Sep 02 2023

NETMANAGEIT

Intelligence Report

A Deep Dive into Brute Ratel C4 payloads

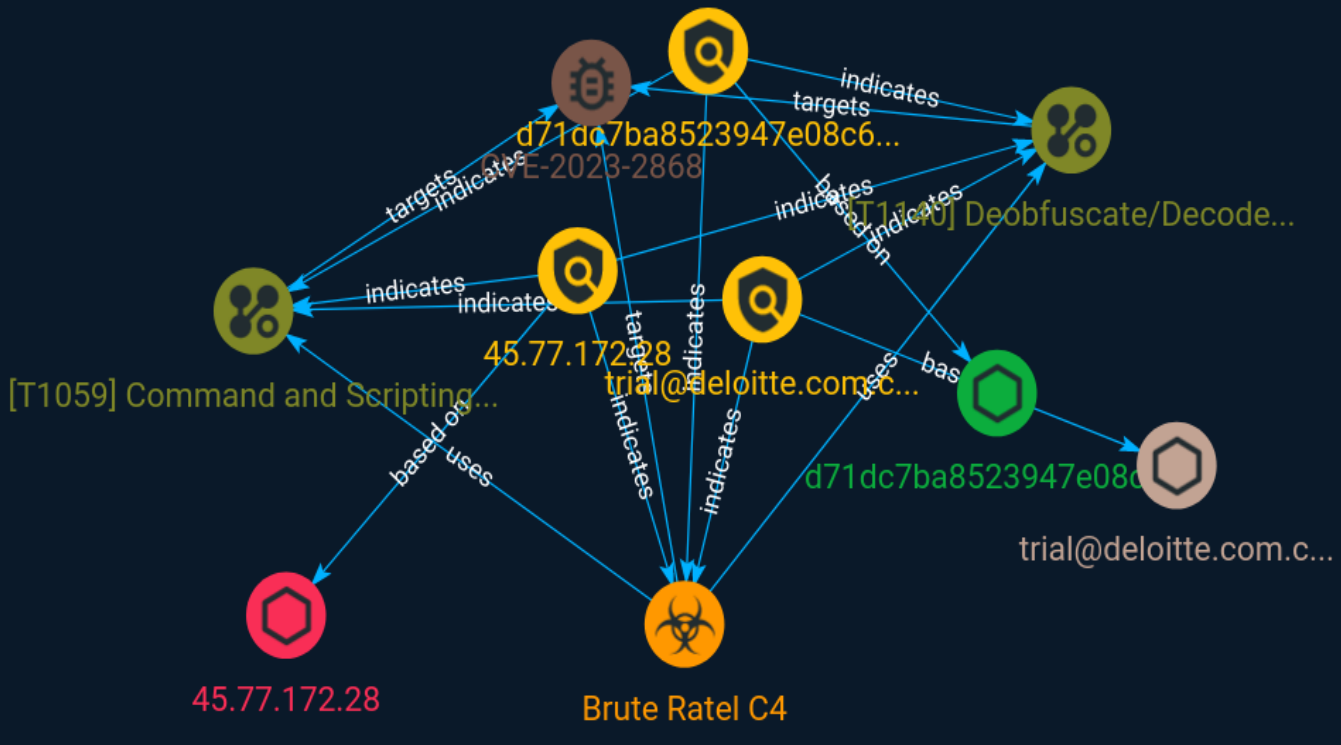

Table of contents

Overview

Entities

Observables

External References

Overview

Description

A technical analysis of a Brute Ratel C4 badger

Confidence

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

15 / 100

Indicator

Name

trial@deloitte.com.cn

Pattern Type

stix

Pattern

[email-addr:value = 'trial@deloitte.com.cn']

Name

45.77.172.28

Description

ISP: The Constant Company, LLC **OS:** None ---------- Hostnames: - 45.77.172.28.vultrusercontent.com ---------- Domains: - vultrusercontent.com ---------- Services: **80:** ``` ``` ---------- **443:** ``` SSL Error: TLSV1_UNRECOGNIZED_NAME ``` ---------- **8443:** ``` HTTP/1.1 200 OK Server: nginx Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: keep-alive Vary: Accept-Encoding Cache-Control: max-age=0, must-revalidate, private Date: Tue, 29 Aug 2023 15:49:50 GMT Expires: Tue, 29 Aug 2023 15:49:50 GMT Set-Cookie: locale=en; path=/; secure; httponly; samesite=lax Set-Cookie: cloudpanel=j8h9mh85m01jabo5vhmcnqcuck; path=/; secure; httponly; samesite=lax ``` HEARTBLEED: 2023/08/29 15:50:01 45.77.172.28:8443 - SAFE ----------

Pattern Type
stix
Pattern
[ipv4-addr:value = '45.77.172.28']
Name
d71dc7ba8523947e08c6eec43a726fe75aed248dfd3a7c4f6537224e9ed05f6f
Description
SLF:MeterRefLoadApiHash
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'd71dc7ba8523947e08c6eec43a726fe75aed248dfd3a7c4f6537224e9ed05f6f']

Malware

Name
Brute Ratel C4

Vulnerability

Name
CVE-2023-2868

Attack-Pattern

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)

Email-Addr

Value
trial@deloitte.com.cn

IPv4-Addr

Value
45.77.172.28

StixFile

Value
d71dc7ba8523947e08c6eec43a726fe75aed248dfd3a7c4f6537224e9ed05f6f

External References

- https://otx.alienvault.com/pulse/64f1e5d7b2ba78bf0012e62d
- https://cybergeeks.tech/a-deep-dive-into-brute-ratel-c4-payloads/