Aug 24 2023

NETMANAGEIT

Intelligence Report

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

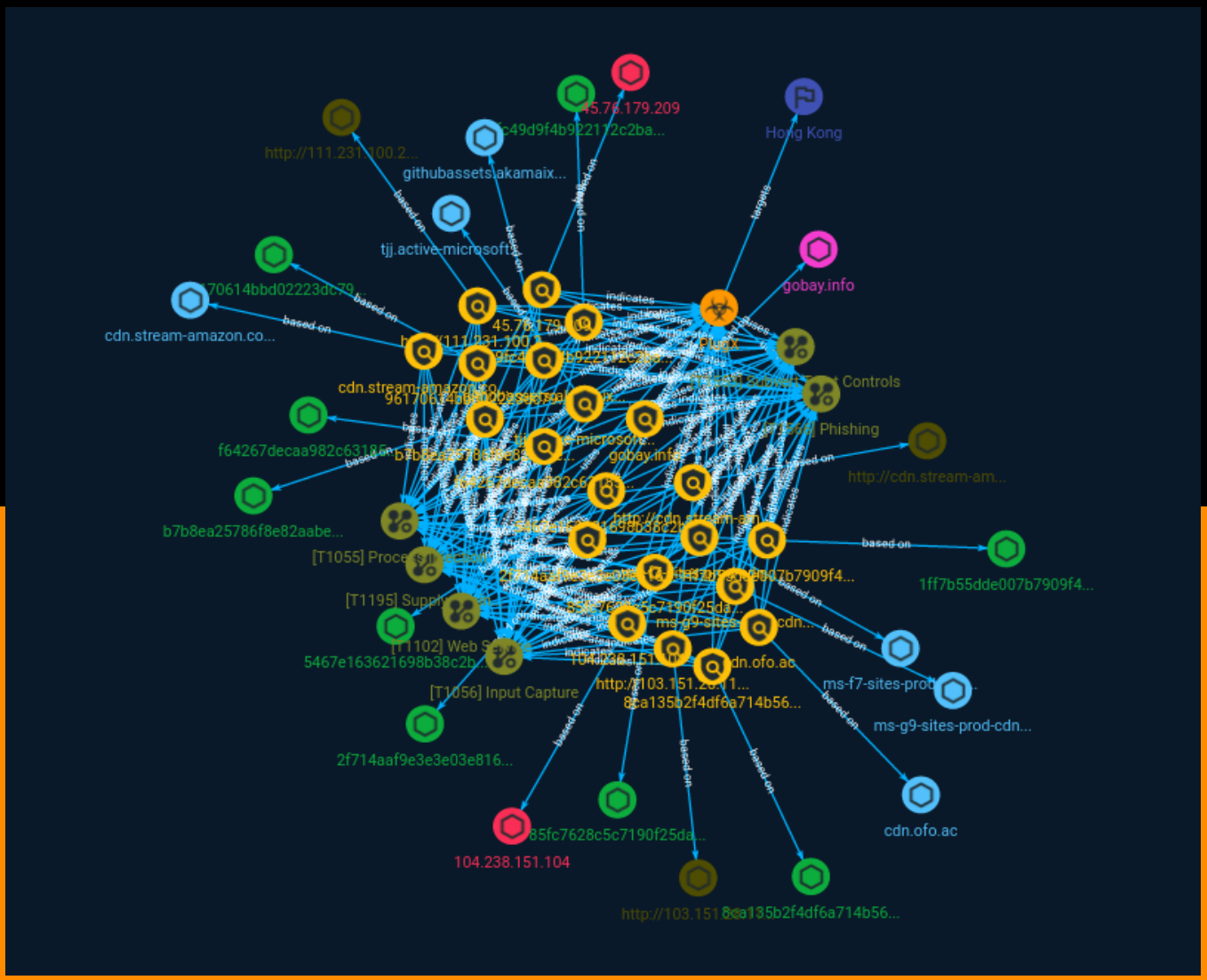

Table of contents

Overview

Entities

Observables

External References

Overview

Description

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.

Confidence

This value represents the confidence in the correctness of the data contained within this report.

15 / 100

Indicator

Name
85fc7628c5c7190f25da7a2c7ee16fc2ad581e1b0b07ba4ac33cff4c6e94c8af
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '85fc7628c5c7190f25da7a2c7ee16fc2ad581e1b0b07ba4ac33cff4c6e94c8af']
Name
ms-g9-sites-prod-cdn.akamaixed.net
Pattern Type
stix
Pattern
[hostname:value = 'ms-g9-sites-prod-cdn.akamaixed.net']
Name

96170614bbd02223dc79cec12afb6b11004c8edb8f3de91f78a6fc54d0844622

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '96170614bbd02223dc79cec12afb6b11004c8edb8f3de91f78a6fc54d0844622']

Name

1ff7b55dde007b7909f43dd47692f7c171caa2897d663eb9db01001062b1fe9d

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1ff7b55dde007b7909f43dd47692f7c171caa2897d663eb9db01001062b1fe9d']

Name

5467e163621698b38c2ba82372bac110cea4121d7c1cec096958a4d9eaa44be7

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5467e163621698b38c2ba82372bac110cea4121d7c1cec096958a4d9eaa44be7']

Name

9fc49d9f4b922112c2bafe3f1181de6540d94f901b823e11c008f6d1b2de218c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9fc49d9f4b922112c2bafe3f1181de6540d94f901b823e11c008f6d1b2de218c']

Name

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

Pattern Type

stix

Pattern

[hostname:value = 'ms-f7-sites-prod-cdn.akamaixed.net']

Name

45.76.179.209

Description

ISP: The Constant Company, LLC **OS:** None ---------- Hostnames: - 45.76.179.209.vultrusercontent.com ---------- Domains: - vultrusercontent.com

---------- Services: **5985:** ``` HTTP/1.1 404 Not Found Content-Type: text/html; charset=us-ascii Server: Microsoft-HTTPAPI/2.0 Date: Wed, 23 Aug 2023 04:58:48 GMT Connection: close Content-Length: 315 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.76.179.209']

Name

githubassets.akamaixed.net

Pattern Type

stix

Pattern

[hostname:value = 'githubassets.akamaixed.net']

Name

http://103.151.28.11:8090/CDGServer3/UpgradeService2

Pattern Type

stix

Pattern

[url:value = 'http://103.151.28.11:8090/CDGServer3/UpgradeService2']

Name
gobay.info
Pattern Type
stix
Pattern
[domain-name:value = 'gobay.info']
Name
8ca135b2f4df6a714b56c1a47ac5baa80a11c6a4fcc1d84a047d77da1628f53f
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '8ca135b2f4df6a714b56c1a47ac5baa80a11c6a4fcc1d84a047d77da1628f53f']
Name
b7b8ea25786f8e82aabe4a4385c6142d9afe03f090d1433d0dc6d4d6ccc27510
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' = 'b7b8ea25786f8e82aabe4a4385c6142d9afe03f090d1433d0dc6d4d6ccc27510']

Name

tjj.active-microsoft.com

Pattern Type

stix

Pattern

[hostname:value = 'tjj.active-microsoft.com']

Name

f64267decaa982c63185d92e028f52c31c036e85b2731a6e0bccdb8f7b646e97

Description

ConventionEngine_Term_Users

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f64267decaa982c63185d92e028f52c31c036e85b2731a6e0bccdb8f7b646e97']

Name

http://111.231.100.228:8888/CDGServer3/UpgradeService2

Pattern Type
stix
Pattern
[url:value = 'http://111.231.100.228:8888/CDGServer3/UpgradeService2']
Name
cdn.ofo.ac
Pattern Type
stix
Pattern
[hostname:value = 'cdn.ofo.ac']
Name
2f714aaf9e3e3e03e8168fe5e22ba6d8c1b04cbfa3d37ff389e9f1568a80cad4
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '2f714aaf9e3e3e03e8168fe5e22ba6d8c1b04cbfa3d37ff389e9f1568a80cad4']
Name

http://cdn.stream-amazon.com/update.zip.

Pattern Type

stix

Pattern

[url:value = 'http://cdn.stream-amazon.com/update.zip.']

Name

104.238.151.104

Description

CC=JP ASN=AS20473 AS-CHOOPA

Pattern Type

stix

Pattern

[ipv4-addr:value = '104.238.151.104']

Name

cdn.stream-amazon.com

Pattern Type

stix

Pattern

```
[hostname:value = 'cdn.stream-amazon.com']
```

Country

Name
Hong Kong

Malware

Name
PlugX

Description
[PlugX](https://attack.mitre.org/software/S0013) is a remote access tool (RAT) with modular plugins that has been used by multiple threat groups.(Citation: Lastline PlugX Analysis)(Citation: FireEye Clandestine Fox Part 2)(Citation: New DragonOK)(Citation: Dell TG-3390)

Attack-Pattern

Name

Supply Chain Compromise

ID

T1195

Description

Adversaries may manipulate products or product delivery mechanisms prior to receipt by a final consumer for the purpose of data or system compromise. Supply chain compromise can take place at any stage of the supply chain including: * Manipulation of development tools * Manipulation of a development environment * Manipulation of source code repositories (public or private) * Manipulation of source code in open-source dependencies * Manipulation of software update/distribution mechanisms * Compromised/infected system images (multiple cases of removable media infected at the factory)(Citation: IBM Storwize)(Citation: Schneider Electric USB Malware) * Replacement of legitimate software with modified versions * Sales of modified/counterfeit products to legitimate distributors * Shipment interdiction While supply chain compromise can impact any component of hardware or software, adversaries looking to gain execution have often focused on malicious additions to legitimate software in software distribution or update channels.(Citation: Avast CCleaner3 2018)(Citation: Microsoft Dofoil 2018)(Citation: Command Five SK 2011) Targeting may be specific to a desired victim set or malicious software may be distributed to a broad set of consumers but only move on to additional tactics on specific victims.(Citation: Symantec Elderwood Sept 2012)(Citation: Avast CCleaner3 2018)(Citation: Command Five SK 2011) Popular open source projects that are used as dependencies in many applications may also be targeted as a means to add malicious code to users of the dependency.(Citation: Trendmicro NPM Compromise)

Name

Subvert Trust Controls

ID

T1553

Description

Adversaries may undermine security controls that will either warn users of untrusted activity or prevent execution of untrusted programs. Operating systems and security products may contain mechanisms to identify programs or websites as possessing some level of trust. Examples of such features would include a program being allowed to run because it is signed by a valid code signing certificate, a program prompting the user with a warning because it has an attribute set from being downloaded from the Internet, or getting an indication that you are about to connect to an untrusted site. Adversaries may attempt to subvert these trust mechanisms. The method adversaries use will depend on the specific mechanism they seek to subvert. Adversaries may conduct [File and Directory Permissions Modification](https://attack.mitre.org/techniques/T1222) or [Modify Registry](https://attack.mitre.org/techniques/T1112) in support of subverting these controls. (Citation: SpectorOps Subverting Trust Sept 2017) Adversaries may also create or steal code signing certificates to acquire trust on target systems.(Citation: Securelist Digital Certificates)(Citation: Symantec Digital Certificates)

Name

Input Capture

ID

T1056

Description

Adversaries may use methods of capturing user input to obtain credentials or collect information. During normal system usage, users often provide credentials to various different locations, such as login pages/portals or system dialog boxes. Input capture

mechanisms may be transparent to the user (e.g. [Credential API Hooking](https://attack.mitre.org/techniques/T1056/004)) or rely on deceiving the user into providing input into what they believe to be a genuine service (e.g. [Web Portal Capture](https://attack.mitre.org/techniques/T1056/003)).

Name

Process Injection

ID

T1055

Description

Adversaries may inject code into processes in order to evade process-based defenses as well as possibly elevate privileges. Process injection is a method of executing arbitrary code in the address space of a separate live process. Running code in the context of another process may allow access to the process's memory, system/network resources, and possibly elevated privileges. Execution via process injection may also evade detection from security products since the execution is masked under a legitimate process. There are many different ways to inject code into a process, many of which abuse legitimate functionalities. These implementations exist for every major OS but are typically platform specific. More sophisticated samples may perform multiple process injections to segment modules and further evade detection, utilizing named pipes or other inter-process communication (IPC) mechanisms as a communication channel.

Name

Phishing

ID

T1566

Description

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns. Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](https://attack.mitre.org/techniques/T1564/008)).(Citation: Microsoft OAuth Spam 2022)(Citation: Palo Alto Unit 42 VBA Infostealer 2014) Another way to accomplish this is by forging or spoofing(Citation: Proofpoint-spoof) the identity of the sender which can be used to fool both the human recipient as well as automated security tools.(Citation: cyberproof-double-bounce) Victims may also receive phishing messages that instruct them to call a phone number where they are directed to visit a malicious URL, download malware,(Citation: sygnia Luna Month)(Citation: CISA Remote Monitoring and Management Software) or install adversary-accessible remote management tools onto their computer (i.e., [User Execution](https://attack.mitre.org/techniques/T1204)).(Citation: Unit42 Luna Moth)

Name

Web Service

ID

T1102

Description

Adversaries may use an existing, legitimate external Web service as a means for relaying data to/from a compromised system. Popular websites and social media acting as a mechanism for C2 may give a significant amount of cover due to the likelihood that hosts within a network are already communicating with them prior to a compromise. Using common services, such as those offered by Google or Twitter, makes it easier for adversaries to hide in expected noise. Web service providers commonly use SSL/TLS encryption, giving adversaries an added level of protection. Use of Web services may also protect back-end C2 infrastructure from discovery through malware binary analysis while

also enabling operational resiliency (since this infrastructure may be dynamically changed).

Domain-Name

Value
gobay.info

StixFile

Value
2f714aaf9e3e3e03e8168fe5e22ba6d8c1b04cbfa3d37ff389e9f1568a80cad4
5467e163621698b38c2ba82372bac110cea4121d7c1cec096958a4d9eaa44be7
f64267decaa982c63185d92e028f52c31c036e85b2731a6e0bccdb8f7b646e97
8ca135b2f4df6a714b56c1a47ac5baa80a11c6a4fcc1d84a047d77da1628f53f
96170614bbd02223dc79cec12afb6b11004c8edb8f3de91f78a6fc54d0844622
1ff7b55dde007b7909f43dd47692f7c171caa2897d663eb9db01001062b1fe9d
85fc7628c5c7190f25da7a2c7ee16fc2ad581e1b0b07ba4ac33cff4c6e94c8af
9fc49d9f4b922112c2bafe3f1181de6540d94f901b823e11c008f6d1b2de218c
b7b8ea25786f8e82aabe4a4385c6142d9afe03f090d1433d0dc6d4d6ccc27510

Hostname

Value
cdn.stream-amazon.com
tjj.active-microsoft.com
ms-f7-sites-prod-cdn.akamaixed.net
cdn.ofo.ac
githubassets.akamaixed.net
ms-g9-sites-prod-cdn.akamaixed.net

IPv4-Addr

Value
104.238.151.104
45.76.179.209

Url

Value
http://cdn.stream-amazon.com/update.zip.
http://111.231.100.228:8888/CDGServer3/UpgradeService2
http://103.151.28.11:8090/CDGServer3/UpgradeService2

External References

- https://otx.alienvault.com/pulse/64e6359e82c27ed835efb4b6
- https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/carderbee-software-supply-chain-certificate-abuse