Jun 11 2023

NETMANAGEIT

Intelligence Report

AndoryuBot's DDOS Rampage

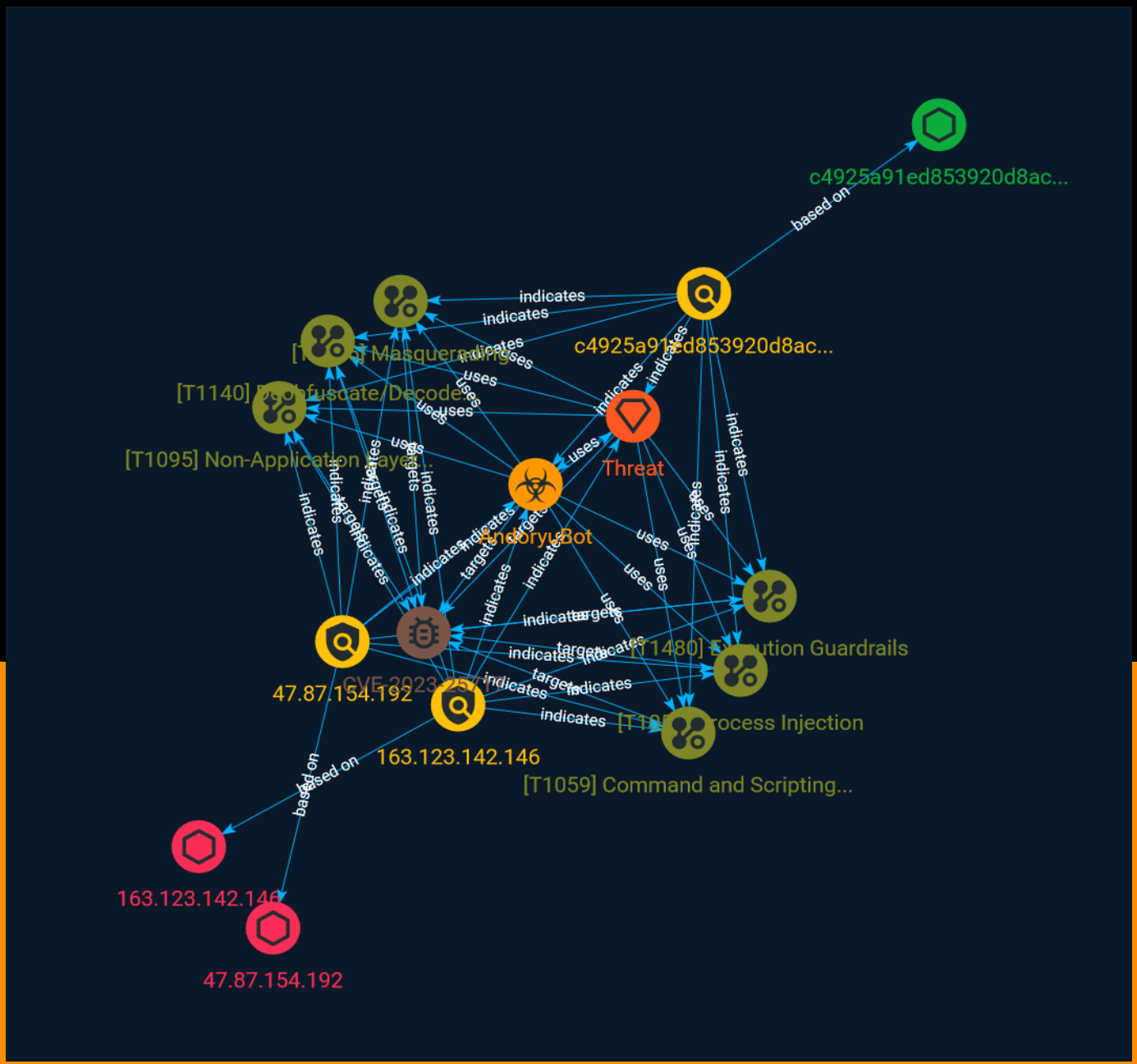

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Researchers have identified a number of Ruckus Wireless Admin panels exposed over the internet to the threat posed by AndoryuBot, a new Botnet malware sold on Telegram.

Confidence

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

15 / 100

Attack-Pattern

Name
Masquerading
ID
T1036
Description
Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names. Renaming abusable system utilities to evade security monitoring is also a form of [Masquerading](https://attack.mitre.org/techniques/T1036).(Citation: LOLBAS Main Site)
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

Non-Application Layer Protocol

ID

T1095

Description

Adversaries may use an OSI non-application layer protocol for communication between host and C2 server or among infected hosts within a network. The list of possible protocols is extensive.(Citation: Wikipedia OSI) Specific examples include use of network layer protocols, such as the Internet Control Message Protocol (ICMP), transport layer protocols, such as the User Datagram Protocol (UDP), session layer protocols, such as Socket Secure (SOCKS), as well as redirected/tunneled protocols, such as Serial over LAN (SOL). ICMP communication between hosts is one example.(Citation: Cisco Synful Knock Evolution) Because ICMP is part of the Internet Protocol Suite, it is required to be implemented by all IP-compatible hosts.(Citation: Microsoft ICMP) However, it is not as commonly monitored as other Internet Protocols such as TCP or UDP and may be used by adversaries to hide communications.

Name

Execution Guardrails

ID

T1480

Description

Adversaries may use execution guardrails to constrain execution or actions based on adversary supplied and environment specific conditions that are expected to be present on the target. Guardrails ensure that a payload only executes against an intended target and reduces collateral damage from an adversary's campaign.(Citation: FireEye Kevin Mandia Guardrails) Values an adversary can provide about a target system or environment to use as guardrails may include specific network share names, attached physical devices, files, joined Active Directory (AD) domains, and local/external IP addresses.(Citation: FireEye Outlook Dec 2019) Guardrails can be used to prevent exposure of capabilities in environments that are not intended to be compromised or operated within. This use of guardrails is distinct from typical [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497). While use of [Virtualization/Sandbox Evasion](https://attack.mitre.org/techniques/T1497) may involve checking for known sandbox values and continuing with execution only if there is no match, the use of guardrails will involve checking for an expected target-specific value and only continuing with execution if there is such a match.

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

Deobfuscate/Decode Files or Information

ID

T1140

Description

Adversaries may use [Obfuscated Files or Information](https://attack.mitre.org/techniques/T1027) to hide artifacts of an intrusion from analysis. They may require separate mechanisms to decode or deobfuscate that information depending on how they intend to use it. Methods for doing that include built-in functionality of malware or by using utilities present on the system. One such example is the use of [certutil](https://attack.mitre.org/software/S0160) to decode a remote access tool portable executable file that has been hidden inside a certificate file.(Citation: Malwarebytes Targeted Attack against Saudi Arabia) Another example is using the Windows `copy /b` command to reassemble binary fragments into a malicious payload.(Citation: Carbon Black Obfuscation Sept 2016) Sometimes a user's action may be required to open it for deobfuscation or decryption as part of [User Execution](https://attack.mitre.org/techniques/T1204). The user may also be required to input a password to open a password protected compressed/encrypted file that was provided by the adversary. (Citation: Volexity PowerDuke November 2016)

Indicator

Name
47.87.154.192
Description
Simple indicator of observable {47.87.154.192}
Pattern Type
stix
Pattern
[ipv4-addr:value = '47.87.154.192']
Name
c4925a91ed853920d8acee79bf0bb9342da4dabc0a2970823027f39ede399bce
Description
Other:Malware-gen\ [Trj] SHA256 of 86d630159a13b4a594e3eae23ccbda891a67f696
Pattern Type
stix

Pattern

[file:hashes.'SHA-256' = 'c4925a91ed853920d8acee79bf0bb9342da4dabc0a2970823027f39ede399bce']

Name

163.123.142.146

Description

ISP: Serverion LLC **OS:** None ---------- Hostnames: ---------- Domains: ---------- Services: **80:** ``` HTTP/1.1 200 OK Date: Thu, 27 Apr 2023 13:34:49 GMT Content-Length: 28 Content-Type: text/plain; charset=utf-8 ``` ---------- **3389:** ``` Remote Desktop Protocol \x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x0f\x08\x00\x02\x00\x00\x00 Remote Desktop Protocol NTLM Info: OS: Windows 8.1/Windows Server 2012 R2 OS Build: 6.3.9600 Target Name: WIN-CLJ1B0GQ6JP NetBIOS Domain Name: WIN-CLJ1B0GQ6JP NetBIOS Computer Name: WIN-CLJ1B0GQ6JP DNS Domain Name: WIN-CLJ1B0GQ6JP FQDN: WIN-CLJ1B0GQ6JP am Windows Server 2012R2 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '163.123.142.146']

Intrusion-Set

Name
Threat

Malware

Name
AndoryuBot

Vulnerability

Name
CVE-2023-25717

StixFile

Value
c4925a91ed853920d8acee79bf0bb9342da4dabc0a2970823027f39ede399bce

IPv4-Addr

Value
163.123.142.146
47.87.154.192

External References

- https://blog.cyble.com/2023/05/17/andoryubots-ddos-rampage/
- https://otx.alienvault.com/pulse/64661d0ea8368c2220aeff78