Nov 30 2023

NETMANAGEIT

Intelligence Report

GoTitan Botnet - Ongoing Exploitation on Apache ActiveMQ

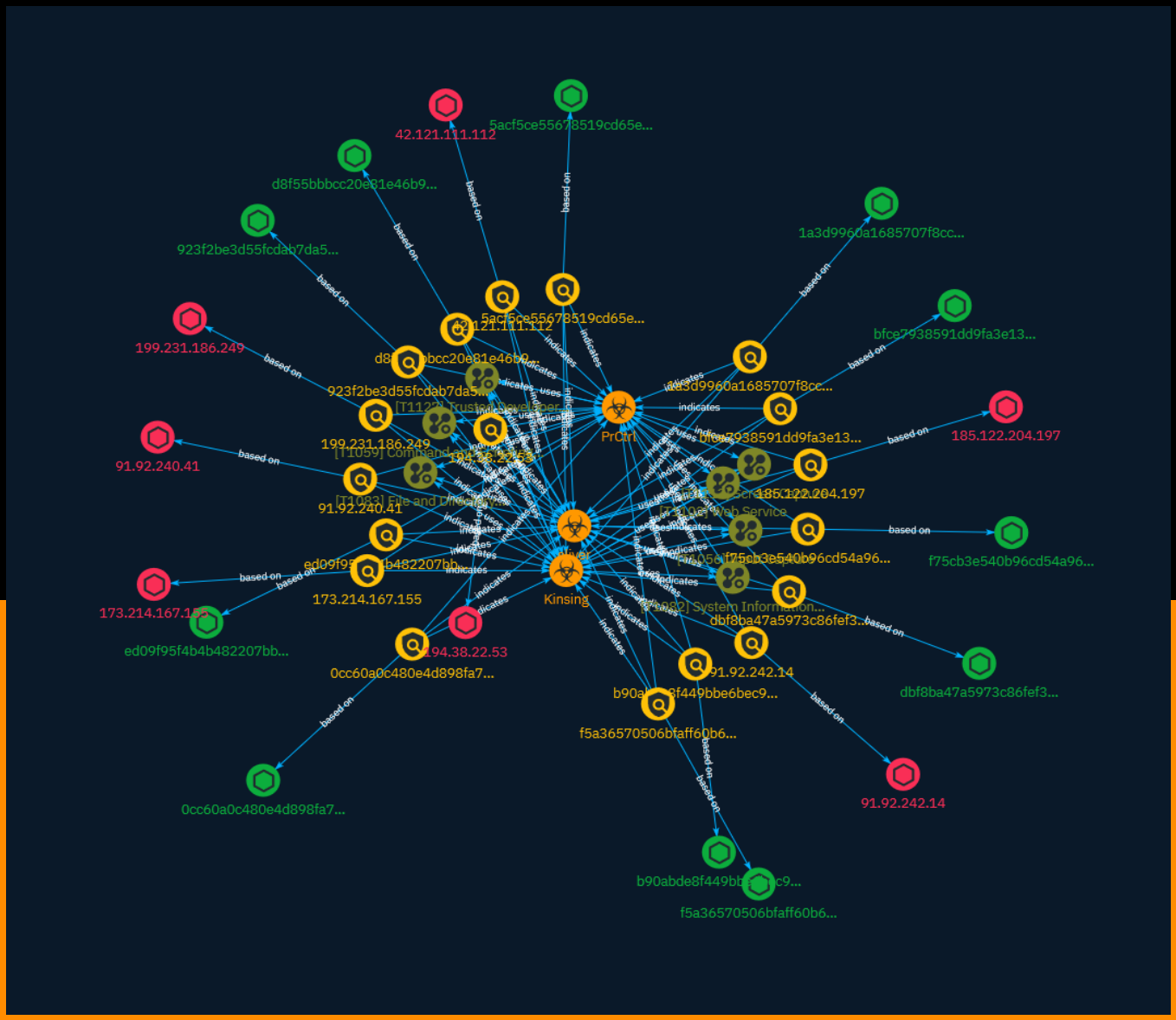

Table of contents

Overview

Entities

Observables

External References

Overview

Description

An ongoing exploitation of a critical Apache ActiveMQ vulnerability has led to the emergence of two new strains of malware, including GoTitan and Ddostf, according to Fortiguard Labs.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

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
Command and Scripting Interpreter
ID
T1059
Description

Adversaries may abuse command and script interpreters to execute commands, scripts, or binaries. These interfaces and languages provide ways of interacting with computer systems and are a common feature across many different platforms. Most systems come with some built-in command-line interface and scripting capabilities, for example, macOS and Linux distributions include some flavor of [Unix Shell](https://attack.mitre.org/techniques/T1059/004) while Windows installations include the [Windows Command Shell](https://attack.mitre.org/techniques/T1059/003) and [PowerShell](https://attack.mitre.org/techniques/T1059/001). There are also cross-platform interpreters such as [Python](https://attack.mitre.org/techniques/T1059/006), as well as those commonly associated with client applications such as [JavaScript](https://attack.mitre.org/techniques/T1059/007) and [Visual Basic](https://attack.mitre.org/techniques/T1059/005). Adversaries may abuse these technologies in various ways as a means of executing arbitrary commands. Commands and scripts can be embedded in [Initial Access](https://attack.mitre.org/tactics/TA0001) payloads delivered to victims as lure documents or as secondary payloads downloaded from an existing C2. Adversaries may also execute commands through interactive terminals/shells, as well as utilize various [Remote Services](https://attack.mitre.org/techniques/T1021) in order to achieve remote Execution. (Citation: Powershell Remote Commands)(Citation: Cisco IOS Software Integrity Assurance - Command History)(Citation: Remote Shell Execution in Python)

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).

Name

Trusted Developer Utilities Proxy Execution

ID

T1127

Description

Adversaries may take advantage of trusted developer utilities to proxy execution of malicious payloads. There are many utilities used for software development related tasks that can be used to execute code in various forms to assist in development, debugging, and reverse engineering.(Citation: engima0x3 DNX Bypass)(Citation: engima0x3 RCSI Bypass)(Citation: Exploit Monday WinDbg)(Citation: LOLBAS Tracker) These utilities may often be signed with legitimate certificates that allow them to execute on a system and proxy execution of malicious code through a trusted process that effectively bypasses application control solutions.

Name

File and Directory Discovery

ID

T1083

Description

Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. Adversaries may use the information from [File and Directory Discovery](https://attack.mitre.org/techniques/T1083) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Many command shell utilities can be used to obtain this information. Examples include `dir`, `tree`, `ls`, `find`, and `locate`.(Citation: Windows Commands JPCERT) Custom tools may also be used to gather file and directory information and interact with the [Native API](https://attack.mitre.org/techniques/T1106). Adversaries may also leverage a [Network Device CLI]

(https://attack.mitre.org/techniques/T1059/008) on network devices to gather file and directory information (e.g. `dir`, `show flash`, and/or `nvram`).(Citation: US-CERT-TA18-106A)

Name

Screen Capture

ID

T1113

Description

Adversaries may attempt to take screen captures of the desktop to gather information over the course of an operation. Screen capturing functionality may be included as a feature of a remote access tool used in post-compromise operations. Taking a screenshot is also typically possible through native utilities or API calls, such as `CopyFromScreen`, `xwd`, or `screencapture`.(Citation: CopyFromScreen .NET)(Citation: Antiquated Mac Malware)

Name

System Information Discovery

ID

T1082

Description

An adversary may attempt to get detailed information about the operating system and hardware, including version, patches, hotfixes, service packs, and architecture. Adversaries may use the information from [System Information Discovery](https://attack.mitre.org/techniques/T1082) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Tools such as [Systeminfo](https://attack.mitre.org/software/S0096) can be used to gather detailed system information. If running with privileged access, a breakdown of system data can be gathered through the `systemsetup` configuration tool on macOS. As an example,

adversaries with user-level access can execute the `df -aH` command to obtain currently mounted disks and associated freely available space. Adversaries may also leverage a [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) on network devices to gather detailed system information (e.g. `show version`).(Citation: US-CERT-TA18-106A) [System Information Discovery](https://attack.mitre.org/techniques/T1082) combined with information gathered from other forms of discovery and reconnaissance can drive payload development and concealment.(Citation: OSX.FairyTale)(Citation: 20 macOS Common Tools and Techniques) Infrastructure as a Service (IaaS) cloud providers such as AWS, GCP, and Azure allow access to instance and virtual machine information via APIs. Successful authenticated API calls can return data such as the operating system platform and status of a particular instance or the model view of a virtual machine.(Citation: Amazon Describe Instance)(Citation: Google Instances Resource)(Citation: Microsoft Virutal Machine API)

Indicator

Name

185.122.204.197

Description

ISP: Chang Way Technologies Co. Limited **OS:** Debian ---------- Hostnames: ---------- Domains: ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.4p1 Debian-5+deb11u1 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQDhNGSHCy6+ +4UcvRFSE84k0+8wWlezl7sU9SDB2qLBsj6l T54X1sUb2crp54TLFQ6ak8gJ/ ZPoaUNLd6amBdq47VZG86PUnaTCvpd655KPQq4w3VFmzydze5Pi Mb/ DgpkDgkUMPP4Di3Q5uDtumWeGIFbWevpmdE1SH8NHcuHNnylZRMk7X9cgz+DxyxZy7WKRFjV1 pW7wZgB9s4xTlyony3GWiXfqBvZivUwyc6WFy/LCenx839YprtEAOTM7vHRn5cM+lqPOWPc+jEYD Llq6jp+2oia16Y7ww2NtrGhFTNcSPAtRGo0Eto570VOw6Wj34Sbe5aP1ZE1y5dFZyLk4NEdJ4+uh Ic0fGJNcNq0vaDrAJIg7ye4yCVcP6pT8nXURGGip1mUW51kbskvZLsU4OXR2DJfTrd2UaEgSJxzG 6eg6OtAA00hQxEgkDu/svKrHm3rLlISMkP7oaZglYgFE/pycdgeDJRPPUbmN6F4R4Kmc1xsuOJxz 7aZCFkrvP9E= Fingerprint: 01:05:9c:fc:df:58:c9:12:f1:8d:78:95:b2:d8:f0:43 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 ``` ---------- **123:** ``` NTP protocolversion: 3 stratum: 2 leap: 0 precision: -24 rootdelay: 0.00131225585938 rootdisp: 0.0495758056641 refid: 3267274753 reftime: 3909323581.97 poll: 3 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.122.204.197']

Name

ed09f95f4b4b482207bb300ff6ec15ed8ca5fdde97af02fa9fbe01adaaf7673b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ed09f95f4b4b482207bb300ff6ec15ed8ca5fdde97af02fa9fbe01adaaf7673b']

Name

5acf5ce55678519cd65e001d3f600fa1de288f1cd3e203b4c9439979f4b67175

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5acf5ce55678519cd65e001d3f600fa1de288f1cd3e203b4c9439979f4b67175']

Name

b90abde8f449bbe6bec9495386fab1833c0654f83c7b2f5ebcf5b14743c30600

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b90abde8f449bbe6bec9495386fab1833c0654f83c7b2f5ebcf5b14743c30600']

Name

194.38.22.53

Description

ISP: Rices Privately owned enterprise **OS:** None ------------------------- Hostnames: - mohavijj1.ntup.network ------------------------- Domains: - ntup.network ------------------------- Services: **22:** ``` SSH-2.0-OpenSSH_8.4p1 Debian-5+deb11u1 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQDO+IZJ/+Nd5h8RwASJ9U8/yoZLMg5kSbFnU+CEWpuDn3Mk jRgTXYzz0vHUSnm2mZ5IRKh0c75D1W7YmMKKsx1Ai7Q9Zy/zTbF6vZDNrIf5YSJJ4M8Kpc2v8Wr8 jsQkBJXLkvT4VIhwL9GtA+ITN2PGxmbjbzMSn7Rk+disfniQnqWlTvUZYQ9lup5q2cYEcyWLwdmR ePf3pA3HLOqrgnANsIbeTpdmdlcvzHx4BDU18f5qk46+kbMWdp0pV6uY1o+QalRNg+DbY8Qt0m eE HvFhMiaGYVfoXs1vH/NMJVc4nf/8s/ EEwmkvbqfXT+3FJwQNpuPr55HEWKaf7vHA5XDaNhEawJyN fwaDnlNFuPeQaYosfCr93L0WNHyXEmXHhdtPF1KykDrxyIx/hLs9uL21SF+GutaRUFacczLf9pgY / HYOLYzFUXE95pVkljZHLMxarIeHDMY4b6Y81Cs/selcOR4QI0kmhEzMQyHe2VgMDCXL4FNvH0OE l7+AqqXcIt0= Fingerprint: de:aa:dc:2e:10:d9:16:e4:d7:1e:c8:c5:81:27:18:1f 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/1.18.0 Date: Tue, 21 Nov 2023 15:34:29 GMT Content-Type: text/html Content-Length: 10701 Last-Modified: Thu, 28 Sep 2023 15:58:05 GMT Connection: keep-alive ETag: "6515a28d-29cd" Accept-Ranges: bytes ``` ---------- **123:** ``` NTP protocolversion: 3 stratum: 0 leap: 3 precision: 0 rootdelay: 0.0 rootdisp: 0.0 refid: 1380013125 reftime: 0.0 poll: 3 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '194.38.22.53']

Name

d8f55bbbcc20e81e46b9bf78f93b73f002c76a8fcdb4dc2ae21b8609445c14f9

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'd8f55bbbcc20e81e46b9bf78f93b73f002c76a8fcdb4dc2ae21b8609445c14f9']

Name

f5a36570506bfaff60b684cd26dde3a64a3db4eaa9da78a1434cfd4b390ef3d5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f5a36570506bfaff60b684cd26dde3a64a3db4eaa9da78a1434cfd4b390ef3d5']

Name

91.92.240.41

Description

CC=BG ASN=AS394711 LIMENET

Pattern Type

stix

Pattern

[ipv4-addr:value = '91.92.240.41']

Name

f75cb3e540b96cd54a966c512c854c832807e354772ae1a326b758394b01b607

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f75cb3e540b96cd54a966c512c854c832807e354772ae1a326b758394b01b607']

Name

0cc60a0c480e4d898fa77ab501bbd2afaf3f5fb89a2917a31e7f5fdaa6c3879c

Description

Trojan:Linux/CoinMiner.AF!MTB

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '0cc60a0c480e4d898fa77ab501bbd2afaf3f5fb89a2917a31e7f5fdaa6c3879c']

Name

42.121.111.112

Description

CC=CN ASN=AS37963 Hangzhou Alibaba Advertising Co.,Ltd.

Pattern Type

stix

Pattern

[ipv4-addr:value = '42.121.111.112']

Name

91.92.242.14

Description

CC=BG ASN=AS394711 LIMENET

Pattern Type

stix

Pattern

[ipv4-addr:value = '91.92.242.14']

Name

199.231.186.249

Description

CC=US ASN=AS19318 IS-AS-1

Pattern Type

stix

Pattern

[ipv4-addr:value = '199.231.186.249']

Name

1a3d9960a1685707f8cc2bc447c88f5c3278454fbf0a35a7959717ad835348cd

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '1a3d9960a1685707f8cc2bc447c88f5c3278454fbf0a35a7959717ad835348cd']

Name

bfce7938591dd9fa3e1368d7eb86fc7f11e935349437fc11de4f124bbbc16dee

Description

Unix.Malware.Sliver-9994108-0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'bfce7938591dd9fa3e1368d7eb86fc7f11e935349437fc11de4f124bbbc16dee']

Name

923f2be3d55fcdab7da5cb2be3c16dfcc1582b83d1e4a831236445a52ca81878

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '923f2be3d55fcdab7da5cb2be3c16dfcc1582b83d1e4a831236445a52ca81878']

Name
dbf8ba47a5973c86fef32c2d696b09e1930a8384087c62ace1aa5c4084ee1a3f
Description
Trojan:Win32/Bicone
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'dbf8ba47a5973c86fef32c2d696b09e1930a8384087c62ace1aa5c4084ee1a3f']
Name
173.214.167.155
Description
CC=US ASN=AS19318 IS-AS-1
Pattern Type
stix
Pattern
[ipv4-addr:value = '173.214.167.155']

Malware

Name
sliver
Name
PrCtrl
Name
Kinsing
Description
[Kinsing](https://attack.mitre.org/software/S0599) is Golang-based malware that runs a cryptocurrency miner and attempts to spread itself to other hosts in the victim environment. (Citation: Aqua Kinsing April 2020)(Citation: Sysdig Kinsing November 2020) (Citation: Aqua Security Cloud Native Threat Report June 2021)

StixFile

Value
0cc60a0c480e4d898fa77ab501bbd2afaf3f5fb89a2917a31e7f5fdaa6c3879c
dbf8ba47a5973c86fef32c2d696b09e1930a8384087c62ace1aa5c4084ee1a3f
ed09f95f4b4b482207bb300ff6ec15ed8ca5fdde97af02fa9fbe01adaaf7673b
bfce7938591dd9fa3e1368d7eb86fc7f11e935349437fc11de4f124bbbc16dee
f75cb3e540b96cd54a966c512c854c832807e354772ae1a326b758394b01b607
d8f55bbbcc20e81e46b9bf78f93b73f002c76a8fcdb4dc2ae21b8609445c14f9
5acf5ce55678519cd65e001d3f600fa1de288f1cd3e203b4c9439979f4b67175
f5a36570506bfaff60b684cd26dde3a64a3db4eaa9da78a1434cfd4b390ef3d5
1a3d9960a1685707f8cc2bc447c88f5c3278454fbf0a35a7959717ad835348cd
923f2be3d55fcdab7da5cb2be3c16dfcc1582b83d1e4a831236445a52ca81878
b90abde8f449bbe6bec9495386fab1833c0654f83c7b2f5ebcf5b14743c30600

IPv4-Addr

Value
199.231.186.249
194.38.22.53
91.92.240.41
42.121.111.112
91.92.242.14
173.214.167.155
185.122.204.197

External References

- https://otx.alienvault.com/pulse/6567c0e6d66026b734340b59
- https://www.fortinet.com/blog/threat-research/gotitan-botnet-exploitation-on-apache-activemq