Carderbee: APT Group use Legit Software in Supply Chain Attack Targeting Orgs in Hong Kong

12.20pm BST, 22 August 2023: Updated with additional IoCs

A previously unknown advanced persistent threat (APT) group used the legitimate Cobra DocGuard software to carry out a supply chain attack with the goal of deploying the Korplug backdoor (aka PlugX) onto victim computers.

In the course of this attack, the attackers used malware signed with a legitimate Microsoft certificate. Most of the victims in this campaign are based in Hong Kong, with some victims based in other regions of Asia.

Korplug is known to be used by multiple APT groups, but we could not link this activity to a known threat actor so we have given the actor behind this activity a new name — Carderbee.

Cobra DocGuard and Previous Activity

Cobra DocGuard Client is software produced by a China-based company called EsafeNet and appears to legitimately be used to protect, encrypt, and decrypt software. EsafeNet is owned by Chinese information security firm NSFOCUS.

According to a report from ESET, in September 2022, a malicious update to this software was used to compromise a gambling company in Hong Kong. The same gambling company had been compromised in September 2021 using the same technique by Budworm (aka LuckyMouse, APT27), which led ESET to attribute this September 2022 attack to Budworm too. In that attack, a new variant of the Korplug malware was also found. In that instance, it used the magic header “ESET”, indicating that it may have been modified to try to bypass ESET products.

A signed version of Korplug was also used in the activity investigated by the Symantec Threat Hunter Team, part of Broadcom. This activity began in April 2023. However, we did not find any other evidence to indicate that this attack was carried out by Budworm. Korplug is a backdoor that is known to be used by multiple APTs, including APT41 and Budworm. We do not have any indication of the industry sectors of the companies targeted in this recent activity, just their geographic location.

Accordingly, it was not possible to link this activity definitively to a known group, which is why we attributed it to a new group, Carderbee.

Attack Chain

Malicious activity was seen on about 100 computers in impacted organizations; however, the Cobra DocGuard software was installed on around 2,000 computers, indicating that the attacker may be selectively pushing payloads to specific victims.

The malicious software was delivered to the following location on infected computers, which is what indicates that a supply chain attack or malicious configuration involving Cobra DocGuard is how the attackers compromised affected computers:

"csidl_system_drive\program files\esafenet\cobra docguard client\update"

Over a period of a few months in 2023, multiple distinct malware families were observed being deployed via this method. In one interesting case, a downloader deployed by the attackers had a digitally signed certificate from Microsoft, called Microsoft Windows Hardware Compatibility Publisher. This downloader was used to install the Korplug backdoor on targeted systems. The downloader attempted to download a file named update.zip from the following location: *http://cdn.stream-amazon[.]com/update.zip.*

The update.zip file is a zlib compressed archive file. It decompresses and executes a file named content.dll. This file is not saved on disk. It acts as a dropper and contains x64 and x86 drivers, which are dropped depending on the system environment. The dropper creates services and registry entries. The dropped drivers read encrypted data from the registry, decrypt it, and inject it into svchost.exe. The injected payload is the Korplug backdoor.

The Korplug sample downloaded here is able to:

- Execute commands via cmd
- Enumerate files

- Check running processes
- Download files
- Open firewall ports
- Act as a keylogger

Microsoft Certificate Abuse

Use of Microsoft-signed malware is a known problem. In December 2022, Mandiant noted a POORTRY driver sample signed with a Microsoft Windows Hardware Compatibility Authenticode signature. Most recently, in July 2023, Trend said that it had found a Microsoft-signed rootkit that appeared to have passed through the Windows Hardware Quality Labs (WHQL) process for getting a valid signature. Microsoft acknowledged the issue and said that drivers certified by Microsoft's Windows Hardware Developer Program (MWHDP) were being used maliciously in post-exploitation activity.

The company said it had investigated the issue and "determined that the activity was limited to the abuse of several developer program accounts and that no Microsoft account compromise has been identified." Malware signed with what appears to be a legitimate certificate can make it much harder for security software to detect.

Supply Chain Attack and Certificate Abuse

It seems clear that the attackers behind this activity are patient and skilled actors. They leverage both a supply chain attack and signed malware to carry out their activity in an attempt to stay under the radar. The fact that they appear to only deploy their payload on a handful of the computers they gain access to also points to a certain amount of planning and reconnaissance on behalf of the attackers behind this activity. Software supply chain attacks remain a major issue for organizations in all sectors, with multiple high-profile supply chain attacks occurring in the last 12 months, including the MOVEit, X_Trader, and 3CX attacks.

Some unanswered questions remain about the activity of Carderbee, such as what sectors the group was targeting with this activity, and whether there are any links between Carderbee and other actors such as Budworm.

Symantec researchers will continue to track this activity, and we share indicators of compromise below so our colleagues in the security community can do so as well.

Protection

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.

SHA256 file hashes:

96170614bbd02223dc79cec12afb6b11004c8edb8f3de91f78a6fc54d0844622

19a6a404605be964ab87905d59402e2890460709a1d9038c66b3fbeedc1a2343

1ff7b55dde007b7909f43dd47692f7c171caa2897d663eb9db01001062b1fe9d

2400d8e66c652f4f8a13c99a5ffb67cb5c0510144b30e93122b1809b58614936

2f714aaf9e3e3e03e8168fe5e22ba6d8c1b04cbfa3d37ff389e9f1568a80cad4

47b660bbaacb2a602640b5e2c589a3adc620a0bfc9f0ecfb8d813a803d7b75e2

5467e163621698b38c2ba82372bac110cea4121d7c1cec096958a4d9eaa44be7

7e6d0f14302662f52e4379eb5b69a3749d8597e8f61266aeda74611258972a3d

85fc7628c5c7190f25da7a2c7ee16fc2ad581e1b0b07ba4ac33cff4c6e94c8af

8bd40da84c8fa5f6f8e058ae7e36e1023aca1b9a9c8379704934a077080da76f

8ca135b2f4df6a714b56c1a47ac5baa80a11c6a4fcc1d84a047d77da1628f53f

9e96f70ce312f2638a99cfbd3820e85798c0103c7dc06fe0182523e3bf1e2805

9fc49d9f4b922112c2bafe3f1181de6540d94f901b823e11c008f6d1b2de218c

b5159f8ae16deda7aa5d55100a0eac6e5dacd1f6502689b543513a742353d1ea

b7b8ea25786f8e82aabe4a4385c6142d9afe03f090d1433d0dc6d4d6ccc27510

b84f68ab098ce43f9cb363d0a20a2267e7130078d3d2d8408bfb32bbca95ca37

f64267decaa982c63185d92e028f52c31c036e85b2731a6e0bccdb8f7b646e97

Remote IP addresses:

45.76.179[.]209

104.238.151[.]104

URLs:

http://111.231.100[.]228:8888/CDGServer3/UpgradeService2

http://103.151.28[.]11:8090/CDGServer3/UpgradeService2

Domains:

cdn.stream-amazon[.]com

cdn.ofo[.]ac

gobay[.]info

tjj.active-microsoft[.]com

githubassets.akamaixed[.]net

ms-g9-sites-prod-cdn.akamaixed[.]net

ms-f7-sites-prod-cdn.akamaixed[.]net