Jun 14 2023

NETMANAGEIT

Intelligence Report

The Phantom Menace: Brute Ratel remains rare and targeted

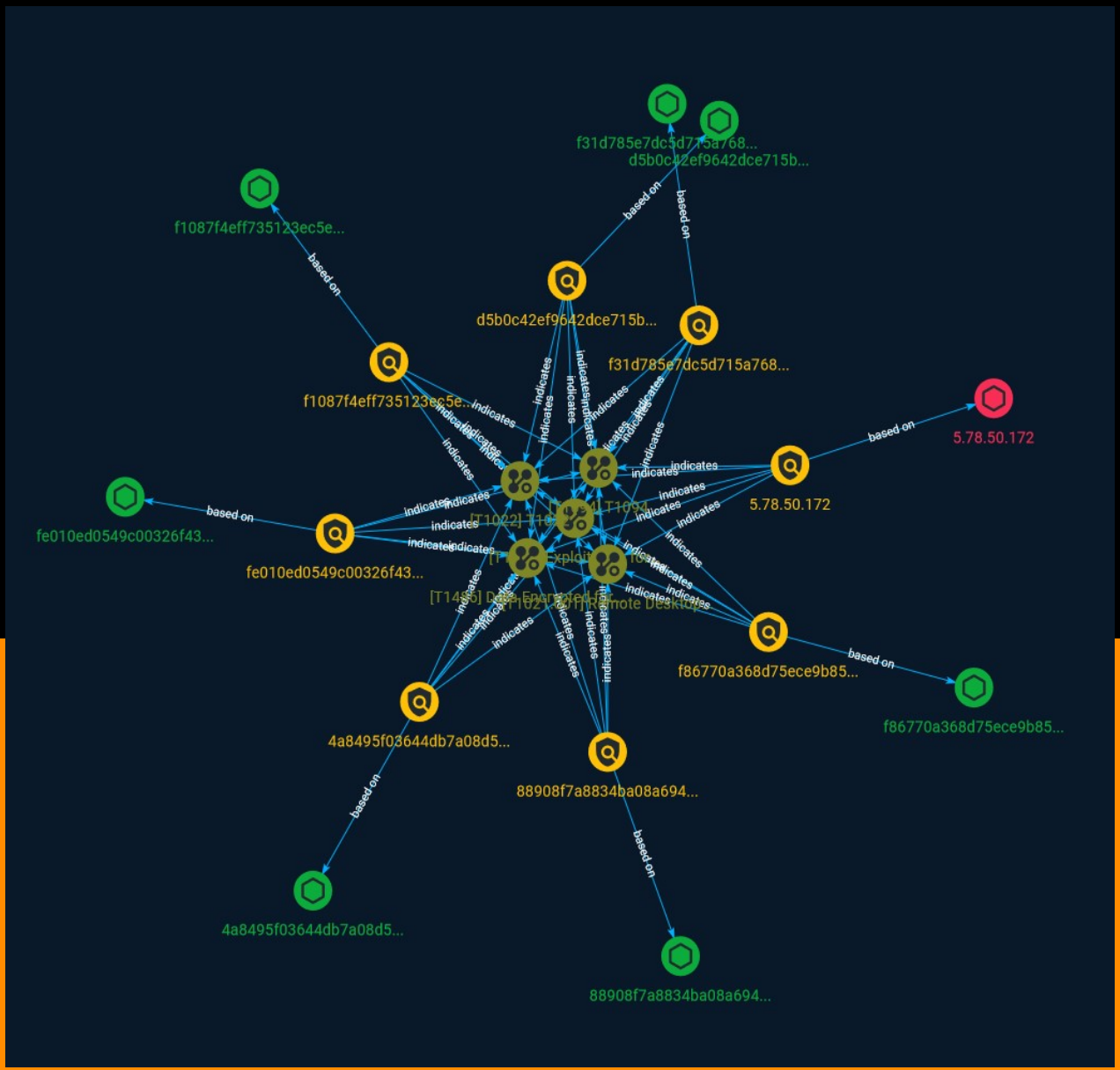

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Last year, we reported the growing use of the commercial offensive security tool Brute Ratel by criminal actors, including those behind Black Cat ransomware incidents. After public exposure of a version of the tool, many were concerned that Brute Ratel would become widely adopted as the successor to Cobalt Strike, the long-lived and long-abused offensive security tool that has been the go-to for malicious actors' lateral movement needs.

Confidence

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

15 / 100

Attack-Pattern

Name
Exploitation for Privilege Escalation
ID
T1068
Description
Adversaries may exploit software vulnerabilities in an attempt to elevate privileges. Exploitation of a software vulnerability occurs when an adversary takes advantage of a programming error in a program, service, or within the operating system software or kernel itself to execute adversary-controlled code. Security constructs such as permission levels will often hinder access to information and use of certain techniques, so adversaries will likely need to perform privilege escalation to include use of software exploitation to circumvent those restrictions. When initially gaining access to a system, an adversary may be operating within a lower privileged process which will prevent them from accessing certain resources on the system. Vulnerabilities may exist, usually in operating system components and software commonly running at higher permissions, that can be exploited to gain higher levels of access on the system. This could enable someone to move from unprivileged or user level permissions to SYSTEM or root permissions depending on the component that is vulnerable. This could also enable an adversary to move from a virtualized environment, such as within a virtual machine or container, onto the underlying host. This may be a necessary step for an adversary compromising an endpoint system that has been properly configured and limits other privilege escalation methods. Adversaries may bring a signed vulnerable driver onto a compromised machine so that they can exploit the vulnerability to execute code in kernel mode. This process is sometimes referred to as Bring Your Own Vulnerable Driver (BYOVD).(Citation: ESET InvisiMole June 2020)(Citation: Unit42 AcidBox June 2020) Adversaries may include the vulnerable driver with files delivered during Initial Access or download it to a

compromised system via [Ingress Tool Transfer](https://attack.mitre.org/techniques/T1105) or [Lateral Tool Transfer](https://attack.mitre.org/techniques/T1570).

Name

Data Encrypted for Impact

ID

T1486

Description

Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.(Citation: US-CERT Ransomware 2016)(Citation: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017)(Citation: US-CERT SamSam 2018) In the case of ransomware, it is typical that common user files like Office documents, PDFs, images, videos, audio, text, and source code files will be encrypted (and often renamed and/or tagged with specific file markers). Adversaries may need to first employ other behaviors, such as [File and Directory Permissions Modification](https://attack.mitre.org/techniques/T1222) or [System Shutdown/Reboot](https://attack.mitre.org/techniques/T1529), in order to unlock and/or gain access to manipulate these files.(Citation: CarbonBlack Conti July 2020) In some cases, adversaries may encrypt critical system files, disk partitions, and the MBR.(Citation: US-CERT NotPetya 2017) To maximize impact on the target organization, malware designed for encrypting data may have worm-like features to propagate across a network by leveraging other attack techniques like [Valid Accounts](https://attack.mitre.org/techniques/T1078), [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), and [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002).(Citation: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017) Encryption malware may also leverage [Internal Defacement](https://attack.mitre.org/techniques/T1491/001), such as changing victim wallpapers, or otherwise intimidate victims by sending ransom notes or other messages to connected printers (known as "print bombing").(Citation: NHS Digital Egregor Nov 2020) In cloud environments, storage objects within compromised accounts may also be encrypted.(Citation: Rhino S3 Ransomware Part 1)

Name

T1094

ID

T1094

Name

Remote Desktop Protocol

ID

T1021.001

Description

Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to log into a computer using the Remote Desktop Protocol (RDP). The adversary may then perform actions as the logged-on user. Remote desktop is a common feature in operating systems. It allows a user to log into an interactive session with a system desktop graphical user interface on a remote system. Microsoft refers to its implementation of the Remote Desktop Protocol (RDP) as Remote Desktop Services (RDS).(Citation: TechNet Remote Desktop Services) Adversaries may connect to a remote system over RDP/RDS to expand access if the service is enabled and allows access to accounts with known credentials. Adversaries will likely use Credential Access techniques to acquire credentials to use with RDP. Adversaries may also use RDP in conjunction with the [Accessibility Features](https://attack.mitre.org/techniques/T1546/008) or [Terminal Services DLL](https://attack.mitre.org/techniques/T1505/005) for Persistence.(Citation: Alperovitch Malware)

Name

T1022

ID

T1022

Indicator

Name

f1087f4eff735123ec5ec7fe67b11208c73fc49110bde60cecd42f1a10ed9c89

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f1087f4eff735123ec5ec7fe67b11208c73fc49110bde60cecd42f1a10ed9c89']

Name

5.78.50.172

Description

ISP: Hetzner Online GmbH **OS:** Debian ---------- Hostnames: - static.172.50.78.5.clients.your-server.de ---------- Domains: - your-server.de ---------- Services: **22:** ``` SSH-2.0-OpenSSH_8.4p1 Debian-5+deb11u1 Key type: ssh-rsa Key: AAAAB3NzaC1yc2EAAAADAQABAAABgQDuVFIv1tIfIapG4UrpbXYSFuorvSUa6cNiWF9xu270o1MMQ3wgP+79lHM0XiD49C+0OkVv7pqVl6xfkMEudZoA0w6Owi6g2hWZA2ddrD+7JpvsgipsTPSqFYY9u8wvS5ZtdP6T+b3LB/g2R0mRWL03Af6pWm6TRdzaKZlxsApW0VjaKoOzcWzfaSjGxL03SqQUJyCV2D4h9e2MwvGOwnz49UhEXd+42iKStVmuGWWqZ5mW4JniyYQi2alU7q3AYk1pjwf/2Suw2VLkhzJSd9epMI6iqhMlRg0wPKMfgvKp2j1U58WxtA5LWRf1Xf5Ych06hQAFjDSG3yUSNLj/fSwb727GAa7pi8IwkI/v1Tpy9LccY2QpjvildgzSvIMTJ0mDPVgOeiEiopBJ3w8hFsU6q3Hyt+xTQIh3CGHWfHkY

XY6Fdir6O5wCm4VyBpzqY8gumScruhFYlPl+xQ8VOEjWmFGuRORtE0StExBR677oLgVJrg+R8lXC iESk+96HsEU= Fingerprint: 1f:ec:8f:3f:a4:81:87:c0:21:63:1d:e6:48:38:ee:7d 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 ``` ----------

Pattern Type

stix

Pattern

[ipv4-addr:value = '5.78.50.172']

Name

4a8495f03644db7a08d5a995b4f373eff2ade8e61261fb4818ac0bb9da7b0540

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '4a8495f03644db7a08d5a995b4f373eff2ade8e61261fb4818ac0bb9da7b0540']

Name

d5b0c42ef9642dce715b252a07fc07ad9917bfdc13bd699d517b78210cc6ec60

Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'd5b0c42ef9642dce715b252a07fc07ad9917bfdc13bd699d517b78210cc6ec60']
Name
f86770a368d75ece9b8542e3087218c01676c0444e18d5d68f53902619049462
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'f86770a368d75ece9b8542e3087218c01676c0444e18d5d68f53902619049462']
Name
fe010ed0549c00326f4319c1ac2d16684957a2fd09e0c7bbfec55e92f5d8606c
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'fe010ed0549c00326f4319c1ac2d16684957a2fd09e0c7bbfec55e92f5d8606c']

Name
f31d785e7dc5d715a768d0d9565488cbeeb9ab35e4a0895785ecea533692176a
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = 'f31d785e7dc5d715a768d0d9565488cbeeb9ab35e4a0895785ecea533692176a']
Name
88908f7a8834ba08a69403af99aca50f61cb8c571fe6b50046ccba5b146f5a45
Pattern Type
stix
Pattern
[file:hashes.'SHA-256' = '88908f7a8834ba08a69403af99aca50f61cb8c571fe6b50046ccba5b146f5a45']

StixFile

Value
d5b0c42ef9642dce715b252a07fc07ad9917bfdc13bd699d517b78210cc6ec60
4a8495f03644db7a08d5a995b4f373eff2ade8e61261fb4818ac0bb9da7b0540
f86770a368d75ece9b8542e3087218c01676c0444e18d5d68f53902619049462
f1087f4eff735123ec5ec7fe67b11208c73fc49110bde60cecd42f1a10ed9c89
f31d785e7dc5d715a768d0d9565488cbeeb9ab35e4a0895785ecea533692176a
fe010ed0549c00326f4319c1ac2d16684957a2fd09e0c7bbfec55e92f5d8606c
88908f7a8834ba08a69403af99aca50f61cb8c571fe6b50046ccba5b146f5a45

IPv4-Addr

Value
5.78.50.172

External References

- https://otx.alienvault.com/pulse/648a0804f0c7af02f1fefd6e
- https://news.sophos.com/en-us/2023/05/18/the-phantom-menace-brute-ratel-remains-rare-and-targeted/
- https://github.com/sophoslabs/IoCs/blob/master/ATK-Brutel.csv