Feb 15 2024

NETMANAGEIT

Intelligence Report

Fileless Revenge RAT Malware

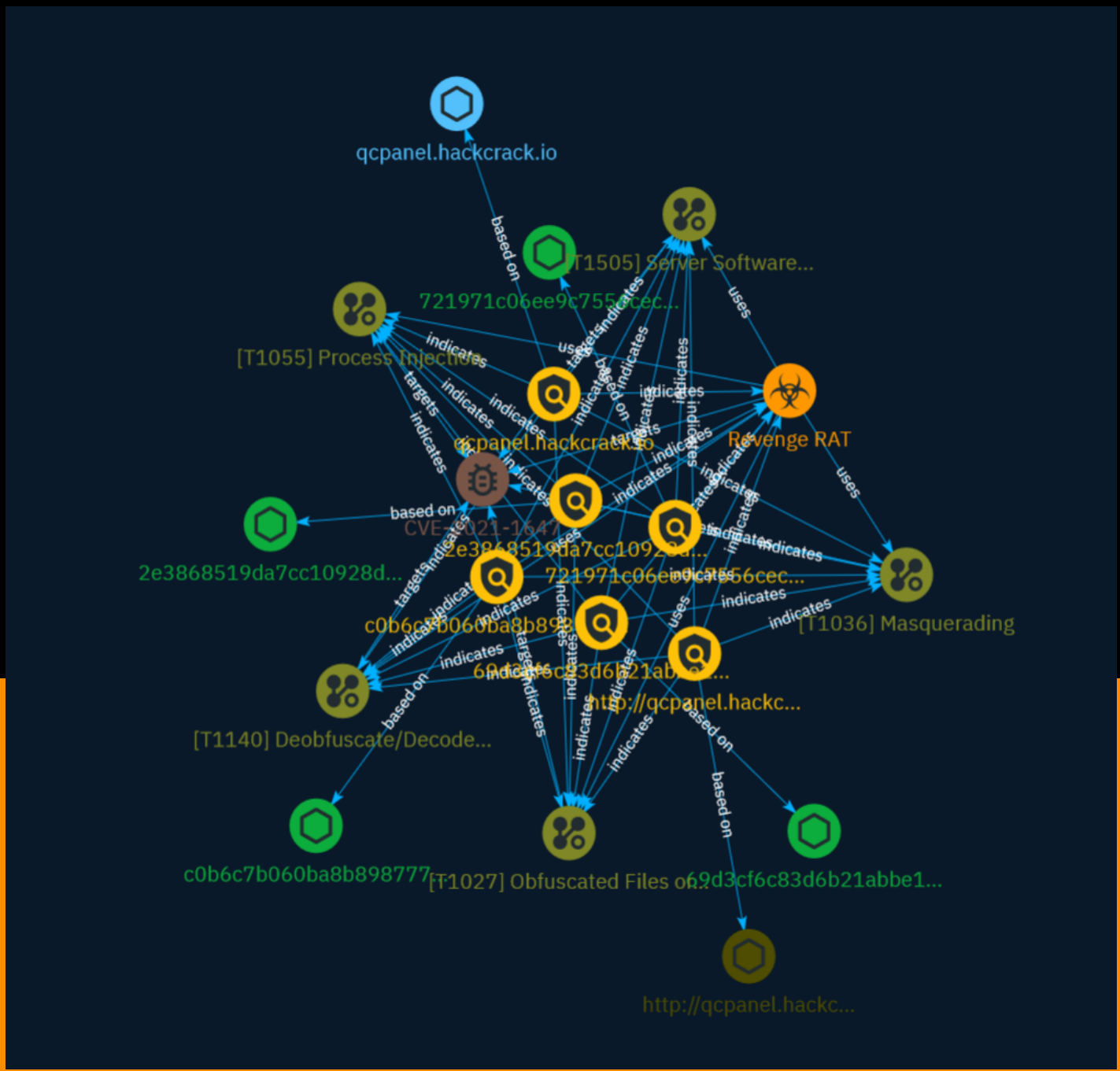

Table of contents

Overview

Entities

Observables

External References

Overview

Description

AhnLab SEcurity intelligence Center (ASEC) recently discovered the distribution of Revenge RAT malware that had been developed based on legitimate tools. It appears that the attackers have used tools such as ‘smtp-validator’ and ‘Email To Sms’. At the time of execution, the malware creates and runs both a legitimate tool and a malicious file, making it difficult for users to realize that a malicious activity has occurred.

Confidence

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

15 / 100

Content

N/A

Indicator

Name

qcpanel.hackcrack.io

Pattern Type

stix

Pattern

[hostname:value = 'qcpanel.hackcrack.io']

Name

http://qcpanel.hackcrack.io:9561

Description

- **Unsafe:** True - **Server:** N/A - **Domain Rank:** 972180 - **DNS Valid:** True - **Parking:** True - **Spamming:** False - **Malware:** True - **Phishing:** True - **Suspicious:** True - **Adult:** False - **Category:** Web Tracker - **Domain Age:** {'human': '2 years ago', 'timestamp': 1648054803, 'iso': '2022-03-23T13:00:03-04:00'} - **IPQS: Domain:** qcpanel.hackcrack.io - **IPQS: IP Address:** 147.185.221.17

Pattern Type

stix

Pattern

[url:value = 'http://qcpanel.hackcrack.io:9561']

Name

c0b6c7b060ba8b898777ce72e4a2d0b0a9df4591dddd10037762da40e6887fc2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'c0b6c7b060ba8b898777ce72e4a2d0b0a9df4591dddd10037762da40e6887fc2']

Name

721971c06ee9c7556cec79f67b2f0177374c4d48877a3e973fcf120e6a1849df

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '721971c06ee9c7556cec79f67b2f0177374c4d48877a3e973fcf120e6a1849df']

Name

69d3cf6c83d6b21abbe13ea46f6fa0462c564712ddad17b9151ac36db85486fe

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '69d3cf6c83d6b21abbe13ea46f6fa0462c564712ddad17b9151ac36db85486fe']

Name

2e3868519da7cc10928d7398cd9b8b989a8018ac9fc99a666da96bc4fbf4ac9c

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '2e3868519da7cc10928d7398cd9b8b989a8018ac9fc99a666da96bc4fbf4ac9c']

Vulnerability

Name
CVE-2021-1647
Description
Microsoft Defender contains an unspecified vulnerability that allows for remote code execution.

Malware

Name
Revenge RAT
Description
[Revenge RAT](https://attack.mitre.org/software/S0379) is a freely available remote access tool written in .NET (C#).(Citation: Cylance Shaheen Nov 2018)(Citation: Cofense RevengeRAT Feb 2019)

Attack-Pattern

Name
Server Software Component
ID
T1505
Description
Adversaries may abuse legitimate extensible development features of servers to establish persistent access to systems. Enterprise server applications may include features that allow developers to write and install software or scripts to extend the functionality of the main application. Adversaries may install malicious components to extend and abuse server applications.(Citation: volexity_0day_sophos_FW)
Name
Obfuscated Files or Information
ID
T1027
Description
Adversaries may attempt to make an executable or file difficult to discover or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. This is common behavior that can be used across different platforms and the network to

evade defenses. Payloads may be compressed, archived, or encrypted in order to avoid detection. These payloads may be used during Initial Access or later to mitigate detection. Sometimes a user's action may be required to open and [Deobfuscate/Decode Files or Information](https://attack.mitre.org/techniques/T1140) for [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) Adversaries may also use compressed or archived scripts, such as JavaScript. Portions of files can also be encoded to hide the plain-text strings that would otherwise help defenders with discovery. (Citation: Linux/Cdorked.A We Live Security Analysis) Payloads may also be split into separate, seemingly benign files that only reveal malicious functionality when reassembled. (Citation: Carbon Black Obfuscation Sept 2016) Adversaries may also abuse [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010) to obscure commands executed from payloads or directly via [Command and Scripting Interpreter](https://attack.mitre.org/techniques/T1059). Environment variables, aliases, characters, and other platform/language specific semantics can be used to evade signature based detections and application control mechanisms. (Citation: FireEye Obfuscation June 2017) (Citation: FireEye Revoke-Obfuscation July 2017)(Citation: PaloAlto EncodedCommand March 2017)

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

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) Masquerading may also include the use of [Proxy](https://attack.mitre.org/techniques/T1090) or VPNs to disguise IP addresses, which can allow adversaries to blend in with normal network traffic and bypass conditional access policies or anti-abuse protections.

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)

Hostname

Value
qcpanel.hackcrack.io

Url

Value
http://qcpanel.hackcrack.io:9561

StixFile

Value
c0b6c7b060ba8b898777ce72e4a2d0b0a9df4591dddd10037762da40e6887fc2
721971c06ee9c7556cec79f67b2f0177374c4d48877a3e973fcf120e6a1849df
69d3cf6c83d6b21abbe13ea46f6fa0462c564712ddad17b9151ac36db85486fe
2e3868519da7cc10928d7398cd9b8b989a8018ac9fc99a666da96bc4fbf4ac9c

External References

- https://asec.ahnlab.com/en/61584/
- https://otx.alienvault.com/pulse/65cc8f2baf18018d9e3b51ee