Oct 15 2023

NETMANAGEIT

Intelligence Report

New APT Group Using Custom Malware to Attack Manufacturing & IT Industries

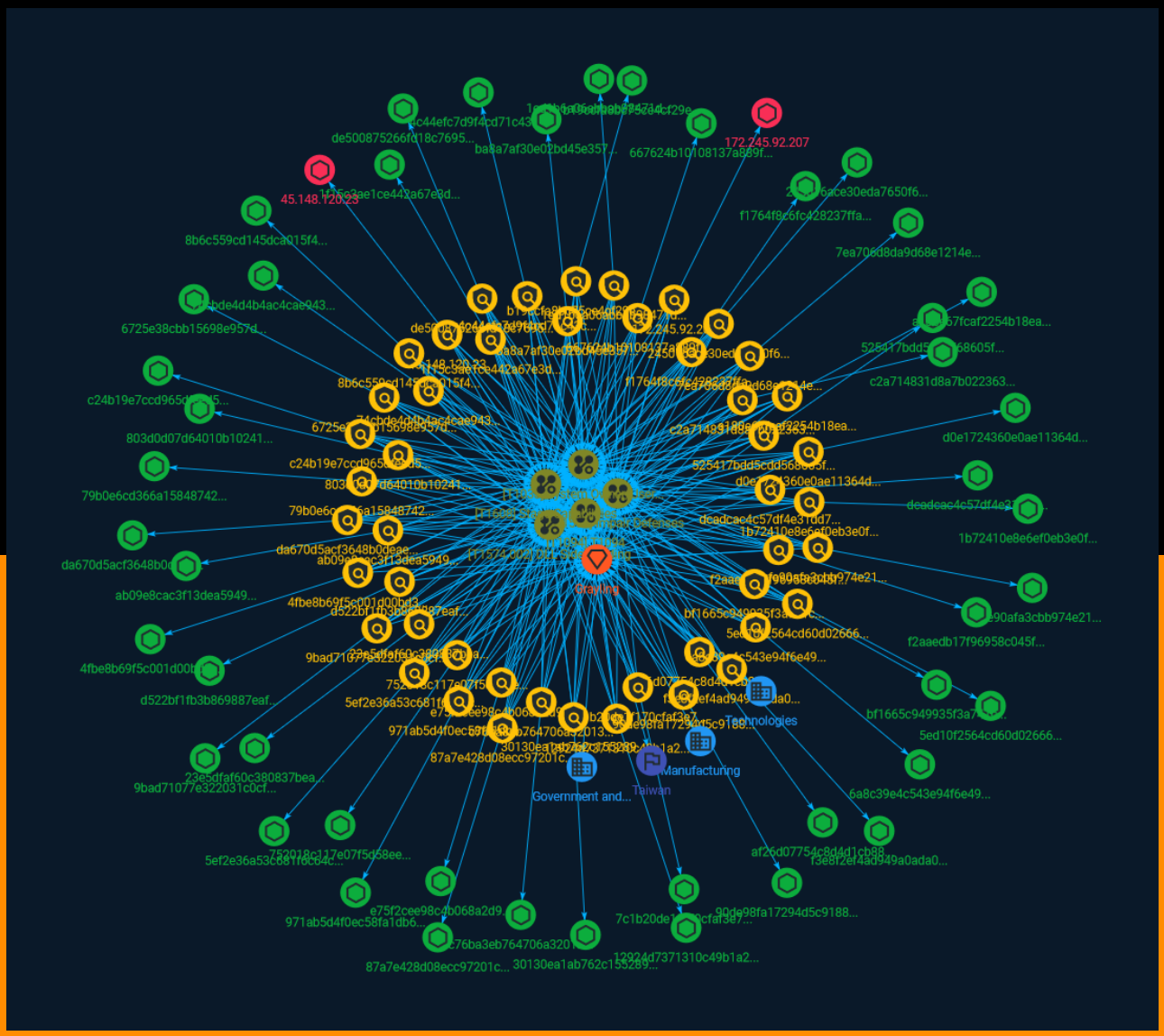

Table of contents

Overview

Entities

Observables

External References

Overview

Description

This activity involves a DLL sideloading attack through API SbieDll_Hook, loading tools such as Cobalt Strike Stager, Cobalt Strike Beacon, the Havoc framework, and NetSpy. Threat actors, in this case, encrypted the payload from imfsb.ini, then used CVE-2019-0803 to run shellcode in an effort to terminate the processes from processlist.txt, and finally sent the Mimikatz for credential dumping.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name
Impair Defenses
ID
T1562
Description
Adversaries may maliciously modify components of a victim environment in order to hinder or disable defensive mechanisms. This not only involves impairing preventative defenses, such as firewalls and anti-virus, but also detection capabilities that defenders can use to audit activity and identify malicious behavior. This may also span both native defenses as well as supplemental capabilities installed by users and administrators. Adversaries may also impair routine operations that contribute to defensive hygiene, such as blocking users from logging out of a computer or stopping it from being shut down. These restrictions can further enable malicious operations as well as the continued propagation of incidents.(Citation: Emotet shutdown) Adversaries could also target event aggregation and analysis mechanisms, or otherwise disrupt these procedures by altering other system components.
Name
DLL Side-Loading
ID
T1574.002

Description

Adversaries may execute their own malicious payloads by side-loading DLLs. Similar to [DLL Search Order Hijacking](https://attack.mitre.org/techniques/T1574/001), side-loading involves hijacking which DLL a program loads. But rather than just planting the DLL within the search order of a program then waiting for the victim application to be invoked, adversaries may directly side-load their payloads by planting then invoking a legitimate application that executes their payload(s). Side-loading takes advantage of the DLL search order used by the loader by positioning both the victim application and malicious payload(s) alongside each other. Adversaries likely use side-loading as a means of masking actions they perform under a legitimate, trusted, and potentially elevated system or software process. Benign executables used to side-load payloads may not be flagged during delivery and/or execution. Adversary payloads may also be encrypted/packed or otherwise obfuscated until loaded into the memory of the trusted process.(Citation: FireEye DLL Side-Loading)

Name

System Owner/User Discovery

ID

T1033

Description

Adversaries may attempt to identify the primary user, currently logged in user, set of users that commonly uses a system, or whether a user is actively using the system. They may do this, for example, by retrieving account usernames or by using [OS Credential Dumping](https://attack.mitre.org/techniques/T1003). The information may be collected in a number of different ways using other Discovery techniques, because user and username details are prevalent throughout a system and include running process ownership, file/directory ownership, session information, and system logs. Adversaries may use the information from [System Owner/User Discovery](https://attack.mitre.org/techniques/T1033) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Various utilities and commands may acquire this information, including `whoami`. In macOS and Linux, the currently logged in user can be identified with `w` and `who`. On macOS the `dscl . list /Users | grep -v '_'` command can also be used to enumerate user accounts. Environment variables, such as `%USERNAME%` and `$USER`, may also be used to access this information. On network

devices, [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `show users` and `show ssh` can be used to display users currently logged into the device.(Citation: show_ssh_users_cmd_cisco)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)

Name

T1094

ID

T1094

Name

Stage Capabilities

ID

T1608

Description

Adversaries may upload, install, or otherwise set up capabilities that can be used during targeting. To support their operations, an adversary may need to take capabilities they developed ([Develop Capabilities](https://attack.mitre.org/techniques/T1587)) or obtained ([Obtain Capabilities](https://attack.mitre.org/techniques/T1588)) and stage them on infrastructure under their control. These capabilities may be staged on infrastructure that was previously purchased/rented by the adversary ([Acquire Infrastructure](https://attack.mitre.org/techniques/T1583)) or was otherwise compromised by them ([Compromise Infrastructure](https://attack.mitre.org/techniques/T1584)). Capabilities may also be staged on web services, such as GitHub or Pastebin, or on Platform-as-a-Service (PaaS) offerings that enable users to easily provision applications.(Citation: Volexity Ocean Lotus November 2020)(Citation: Dragos Heroku Watering Hole)(Citation: Malwarebytes Heroku Skimmers)(Citation: Netskope GCP Redirection)(Citation: Netskope Cloud Phishing) Staging of capabilities can aid the adversary in a number of initial access and post-compromise behaviors, including (but not limited to): * Staging web resources necessary to conduct [Drive-by Compromise](https://attack.mitre.org/techniques/T1189) when a user browses to a site.(Citation: FireEye CFR Watering Hole 2012)(Citation: Gallagher 2015)(Citation: ATT

ScanBox) * Staging web resources for a link target to be used with spearphishing.(Citation: Malwarebytes Silent Librarian October 2020)(Citation: Proofpoint TA407 September 2019) * Uploading malware or tools to a location accessible to a victim network to enable [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105).(Citation: Volexity Ocean Lotus November 2020) * Installing a previously acquired SSL/TLS certificate to use to encrypt command and control traffic (ex: [Asymmetric Cryptography](https://attack.mitre.org/techniques/T1573/002) with [Web Protocols](https://attack.mitre.org/techniques/T1071/001)).(Citation: DigiCert Install SSL Cert)

Sector

Name
Manufacturing
Description
Private entities transforming and selling goods, products and equipment which are not included in other activity sectors.
Name
Government and administrations
Description
Civilian government institutions and administrations of the executive and legislative branches. The diplomatic and judicial branches are not included.
Name
Technologies
Description
Private entities related to the research, development, manufacturing and distribution of electronics, softwares, computers and products related to information technologies.

Indicator

Name
f2aaedb17f96958c045f2911655bfe46f3db21a2de9b0d396936ef6e362fea1b
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'f2aaedb17f96958c045f2911655bfe46f3db21a2de9b0d396936ef6e362fea1b']
Name
ab09e8cac3f13dea5949e7a2eaf9c9f98d3e78f3db2f140c7d85118b9bc6125f
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'ab09e8cac3f13dea5949e7a2eaf9c9f98d3e78f3db2f140c7d85118b9bc6125f']
Name

f1764f8c6fc428237ffafeb08eb0503558c68c6ccf6f2510a2ef8c574ba347e0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f1764f8c6fc428237ffafeb08eb0503558c68c6ccf6f2510a2ef8c574ba347e0']

Name

12924d7371310c49b1a215019621597926ef3c0b4649352e032a884750fab746

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '12924d7371310c49b1a215019621597926ef3c0b4649352e032a884750fab746']

Name

74cbde4d4b4ac4cae943831035bff90814fa54fd21c3a6a6ec16e7e3fb235f87

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '74cbde4d4b4ac4cae943831035bff90814fa54fd21c3a6a6ec16e7e3fb235f87']

Name

3acfe90afa3cbb974e219a5ab8a9ee8c933b397d1c1c97d6e12015726b109f1b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3acfe90afa3cbb974e219a5ab8a9ee8c933b397d1c1c97d6e12015726b109f1b']

Name

752018c117e07f5d58eed35622777e971a5f495184df1c25041ff525ca72acea

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '752018c117e07f5d58eed35622777e971a5f495184df1c25041ff525ca72acea']

Name

667624b10108137a889f0df8f408395ae332cc8d9ad550632a3501f6debc4f2c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '667624b10108137a889f0df8f408395ae332cc8d9ad550632a3501f6debc4f2c']

Name

af26d07754c8d4d1cb88195f7dc53e2e4ebee382c5b84fc54a81ba1cee4d0889

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'af26d07754c8d4d1cb88195f7dc53e2e4ebee382c5b84fc54a81ba1cee4d0889']

Name

79b0e6cd366a15848742e26c3396e0b63338ead964710b6572a8582b0530db17

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '79b0e6cd366a15848742e26c3396e0b63338ead964710b6572a8582b0530db17']

Name

525417bdd5cdd568605fdbd3dc153bcc20a4715635c02f4965a458c5d008eba9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '525417bdd5cdd568605fdbd3dc153bcc20a4715635c02f4965a458c5d008eba9']

Name

e75f2cee98c4b068a2d9e7e77599998196fd718591d3fa23b8f684133d1715c3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e75f2cee98c4b068a2d9e7e77599998196fd718591d3fa23b8f684133d1715c3']

Name

1f15c3ae1ce442a67e3d01ed291604bfc1cb196454b717e4fb5ac52daa37ecce

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1f15c3ae1ce442a67e3d01ed291604bfc1cb196454b717e4fb5ac52daa37ecce']

Name

6a8c39e4c543e94f6e4901d0facee7793f932cd2351259d8054981cf2b4da814

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6a8c39e4c543e94f6e4901d0facee7793f932cd2351259d8054981cf2b4da814']

Name

d522bf1fb3b869887eaf54f6c0e52d90514d7635b3ff8a7fd2ce9f1d06449e2c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd522bf1fb3b869887eaf54f6c0e52d90514d7635b3ff8a7fd2ce9f1d06449e2c']

Name

172.245.92.207

Description

ISP: ColoCrossing **OS:** None ---------- Hostnames: - 172-245-92-207-host.colocrossing.com ---------- Domains: - colocrossing.com ---------- Services: **22:** ``` SSH-2.0-OpenSSH_7.4 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABAQDUE1/HwpkbEJH9xLMOptweRVmrg5IDfEHTZznpjZUhmT5rb75TQ2f2PSs03UVzmEI02VcluDY3jYfIE+v2DYkMAUyQrAibGCUOXSWLil1waL0cqaurQ8YTWwS+W8UbFRdhPAxcOz5dVDmHW51W3sidZ/9rzTrbRxs8e88RusKfGeIjC0q0CSgLVo4HqDjvPBLuqugqgPdUow7/NKIA+qjxp7Q1YvyNwKh+r8CORR+NRXzOK1b9lotl5IrrqQlTdLFnL3ZQAsH3uW45RP4m+5UNf0XDe/It0O4db1IQppyunzhCJX7JPKwVl4VtmvLJoo+jqWElReqAb9YDJO6uochN Fingerprint: b4:fd:0e:48:d7:f4:a0:a7:ff:23:ab:67:94:74:6d:0f Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group-exchange-sha1 diffie-hellman-group14-sha256 diffie-hellman-group14-sha1 diffie-hellman-group1-sha1 Server Host Key Algorithms: ssh-rsa rsa-sha2-512 rsa-sha2-256 ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com aes128-cbc aes192-cbc aes256-cbc blowfish-cbc cast128-cbc 3des-cbc MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ---------- **25:** ``` 220 gewoplan.com ESMTP Postfix 250-gewoplan.com 250-PIPELINING 250-SIZE 250-VRFY 250-ETRN 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN ``` ---------- **53:** ``` get lost Resolver name: gewoplan.com ``` ---------- **80:** ``` HTTP/1.1 200 OK Date: Sat, 23 Sep 2023 12:48:27 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.2.34 Last-Modified: Mon, 04 Sep 2023 09:10:52 GMT ETag: "27b-60484e31443cd" Accept-Ranges: bytes Content-Length: 635 Content-Type: text/html; charset=UTF-8 ``` ---------- **143:** ``` * OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE STARTTLS LOGINDISABLED] Dovecot ready. * CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE STARTTLS LOGINDISABLED A001 OK Pre-login capabilities listed, post-login capabilities have more. * ID ("name" "Dovecot") A002 OK ID completed. A003 BAD Error in IMAP command received by server. * BYE Logging out A004 OK Logout completed. ``` ---------- **443:** ``` HTTP/1.1 200 OK Date: Wed, 20 Sep 2023 13:36:56 GMT Server: Apache/2.4.6 (CentOS) OpenSSL/1.0.2k-fips PHP/7.2.34 Last-Modified: Mon, 04 Sep 2023 09:10:52 GMT ETag: "27b-60484e31443cd" Accept-Ranges: bytes Content-Length: 635 Content-Type: text/html; charset=UTF-8 ``` HEARTBLEED: 2023/09/20 13:37:00 172.245.92.207:443 - SAFE ---------- **993:** ``` * OK [CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN AUTH=LOGIN] Dovecot ready. * CAPABILITY IMAP4rev1 LITERAL+ SASL-IR LOGIN-REFERRALS ID ENABLE IDLE AUTH=PLAIN AUTH=LOGIN A001 OK Pre-login capabilities listed, post-login capabilities have more. * ID ("name" "Dovecot") A002 OK ID completed. A003 BAD Error in IMAP command received by server. * BYE Logging out A004 OK Logout completed. ``` HEARTBLEED: 2023/09/13 03:27:01 172.245.92.207:993 - SAFE

---------- **995:** ``` +OK Dovecot ready. +OK CAPA TOP UIDL RESP-CODES PIPELINING AUTH-RESP-CODE USER SASL PLAIN LOGIN . ``` HEARTBLEED: 2023/09/26 15:32:25 172.245.92.207:995 - SAFE ---------- **2525:** ``` 220 gewoplan.com ESMTP service ready\r\n ``` ---------- **3306:** ``` MySQL: Error Message: Host '224.177.171.88' is not allowed to connect to this MySQL server Error Code: 1130 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '172.245.92.207']

Name

90de98fa17294d5c918865dfb1a799be80c8771df1dc0ec2be9d1c1b772d9cf0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '90de98fa17294d5c918865dfb1a799be80c8771df1dc0ec2be9d1c1b772d9cf0']

Name

803d0d07d64010b102413da61bbf7b4d378891e2a46848b88ef69ca9357e3721

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '803d0d07d64010b102413da61bbf7b4d378891e2a46848b88ef69ca9357e3721']

Name

dcadcac4c57df4e31dd7094ae96657f54b22c87233e8277a2c40ba56eafcf548

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'dcadcac4c57df4e31dd7094ae96657f54b22c87233e8277a2c40ba56eafcf548']

Name

5ef2e36a53c681f6c64cfea16c2ca156cf468579cc96f6c527eca8024bfdc581

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5ef2e36a53c681f6c64cfea16c2ca156cf468579cc96f6c527eca8024bfdc581']

Name

ba8a7af30e02bd45e3570de20777ab7c1eec4797919bfcd39dde681eb69b9faf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ba8a7af30e02bd45e3570de20777ab7c1eec4797919bfcd39dde681eb69b9faf']

Name

bf1665c949935f3a741cfe44ab2509ec3751b9384b9eda7fb31c12bfbb2a12ec

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bf1665c949935f3a741cfe44ab2509ec3751b9384b9eda7fb31c12bfbb2a12ec']

Name

da670d5acf3648b0deaecb64710ae2b7fc41fc6ae8ab8343a1415144490a9ae9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'da670d5acf3648b0deaecb64710ae2b7fc41fc6ae8ab8343a1415144490a9ae9']

Name

245016ace30eda7650f6bb3b2405761a6a5ff1f44b94159792a6eb64ced023aa

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '245016ace30eda7650f6bb3b2405761a6a5ff1f44b94159792a6eb64ced023aa']

Name

87a7e428d08ecc97201cc8f229877a6202545e562de231a7b4cab4d9b6bbc0f8

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '87a7e428d08ecc97201cc8f229877a6202545e562de231a7b4cab4d9b6bbc0f8']

Name

45.148.120.23

Description

ISP: Phanes Networks B.V. **OS:** None ---------- Hostnames: - prime-proxy.ezoservers.com ---------- Domains: - ezoservers.com ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.2p1 Ubuntu-4ubuntu0.9 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQCu/5qxJUfM766goJ3bZANgSUSQ0AwvSuJeKz5MIesyXAsMLFbkuQLAMmIS8NU0It8aprjMyhy+6FbA8rfsuWYFlxLthf9ZOk39o1xyO2Jno/6KaDnD7M6o/dCJPzNqawg6f+QAaz/WddqeG6GwfkbNAK+oVKqjXuqj/HUJBP/FArvG5DVIAFQj8cfka065D5IiMAdH

9N5y3n3XjPu5MzAK5PVQ2fjsZS/A2dlX3W4WeDTzexSGHw8yX8W+il7lYoEXlcXl9DcXOAiZX0V3 HhjHllkvnlJ7ux5ubpl/zNhwc4N3gaM/p3NZYTCzWP7IfJbWs+uW+p6JJLvfdBlfeF0lKUyGKsXo dD3B5ASxJllJSh4JzcAp4etX5+zvSYHwZgJaRvS3yic/pHovnCWXbtvxmZtB7oPKVpSIYbfmovN+ N8w4bHNT+37RaL6TrseulEvCH4FLS/z8gPJrF0pN6Onn3EiFas/QF57P9pdVm6UWxqeiJINqLvnU cu7wumG8dbE= Fingerprint: 49:53:a2:36:1f:0d:7b:87:b3:4a:e3:8c:9e:b6:92:61 Kex Algorithms: curve25519-sha256 curve25519-sha256@libssh.org ecdh-sha2-nistp256 ecdh-sha2-nistp384 ecdh-sha2-nistp521 diffie-hellman-group-exchange-sha256 diffie-hellman-group16-sha512 diffie-hellman-group18-sha512 diffie-hellman-group14-sha256 Server Host Key Algorithms: rsa-sha2-512 rsa-sha2-256 ssh-rsa ecdsa-sha2-nistp256 ssh-ed25519 Encryption Algorithms: chacha20-poly1305@openssh.com aes128-ctr aes192-ctr aes256-ctr aes128-gcm@openssh.com aes256-gcm@openssh.com MAC Algorithms: umac-64-etm@openssh.com umac-128-etm@openssh.com hmac-sha2-256-etm@openssh.com hmac-sha2-512-etm@openssh.com hmac-sha1-etm@openssh.com umac-64@openssh.com umac-128@openssh.com hmac-sha2-256 hmac-sha2-512 hmac-sha1 Compression Algorithms: none zlib@openssh.com ``` ---------- **80:** ``` HTTP/1.1 200 OK Server: nginx Date: Wed, 04 Oct 2023 10:44:23 GMT Content-Type: text/html Content-Length: 615 Last-Modified: Fri, 14 Jan 2022 07:23:06 GMT Connection: keep-alive ETag: "61e124da-267" Accept-Ranges: bytes ``` ---------- **443:** ``` HTTP/1.1 200 OK Server: nginx Date: Sat, 30 Sep 2023 05:05:37 GMT Content-Type: text/html Content-Length: 903 Last-Modified: Sat, 09 Sep 2023 07:27:15 GMT Connection: keep-alive ETag: "64fc1e53-387" Strict-Transport-Security: max-age=31536000 Accept-Ranges: bytes ``` HEARTBLEED: 2023/09/30 05:05:46 45.148.120.23:443 - SAFE ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '45.148.120.23']

Name

1b72410e8e6ef0eb3e0f950ec4ced1be0ee6ac0a9349c8280cd8d12cc00850f9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1b72410e8e6ef0eb3e0f950ec4ced1be0ee6ac0a9349c8280cd8d12cc00850f9']

Name

9bad71077e322031c0cf7f541d64c3fed6b1dc7c261b0b994b63e56bc3215739

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '9bad71077e322031c0cf7f541d64c3fed6b1dc7c261b0b994b63e56bc3215739']

Name

1ed1b6a06abbab98471d5af33e242acc76d17b41c6e96cce0938a05703b58b91

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1ed1b6a06abbab98471d5af33e242acc76d17b41c6e96cce0938a05703b58b91']

Name

7c1b20de1f170cfaf3e75ebc7e81860378e353c84469795a162cd3cfd7263ba2

Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '7c1b20de1f170cfaf3e75ebc7e81860378e353c84469795a162cd3cfd7263ba2']
Name
6725e38cbb15698e957d50b8bc67bd66ece554bbf6bcb90e72eaf32b1d969e50
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '6725e38cbb15698e957d50b8bc67bd66ece554bbf6bcb90e72eaf32b1d969e50']
Name
a180e67fcaf2254b18eafdc95b83038e9a4385b1a5c2651651d9d288fa0500fe
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'a180e67fcaf2254b18eafdc95b83038e9a4385b1a5c2651651d9d288fa0500fe']

Name

971ab5d4f0ec58fa1db61622a735a51e14e70ee5d99ab3cd554e0070b248eb1f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '971ab5d4f0ec58fa1db61622a735a51e14e70ee5d99ab3cd554e0070b248eb1f']

Name

4c44efc7d9f4cd71c43c6596c62b91740eb84b7eb9b8cf22c7034b75b5f432d9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4c44efc7d9f4cd71c43c6596c62b91740eb84b7eb9b8cf22c7034b75b5f432d9']

Name

5ed10f2564cd60d02666637e9eac36db36f3a13906b851ec1207c7df620d8970

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5ed10f2564cd60d02666637e9eac36db36f3a13906b851ec1207c7df620d8970']

Name

4fbe8b69f5c001d00bd39e4fdb3058c96ed796326d6e5e582610d67252d11aba

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4fbe8b69f5c001d00bd39e4fdb3058c96ed796326d6e5e582610d67252d11aba']

Name

7ea706d8da9d68e1214e30c6373713da3585df8a337bc64fcc154fc5363f5f1f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7ea706d8da9d68e1214e30c6373713da3585df8a337bc64fcc154fc5363f5f1f']

Name

c76ba3eb764706a32013007c147309f0be19efff3e6a172393d72d46631f712e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c76ba3eb764706a32013007c147309f0be19efff3e6a172393d72d46631f712e']

Name

8b6c559cd145dca015f4fa06ef1c9cd2446662a1e62eb51ba2c86f4183231ed2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '8b6c559cd145dca015f4fa06ef1c9cd2446662a1e62eb51ba2c86f4183231ed2']

Name

d0e1724360e0ae11364d3ac0eb8518ecf5d859128d094e9241d8e6feb43a9f29

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd0e1724360e0ae11364d3ac0eb8518ecf5d859128d094e9241d8e6feb43a9f29']

Name

23e5dfaf60c380837beaddaaa9eb550809cd995f2cda99e3fe4ca8b281d770ae

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '23e5dfaf60c380837beaddaaa9eb550809cd995f2cda99e3fe4ca8b281d770ae']

Name

b19ccfa8bc75ce4cf29eb52d4afe79fe7c3819ac08b68bd87b35225a762112ba

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b19ccfa8bc75ce4cf29eb52d4afe79fe7c3819ac08b68bd87b35225a762112ba']

Name

f3e8f2ef4ad949a0ada037f52f4c0e6000d111a4ac813e64138f0ded865e6e31

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f3e8f2ef4ad949a0ada037f52f4c0e6000d111a4ac813e64138f0ded865e6e31']

Name

c24b19e7ccd965dfeed553c94b093533e527c55d5adbc9f0e87815d477924be5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c24b19e7ccd965dfeed553c94b093533e527c55d5adbc9f0e87815d477924be5']

Name

c2a714831d8a7b0223631eda655ce62ff3c262d910c0a2ed67c5ca92ef4447e3

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c2a714831d8a7b0223631eda655ce62ff3c262d910c0a2ed67c5ca92ef4447e3']

Name

30130ea1ab762c155289a32db810168f59c3d37b69bcbedfd284c4a861d749d6

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '30130ea1ab762c155289a32db810168f59c3d37b69bcbedfd284c4a861d749d6']

Name

de500875266fd18c76959839e8c6b075e4408dcbc0b620f7544f28978b852c1c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'de500875266fd18c76959839e8c6b075e4408dcbc0b620f7544f28978b852c1c']

Intrusion-Set

Name
Grayling

Country

Name
Taiwan

StixFile

Value
e75f2cee98c4b068a2d9e7e77599998196fd718591d3fa23b8f684133d1715c3
c76ba3eb764706a32013007c147309f0be19efff3e6a172393d72d46631f712e
4c44efc7d9f4cd71c43c6596c62b91740eb84b7eb9b8cf22c7034b75b5f432d9
5ed10f2564cd60d02666637e9eac36db36f3a13906b851ec1207c7df620d8970
f1764f8c6fc428237ffafeb08eb0503558c68c6ccf6f2510a2ef8c574ba347e0
525417bdd5cdd568605fdbd3dc153bcc20a4715635c02f4965a458c5d008eba9
9bad71077e322031c0cf7f541d64c3fed6b1dc7c261b0b994b63e56bc3215739
8b6c559cd145dca015f4fa06ef1c9cd2446662a1e62eb51ba2c86f4183231ed2
971ab5d4f0ec58fa1db61622a735a51e14e70ee5d99ab3cd554e0070b248eb1f
c2a714831d8a7b0223631eda655ce62ff3c262d910c0a2ed67c5ca92ef4447e3
245016ace30eda7650f6bb3b2405761a6a5ff1f44b94159792a6eb64ced023aa
90de98fa17294d5c918865dfb1a799be80c8771df1dc0ec2be9d1c1b772d9cf0
5ef2e36a53c681f6c64cfea16c2ca156cf468579cc96f6c527eca8024bfdc581

b19ccfa8bc75ce4cf29eb52d4afe79fe7c3819ac08b68bd87b35225a762112ba

3acfe90afa3cbb974e219a5ab8a9ee8c933b397d1c1c97d6e12015726b109f1b

1f15c3ae1ce442a67e3d01ed291604bfc1cb196454b717e4fb5ac52daa37ecce

7ea706d8da9d68e1214e30c6373713da3585df8a337bc64fcc154fc5363f5f1f

da670d5acf3648b0deaecb64710ae2b7fc41fc6ae8ab8343a1415144490a9ae9

ba8a7af30e02bd45e3570de20777ab7c1eec4797919bfcd39dde681eb69b9faf

d522bf1fb3b869887eaf54f6c0e52d90514d7635b3ff8a7fd2ce9f1d06449e2c

803d0d07d64010b102413da61bbf7b4d378891e2a46848b88ef69ca9357e3721

de500875266fd18c76959839e8c6b075e4408dcbc0b620f7544f28978b852c1c

79b0e6cd366a15848742e26c3396e0b63338ead964710b6572a8582b0530db17

4fbe8b69f5c001d00bd39e4fdb3058c96ed796326d6e5e582610d67252d11aba

f3e8f2ef4ad949a0ada037f52f4c0e6000d111a4ac813e64138f0ded865e6e31

6725e38cbb15698e957d50b8bc67bd66ece554bbf6bcb90e72eaf32b1d969e50

23e5dfaf60c380837beaddaaa9eb550809cd995f2cda99e3fe4ca8b281d770ae

dcadcac4c57df4e31dd7094ae96657f54b22c87233e8277a2c40ba56eafcf548

bf1665c949935f3a741cfe44ab2509ec3751b9384b9eda7fb31c12bfbb2a12ec

1b72410e8e6ef0eb3e0f950ec4ced1be0ee6ac0a9349c8280cd8d12cc00850f9

752018c117e07f5d58eed35622777e971a5f495184df1c25041ff525ca72acea

c24b19e7ccd965dfeed553c94b093533e527c55d5adbc9f0e87815d477924be5

30130ea1ab762c155289a32db810168f59c3d37b69bcbedfd284c4a861d749d6

7c1b20de1f170cfaf3e75ebc7e81860378e353c84469795a162cd3cfd7263ba2

12924d7371310c49b1a215019621597926ef3c0b4649352e032a884750fab746

74cbde4d4b4ac4cae943831035bff90814fa54fd21c3a6a6ec16e7e3fb235f87

f2aaedb17f96958c045f2911655bfe46f3db21a2de9b0d396936ef6e362fea1b

af26d07754c8d4d1cb88195f7dc53e2e4ebee382c5b84fc54a81ba1cee4d0889

ab09e8cac3f13dea5949e7a2eaf9c9f98d3e78f3db2f140c7d85118b9bc6125f

d0e1724360e0ae11364d3ac0eb8518ecf5d859128d094e9241d8e6feb43a9f29

6a8c39e4c543e94f6e4901d0facee7793f932cd2351259d8054981cf2b4da814

87a7e428d08ecc97201cc8f229877a6202545e562de231a7b4cab4d9b6bbc0f8

667624b10108137a889f0df8f408395ae332cc8d9ad550632a3501f6debc4f2c

1ed1b6a06abbab98471d5af33e242acc76d17b41c6e96cce0938a05703b58b91

a180e67fcaf2254b18eafdc95b83038e9a4385b1a5c2651651d9d288fa0500fe

IPv4-Addr

Value
172.245.92.207
45.148.120.23

External References

- https://otx.alienvault.com/pulse/65281d5afbb224d10c5f287e
- https://cybersecuritynews.com/apt-group-custom-malware/