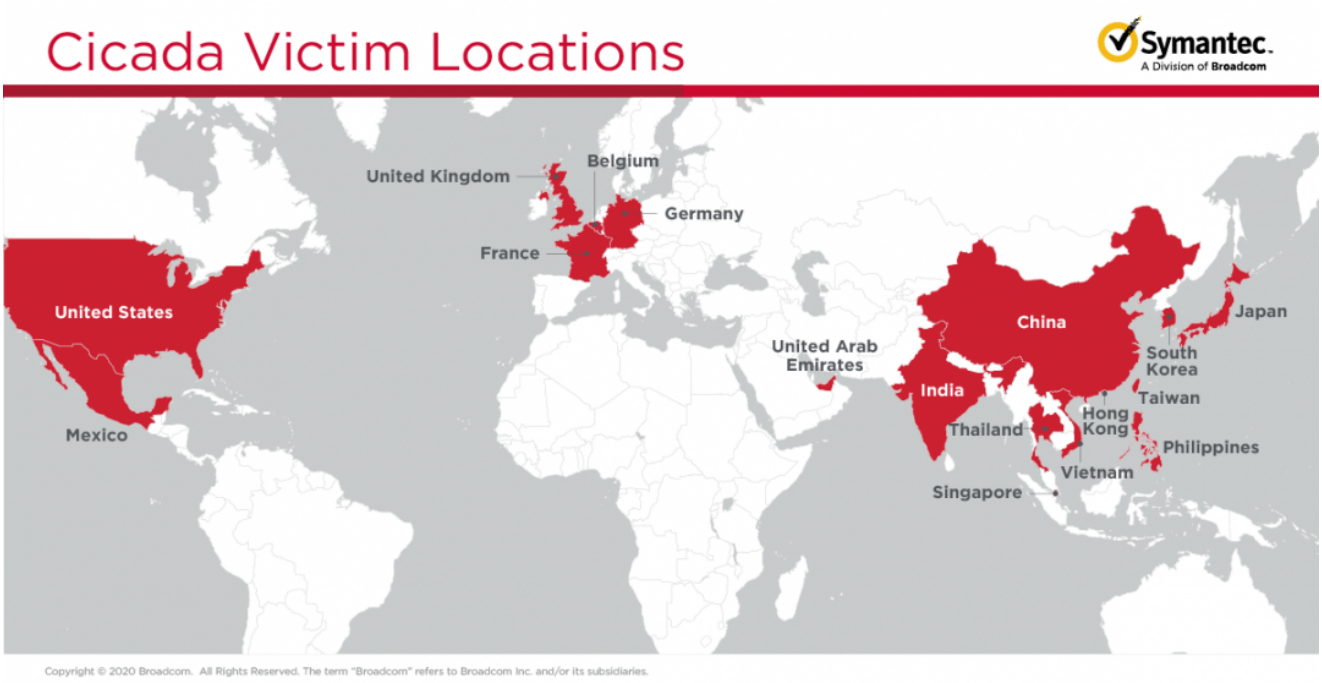


Figure 1. Locations of some of the companies targeted in this campaign; most of those targeted have links to Japan or Japanese organizations

The companies hit are, in the main, large, well-known organizations, many of which have links to Japan or Japanese companies, which is one of the main factors tying the victims together. Cicada has been known to have a strong focus on Japanese organizations in previous attack campaigns. As is clear from the map in *Figure 1*, South and East Asia are strong areas of focus for the attackers in this campaign. It is unusual to see a reportedly Chinese-government-linked group attacking companies within China's borders but, like many of the companies targeted in this campaign, the target in that instance is a subsidiary of a Japanese organization.

We also saw similar loaders on all the victim networks. These are among the main factors linking these victims together, with all of them coming from a wide variety of sectors, including:

- Automotive, with some manufacturers and organizations involved in supplying parts to the motor industry also targeted, indicating that this is a sector of strong interest to the attackers
- Clothing
- Conglomerates
- Electronics
- Engineering
- General Trading Company
- Government
- Industrial Products
- Managed Service Providers

- Manufacturing
- Pharmaceutical
- Professional Services

The amount of time the attackers spent on the networks of victims varied, with the attackers spending a significant amount of time on the networks of some victims, while spending just days on other victim networks. In some cases, too, the attackers spent some time on a network but then the activity would cease, but start again some months later.

Tactics, tools, and procedures

We observed the attackers using a wide variety of living-off-the-land, dual-use, and publicly available tools and techniques in these attacks, including:

- Network Reconnaissance – gathering information from machines on the network.
- Credential Theft – stealing user names and passwords, potentially to provide them with further access to the victim network.
- RAR archiving – files are transferred to staging servers before exfiltration. They may be encrypted or compressed, to make them easier to extract.
- Certutil – a command-line utility that can be exploited and used for various malicious purposes, such as to decode information, to download files, and to install browser root certificates.
- Adfind – a command-line tool that can be used to perform Active Directory queries.
- Csvde – can be used to extract Active Directory files and data.
- Ntdsutil – can be used as a credential-dumping tool.
- WMIExec – can be used for lateral movement and to execute commands remotely.
- PowerShell - a powerful interactive command-line interface and scripting environment included in the Windows operating system. It can be used to find information and execute code, and is frequently abused by malicious actors.

The threat actors also use a legitimate cloud file-hosting service for exfiltration.

The attackers also use DLL side-loading at multiple stages during the attack, including using it to load Backdoor.Hartip. DLL side-loading occurs when attackers are able to replace a legitimate library with a malicious one, allowing them to load malware into legitimate processes. Attackers use DLL side-loading to try and hide their activity by making it look legitimate, and it also helps them avoid detection by security software. It is a tactic that is commonly used by APT groups and has often been observed being used by nation-state backed actors. Monitoring networks for unusual activity, as Symantec's Cloud Analytics technology does, is key for detecting this kind of malicious activity.

The attackers were also seen deploying a tool capable of exploiting the ZeroLogon vulnerability (CVE-2020-1472). The critical elevation-of-privilege vulnerability was first disclosed and patched on August 11, 2020, and can allow attackers to spoof a domain controller account and then potentially use it to steal domain credentials, take over the domain, and completely compromise all Active Directory identity services. It has been exploited by multiple malicious actors since its disclosure, leading both Microsoft and the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) to issue warnings to Windows users to patch the issue as quickly as possible.

Links to Cicada

The scale and sophistication of this attack campaign indicate that it is the work of a large and well-resourced group, such as a nation-state actor, with Symantec discovering enough evidence to attribute it with medium confidence to Cicada.

Symantec analysts have linked this activity to Cicada due to the use of previously seen obfuscation techniques and shellcode on loader DLLs.

Activity seen in one of the victim organizations has various trait similarities with previously seen Cicada activity that was described in a blog by Cylance in 2019, including:

- Third-stage DLL has an export named "FuckYouAnti"
- Third-stage DLL uses CppHostCLR technique to inject and execute the .NET loader assembly
- .NET Loader is obfuscated with ConfuserEx v1.0.0
- Final payload is QuasarRAT – an open-source backdoor used by Cicada in the past

In another affected organization, the loaders deploying Backdoor.Hartip overlap in the obfuscation and shellcode used, making us confident it is the same actor in both organizations.

Similarities between activity in both organizations

- Side-loading DLL
- C++ usage
- API call sequence
- GetModuleFileName -> lstrcat -> CreateFile -> ReadFile
- Load next-stage payload from another file
- Obfuscation: lots of garbage OutputDebugString, _time64, srand, rand API calls

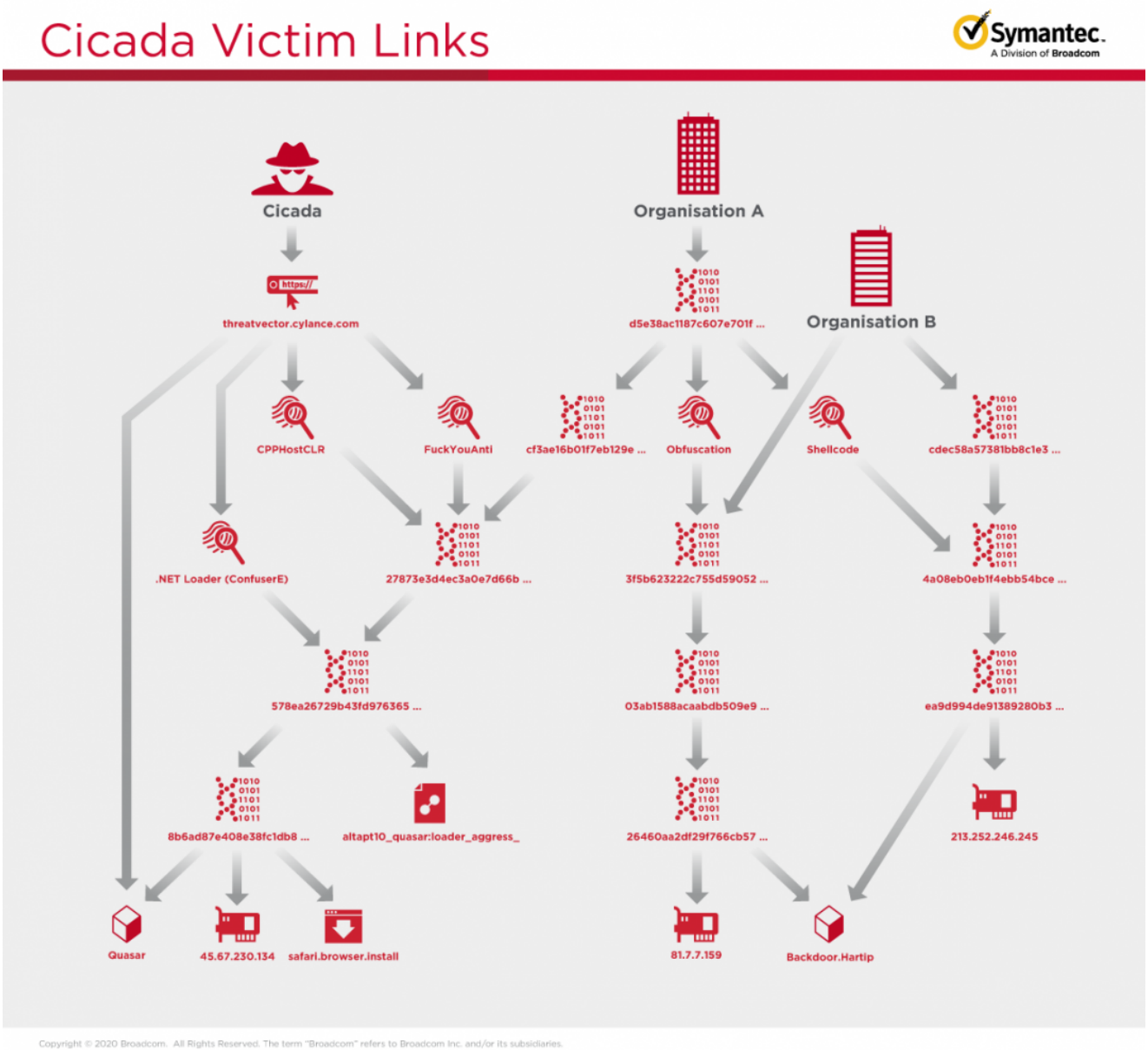


Figure 2. Image showing links between Cicada and two victim organizations in this campaign

These similarities leave us confident that this is the same group carrying out this activity in both organizations, and that this group is Cicada. Historically, Cicada has been seen using custom DLL loaders to decrypt and execute its final payload, as is observed in these attacks. We also saw similar loaders as those used in these two organizations used on other victim networks.

The scale of the operations also points to a group of Cicada's size and capabilities. 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. The link all the victims have to Japan also points towards Cicada, which has been known to target Japanese organizations in the past.

The targeting of MSPs is also a hallmark of Cicada's activity. Successfully compromising an MSP can give attackers high-level access to multiple companies without them having to compromise the individual companies' networks.

We have also seen Cicada utilizing some of the same publicly available tools – such as WMIExec – in the past. The attackers also take various steps to reduce the chances of their activity being spotted – including searching for security software on victim machines using WMIC, and using PowerShell to clear event logs to hide their activity once they are finished on victim machines. This kind of activity is the hallmark of sophisticated and experienced threat actors.

All of these facts point to Cicada being the perpetrator of these wide-ranging and sophisticated attacks.

Intelligence gathering and stealing information has generally been the motivation behind Cicada's attacks in the past, and that would appear to be the case in this attack campaign too. We observed the attackers archiving some folders of interest in these attacks, including in one organization folders relating to human resources (HR), audit and expense data, and meeting memos.

Conclusion

Japan-linked organizations need to be on alert as it is clear they are a key target of this sophisticated and well-resourced group, with the automotive industry seemingly a key target in this attack campaign. However, with the wide range of industries targeted by these attacks, Japanese organizations in all sectors need to be aware that they are at risk of this kind of activity.

Cicada clearly still has access to a lot of resources and skills to allow it to carry out a sophisticated and wide-ranging campaign like this, so the group remains highly dangerous. Its use of a tool to exploit the recently disclosed ZeroLogon vulnerability and a custom backdoor that has not been observed by Symantec before show that it continues to evolve its tools and tactics to actively target its victims.

The group's use of techniques such as DLL side-loading and a wide array of living-off-the-land tools underline the need for organizations to have a comprehensive security solution in place to detect this kind of suspicious activity before actors like Cicada have the chance to deploy malware or steal information from their networks.

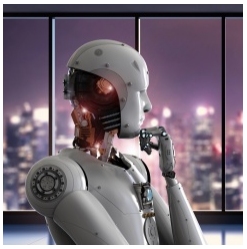
Protection/Mitigation

This activity was first discovered thanks to an alert triggered by our Cloud Analytics technology, which is available in Symantec Endpoint Security Complete (SESC).

Indicators of Compromise (IoCs)

8b6ad87e408e38fc1db868da6e643f616dac59fbae08382c4a7dd4ea119ea057
d5e38ac1187c607e701f506c4015bde94be6c485d566d004d810d7565c188743
26460aa2df29f766cb5712ebca44cb3365ebfdb5cae0b2ec36ef1e3568911d6a
cdec58a57381bb8c1e374efb0bf1897d89d1e096d2b704820893859d9f08d086
ea9d994de9138928 0b334f2af991baa49ca613a6bf898d7bb25f88cc66488f5c
3f5b623222c755d59052fab9e096c9d2b9a47d06b3a5de62fb9a66750af4efc4
27873e3d4ec3a0e7d66bee8bda4d65cc8fcefbdca2c8d5c049372a63ff0bc2ed
cf3ae16b01f7eb129e0e7387ac7feb61ecfce5db0d7494b3962c02c681f504d4
578ea26729b43fd976365a6700c80950e0b71a39e67bfff715423d60ae6bfab9
03ab1588acaabdb509e9db7cfe1e60522bc8baa13bbd35160b4bde7d1b6402ef
4a08eb0eb1f4ebb54bceabbebcb7da48238f0278ae5421326ee65ec7951e4239

178.73.210.238
188.119.112.225
213.252.246.245
45.14.224.93
45.67.230.134
81.7.7.159
95.179.143.32



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.