Dec 06 2023

NETMANAGEIT

Intelligence Report

AsyncRAT Distributed via WSF Script

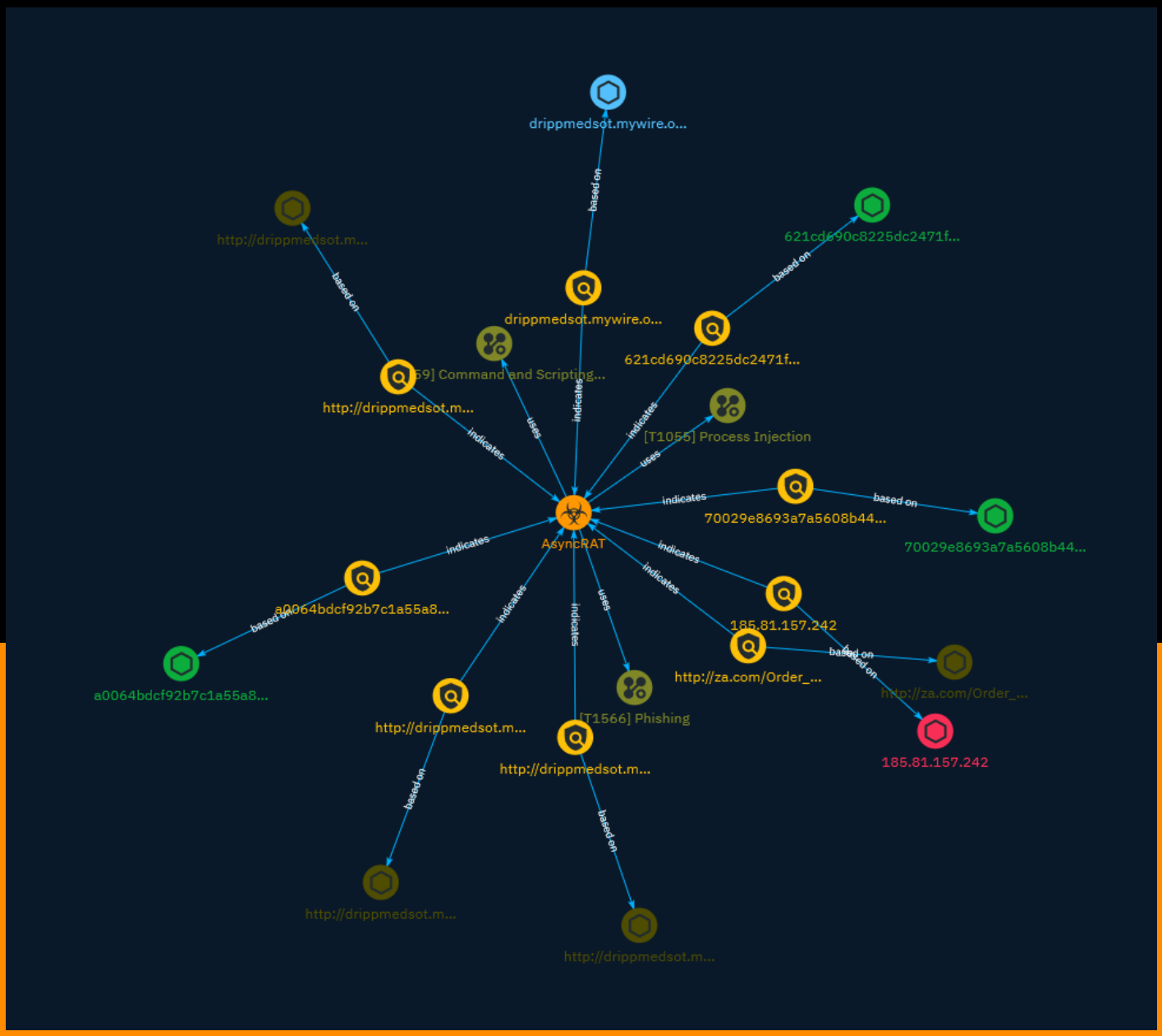

Table of contents

Overview

- Description 4
- Confidence 4
- Content 5

Entities

- Attack-Pattern 6
- Indicator 9
- Malware 13

Observables

- StixFile 14
- Hostname 15
- IPv4-Addr 16
- Url 17

External References

- External References 18

Overview

Description

AsyncRAT malware is being distributed via a file-less attack.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

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

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)

Indicator

Name
a0064bdcf92b7c1a55a8e88fd4ecb38d27c4d602f7bf5feb18c2304d775d7387
Description
SHA256 of 61b7507a6814e81cda6b57850f9f31da
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'a0064bdcf92b7c1a55a8e88fd4ecb38d27c4d602f7bf5feb18c2304d775d7387']
Name
drippmedsot.mywire.org
Pattern Type
stix
Pattern

[hostname:value = 'drippmedsot.mywire.org']

Name

185.81.157.242

Description

AsyncRAT botnet C2 server (confidence level: 100%)

Pattern Type

stix

Pattern

[ipv4-addr:value = '185.81.157.242']

Name

http://drippmedsot.mywire.org:7707

Pattern Type

stix

Pattern

[url:value = 'http://drippmedsot.mywire.org:7707']

Name

621cd690c8225dc2471fa2d94f6b568d4212baddc1a05a96a0edc9a1bbe6f29c

Description

SHA256 of 790562cefbb2c6b9d890b6d2b4adc548

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '621cd690c8225dc2471fa2d94f6b568d4212baddc1a05a96a0edc9a1bbe6f29c']

Name

http://za.com/Order_ed333c91f0fd.zip

Pattern Type

stix

Pattern

[url:value = 'http://za.com/Order_ed333c91f0fd.zip']

Name

http://drippmedsot.mywire.org:6606

Pattern Type

stix

Pattern

[url:value = 'http://drippmedsot.mywire.org:6606']

Name
70029e8693a7a5608b442b1944a3f6c11fe2ff1949f26e3f6178472b87837d75
Description
SHA256 of a31191ca8fe50b0a70eb48b82c4d6f39
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '70029e8693a7a5608b442b1944a3f6c11fe2ff1949f26e3f6178472b87837d75']
Name
http://drippmedsot.mywire.org:8808
Pattern Type
stix
Pattern
[url:value = 'http://drippmedsot.mywire.org:8808']

Malware

Name
AsyncRAT

StixFile

Value
70029e8693a7a5608b442b1944a3f6c11fe2ff1949f26e3f6178472b87837d75
a0064bdcf92b7c1a55a8e88fd4ecb38d27c4d602f7bf5feb18c2304d775d7387
621cd690c8225dc2471fa2d94f6b568d4212baddc1a05a96a0edc9a1bbe6f29c

Hostname

Value
drippmedsot.mywire.org

IPv4-Addr

Value
185.81.157.242

Url

Value
http://za.com/Order_ed333c91f0fd.zip
http://drippmedsot.mywire.org:7707
http://drippmedsot.mywire.org:6606
http://drippmedsot.mywire.org:8808

External References

- https://otx.alienvault.com/pulse/65708908da87706f34dfe252
- https://asec.ahnlab.com/en/59573/