Jun 21 2023

NETMANAGEIT

Intelligence Report

Condi DDoS Botnet Spreads via TP-Link's CVE-2023-1389

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Researchers have identified a botnet calling itself Condi that is exploiting TP-Link routers vulnerable to a security vulnerability known as CVE-2023-1389, and sells the malware source code.

Confidence

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

15 / 100

Attack-Pattern

Name

Process Discovery

ID

T1057

Description

Adversaries may attempt to get information about running processes on a system. Information obtained could be used to gain an understanding of common software/applications running on systems within the network. Adversaries may use the information from [Process Discovery](https://attack.mitre.org/techniques/T1057) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. In Windows environments, adversaries could obtain details on running processes using the [Tasklist](https://attack.mitre.org/software/S0057) utility via [cmd](https://attack.mitre.org/software/S0106) or `Get-Process` via [PowerShell](https://attack.mitre.org/techniques/T1059/001). Information about processes can also be extracted from the output of [Native API](https://attack.mitre.org/techniques/T1106) calls such as `CreateToolhelp32Snapshot`. In Mac and Linux, this is accomplished with the `ps` command. Adversaries may also opt to enumerate processes via /proc. On network devices, [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `show processes` can be used to display current running processes.(Citation: US-CERT-TA18-106A)(Citation: show_processes_cisco_cmd)

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
admin.duc3k.com
Pattern Type
stix
Pattern
[hostname:value = 'admin.duc3k.com']
Name
cbff9c7b5eea051188cfd0c47bd7f5fe51983fba0b237f400522f22ab91d2772
Description
is__elf
Pattern Type
stix
Pattern

[file:hashes.'SHA-256' = 'cbff9c7b5eea051188cfd0c47bd7f5fe51983fba0b237f400522f22ab91d2772']

Name

f7fb5f3dc06aebcb56f7a9550b005c2c4fc6b2e2a50430d64389914f882d67cf

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f7fb5f3dc06aebcb56f7a9550b005c2c4fc6b2e2a50430d64389914f882d67cf']

Name

5e841db73f5faefe97e38c131433689cb2df6f024466081f26c07c4901fdf612

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '5e841db73f5faefe97e38c131433689cb2df6f024466081f26c07c4901fdf612']

Name

449ad6e25b703b85fb0849a234cbb62770653e6518cf1584a94a52cca31b1190

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '449ad6e25b703b85fb0849a234cbb62770653e6518cf1584a94a52cca31b1190']

Name

291e6383284d38f958fb90d56780536b03bcc321f1177713d3834495f64a3144

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '291e6383284d38f958fb90d56780536b03bcc321f1177713d3834495f64a3144']

Name

e7a4aae413d4742d9c0e25066997153b844789a1409fd0aecce8cc6868729a15

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e7a4aae413d4742d9c0e25066997153b844789a1409fd0aecce8cc6868729a15']

Name

509f5bb6bcc0f2da762847364f7c433d1179fb2b2f4828eefb30828c485a3084

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '509f5bb6bcc0f2da762847364f7c433d1179fb2b2f4828eefb30828c485a3084']

Name

091d1aca4fcd399102610265a57f5a6016f06b1947f86382a2bf2a668912554f

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '091d1aca4fcd399102610265a57f5a6016f06b1947f86382a2bf2a668912554f']

Name

cdn2.duc3k.com

Pattern Type

stix

Pattern

[hostname:value = 'cdn2.duc3k.com']

Name

ccda8a68a412eb1bc468e82dda12eb9a7c9d186fabf0bbdc3f24cd0fb20458cc

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ccda8a68a412eb1bc468e82dda12eb9a7c9d186fabf0bbdc3f24cd0fb20458cc']

Name

85.217.144.35

Description

CC=US ASN=AS211252 Delis LLC

Pattern Type

stix

Pattern

[ipv4-addr:value = '85.217.144.35']

Name

http://cdn2.duc3k.com/t

Pattern Type

stix

Pattern

[url:value = 'http://cdn2.duc3k.com/t']

Name

593e75b5809591469dbf57a7f76f93cb256471d89267c3800f855cabefe49315

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '593e75b5809591469dbf57a7f76f93cb256471d89267c3800f855cabefe49315']

Name

4e3fa5fa2dcc6328c71fed84c9d18dfdbd34f8688c6bee1526fd22ee1d749e5a

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4e3fa5fa2dcc6328c71fed84c9d18dfdbd34f8688c6bee1526fd22ee1d749e5a']

Malware

Name
Mirai
Name
Moobot
Name
Condi

Vulnerability

Name
CVE-2023-1389

StixFile

Value
509f5bb6bcc0f2da762847364f7c433d1179fb2b2f4828eefb30828c485a3084
291e6383284d38f958fb90d56780536b03bcc321f1177713d3834495f64a3144
cbff9c7b5eea051188cfd0c47bd7f5fe51983fba0b237f400522f22ab91d2772
5e841db73f5faefe97e38c131433689cb2df6f024466081f26c07c4901fdf612
449ad6e25b703b85fb0849a234cbb62770653e6518cf1584a94a52cca31b1190
4e3fa5fa2dcc6328c71fed84c9d18dfdbd34f8688c6bee1526fd22ee1d749e5a
f7fb5f3dc06aebcb56f7a9550b005c2c4fc6b2e2a50430d64389914f882d67cf
593e75b5809591469dbf57a7f76f93cb256471d89267c3800f855cabefe49315
091d1aca4fcd399102610265a57f5a6016f06b1947f86382a2bf2a668912554f
e7a4aae413d4742d9c0e25066997153b844789a1409fd0aecce8cc6868729a15
ccda8a68a412eb1bc468e82dda12eb9a7c9d186fabf0bbdc3f24cd0fb20458cc

Hostname

Value
cdn2.duc3k.com
admin.duc3k.com

IPv4-Addr

Value
85.217.144.35

Url

Value
http://cdn2.duc3k.com/t

External References

- https://otx.alienvault.com/pulse/6492f7af0392421eda959d85
- https://www.fortinet.com/blog/threat-research/condi-ddos-botnet-spreads-via-tp-links-cve-2023-1389