Jul 05 2023

NETMANAGEIT

Intelligence Report

Crysis Threat Actor Installing Venus Ransomware Through RDP

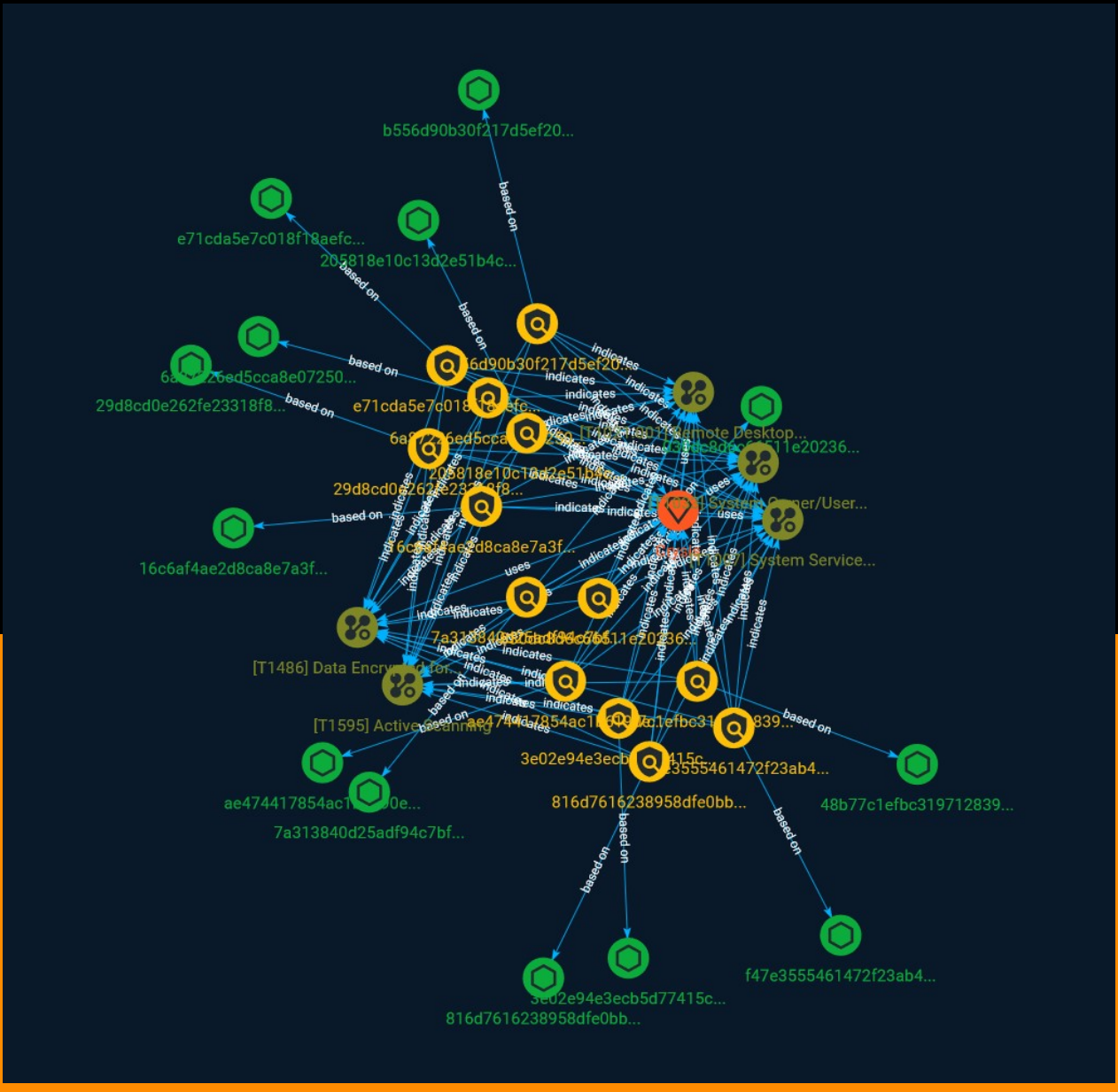

Table of contents

Overview

Entities

Observables

External References

Overview

Description

AhnLab Security Emergency response Center (ASEC) has recently discovered that the Crysis ransomware's threat actor is also using the Venus ransomware in the attacks. Crysis and Venus are both major ransomware types known to target externally exposed remote desktop services. [1] Actual logs from the AhnLab Smart Defense (ASD) infrastructure also show attacks being launched through RDP.

Confidence

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

15 / 100

Indicator

Name

48b77c1efbc3197128391a35d0e1ed0b5cc3a05b96dd12c98ac73ffc6a886fc8

Description

ChromePass SHA256 of 2a541cb2c47e26791bca8f7ef337fe38

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '48b77c1efbc3197128391a35d0e1ed0b5cc3a05b96dd12c98ac73ffc6a886fc8']

Name

29d8cd0e262fe23318f8d8adc4a34dd9c33da769a5136c3ff3c7dba42fbf4237

Description

HackTool:Win32/Mikatz!dha SHA256 of 51373c09f0cb65ab149b0423d85f057e

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '29d8cd0e262fe23318f8d8adc4a34dd9c33da769a5136c3ff3c7dba42fbf4237']

Name

3e02e94e3ecb5d77415c25ee7ecece24953b4d7bd21bf9f9e3413ffbdad472d2

Description

HackTool:Win32/Mimikatz.D SHA256 of 8d0a0f482090df08b986c7389c1401c2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '3e02e94e3ecb5d77415c25ee7ecece24953b4d7bd21bf9f9e3413ffbdad472d2']

Name

7a313840d25adf94c7bf1d17393f5b991ba8baf50b8cacb7ce0420189c177e26

Description

Win.Trojan.Sality-126545 SHA256 of df218168bf83d26386dfd4ece7aef2d0

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '7a313840d25adf94c7bf1d17393f5b991ba8baf50b8cacb7ce0420189c177e26']

Name

16c6af4ae2d8ca8e7a3f2051b913fa1cb7e1fbd0110b0736614a1e02bbbbceaf

Description

#Lowfi:SIGATTR:PossibleIMSteal SHA256 of cc2d70a961bc6dce79168ae99ab30673

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '16c6af4ae2d8ca8e7a3f2051b913fa1cb7e1fbd0110b0736614a1e02bbbbceaf']

Name

ae474417854ac1b6190e15cc514728433a26cc815fdc6d12150ef55e92d643ea

Description

Nrv2x SHA256 of 3684fe7a1cfe5285f3f71d4ba84ffab2

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'ae474417854ac1b6190e15cc514728433a26cc815fdc6d12150ef55e92d643ea']

Name

b556d90b30f217d5ef20ebe3f15cce6382c4199e900b5ad2262a751909da1b34

Description

HackTool:Win32/Passview.ARD!MTB SHA256 of 57445041f7a1e57da92e858fc3efeabe

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'b556d90b30f217d5ef20ebe3f15cce6382c4199e900b5ad2262a751909da1b34']

Name

f47e3555461472f23ab4766e4d5b6f6fd260e335a6abc31b860e569a720a5446

Description

Win.Tool.ShareScanner-6827521-0 SHA256 of 597de376b1f80c06d501415dd973dcec

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'f47e3555461472f23ab4766e4d5b6f6fd260e335a6abc31b860e569a720a5446']

Name

030dc8d6c66511e2023640aa2fdf7eed90e498ef82b88c44514fb547b1193c2c

Description

HackTool:Win64/Mikatz!dha SHA256 of 4984b907639851dfa8409e60c838e885

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '030dc8d6c66511e2023640aa2fdf7eed90e498ef82b88c44514fb547b1193c2c']

Name

6a87226ed5cca8e072507d6c24289c57757dd96177f329a00b00e40427a1d473

Description

SHA256 of f627c30429d967082cdcf634aa735410

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '6a87226ed5cca8e072507d6c24289c57757dd96177f329a00b00e40427a1d473']

Name

816d7616238958dfe0bb811a063eb3102efd82eff14408f5cab4cb5258bfd019

Description

SHA256 of d28f0cfae377553fcb85918c29f4889b

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '816d7616238958dfe0bb811a063eb3102efd82eff14408f5cab4cb5258bfd019']

Name

e71cda5e7c018f18aefcdfbce171cfeee7b8d556e5036d8b8f0864efc5f2156b

Description

SHA256 of 7f31636f9b74ab93a268f5a473066053

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = 'e71cda5e7c018f18aefcdfbce171cfeee7b8d556e5036d8b8f0864efc5f2156b']

Name

205818e10c13d2e51b4c0196ca30111276ca1107fc8e25a0992fe67879eab964

Description

HackTool:Win32/Passview!MSR SHA256 of 44bd492dfb54107ebfe063fcbfbddff5

Pattern Type

stix

Pattern

[file:hashes.'SHA-256' = '205818e10c13d2e51b4c0196ca30111276ca1107fc8e25a0992fe67879eab964']

Intrusion-Set

Name
Crysis

Attack-Pattern

Name
Active Scanning
ID
T1595
Description
Adversaries may execute active reconnaissance scans to gather information that can be used during targeting. Active scans are those where the adversary probes victim infrastructure via network traffic, as opposed to other forms of reconnaissance that do not involve direct interaction. Adversaries may perform different forms of active scanning depending on what information they seek to gather. These scans can also be performed in various ways, including using native features of network protocols such as ICMP.(Citation: Botnet Scan)(Citation: OWASP Fingerprinting) Information from these scans may reveal opportunities for other forms of reconnaissance (ex: [Search Open Websites/Domains](https://attack.mitre.org/techniques/T1593) or [Search Open Technical Databases](https://attack.mitre.org/techniques/T1596)), establishing operational resources (ex: [Develop Capabilities](https://attack.mitre.org/techniques/T1587) or [Obtain Capabilities](https://attack.mitre.org/techniques/T1588)), and/or initial access (ex: [External Remote Services](https://attack.mitre.org/techniques/T1133) or [Exploit Public-Facing Application](https://attack.mitre.org/techniques/T1190)).
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

System Service Discovery

ID

T1007

Description

Adversaries may try to gather information about registered local system services. Adversaries may obtain information about services using tools as well as OS utility commands such as `sc query`, `tasklist /svc`, `systemctl --type=service`, and `net start`. Adversaries may use the information from [System Service Discovery](https://attack.mitre.org/techniques/T1007) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions.

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

System Owner/User Discovery

ID

T1033

Description

Adversaries may attempt to identify the primary user, currently logged in user, set of users that commonly uses a system, or whether a user is actively using the system. They may do this, for example, by retrieving account usernames or by using [OS Credential Dumping](https://attack.mitre.org/techniques/T1003). The information may be collected in a number of different ways using other Discovery techniques, because user and username details are prevalent throughout a system and include running process ownership, file/directory ownership, session information, and system logs. Adversaries may use the information from [System Owner/User Discovery](https://attack.mitre.org/techniques/T1033) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Various utilities and commands may acquire this information, including `whoami`. In macOS and Linux, the currently logged in user can be identified with `w` and `who`. On macOS the `dscl . list /Users | grep -v '_'` command can also be used to enumerate user accounts. Environment variables, such as `%USERNAME%` and `$USER`, may also be used to access this information. On network devices, [Network Device CLI](https://attack.mitre.org/techniques/T1059/008) commands such as `show users` and `show ssh` can be used to display users currently logged into the device.(Citation: show_ssh_users_cmd_cisco)(Citation: US-CERT TA18-106A Network Infrastructure Devices 2018)

StixFile

Value
ae474417854ac1b6190e15cc514728433a26cc815fdc6d12150ef55e92d643ea
f47e3555461472f23ab4766e4d5b6f6fd260e335a6abc31b860e569a720a5446
16c6af4ae2d8ca8e7a3f2051b913fa1cb7e1fbd0110b0736614a1e02bbbbceaf
030dc8d6c66511e2023640aa2fdf7eed90e498ef82b88c44514fb547b1193c2c
3e02e94e3ecb5d77415c25ee7ecece24953b4d7bd21bf9f9e3413ffbdad472d2
29d8cd0e262fe23318f8d8adc4a34dd9c33da769a5136c3ff3c7dba42fbf4237
48b77c1efbc3197128391a35d0e1ed0b5cc3a05b96dd12c98ac73ffc6a886fc8
6a87226ed5cca8e072507d6c24289c57757dd96177f329a00b00e40427a1d473
b556d90b30f217d5ef20ebe3f15cce6382c4199e900b5ad2262a751909da1b34
7a313840d25adf94c7bf1d17393f5b991ba8baf50b8cacb7ce0420189c177e26
205818e10c13d2e51b4c0196ca30111276ca1107fc8e25a0992fe67879eab964
e71cda5e7c018f18aefcdfbce171cfeee7b8d556e5036d8b8f0864efc5f2156b
816d7616238958dfe0bb811a063eb3102efd82eff14408f5cab4cb5258bfd019

External References

- https://asec.ahnlab.com/en/54937/
- https://otx.alienvault.com/pulse/64a58f7faf97c4314d8c529a