Aug 31 2023

NETMANAGEIT

Intelligence Report

Threat Actor Interplay | Good Day’s Victim Portals and Their Ties to Cloak

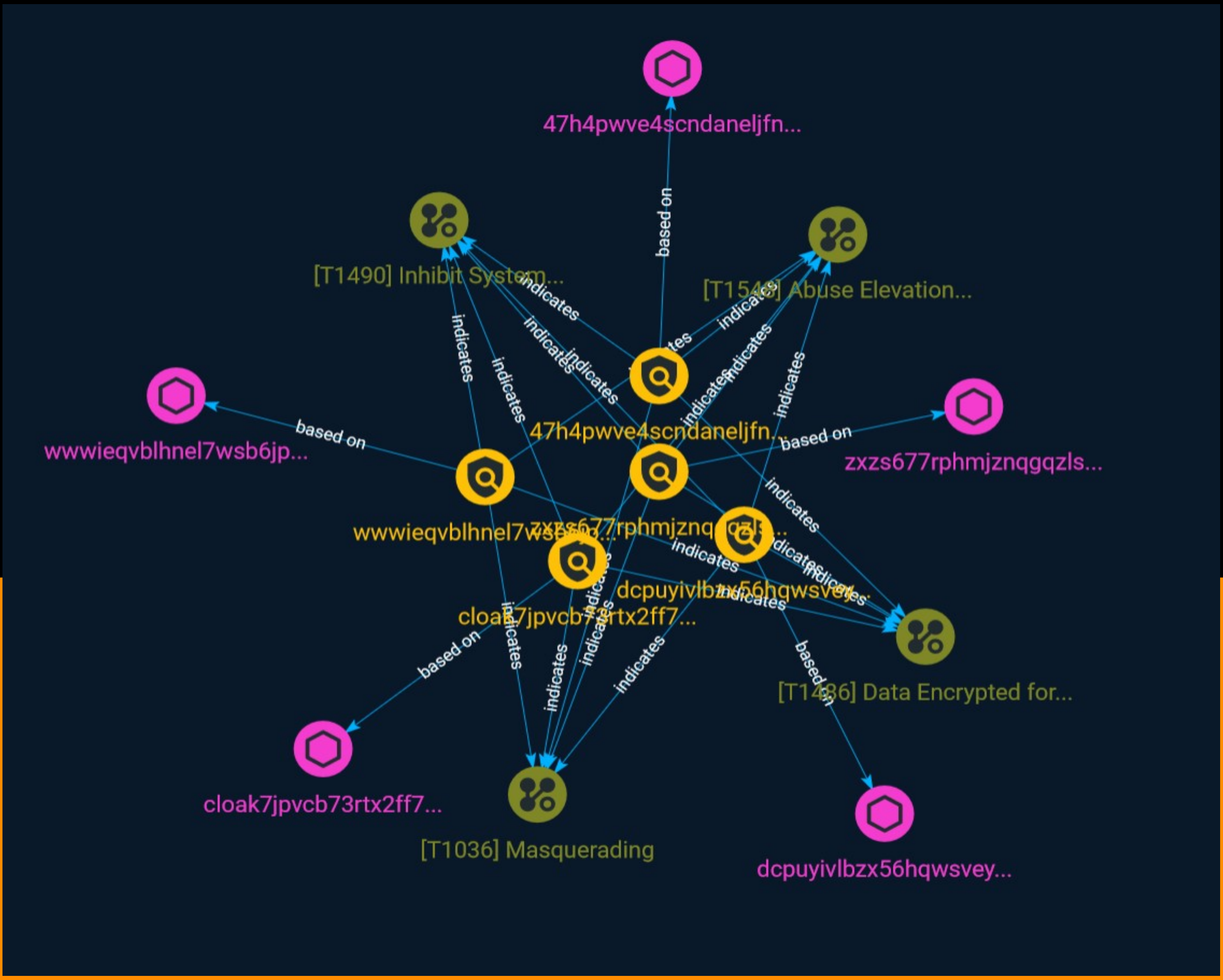

Table of contents

Overview

Entities

Observables

External References

Overview

Description

Good Day ransomware, a variant within the ARCrypter family, was first observed in-the-wild in May of 2023. Between June and August of 2023, we observed an uptick in Good Day ransomware campaigns and a proliferation of new ransom note samples in public malware repositories. This new wave of Good Day attacks feature individual TOR-based victim portals for each target.

Confidence

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

15 / 100

Indicator

Name

dcpuyivlbzx56hqwsvey33bxobxw3timjgljjy3index6qvdls5bjoad.onion

Pattern Type

stix

Pattern

[domain-name:value =
'dcpuyivlbzx56hqwsvey33bxobxw3timjgljjy3index6qvdls5bjoad.onion']

Name

zxzs677rphmjznqgqzlsmjtqwqlydq47rwjesrt4dkkh6cc2ftlfhuqd.onion

Pattern Type

stix

Pattern

[domain-name:value =
'zxzs677rphmjznqgqzlsmjtqwqlydq47rwjesrt4dkkh6cc2ftlfhuqd.onion']

Name

47h4pwve4scndaneljfnxdhzoulgsyfzbgayyonbwztfz74gsdprz5qd.onion

Pattern Type

stix

Pattern

[domain-name:value = '47h4pwve4scndaneljfnxdhzoulgsyfzbgayyonbwztfz74gsdprz5qd.onion']

Name

cloak7jpvcb73rtx2ff7kaw2kholu7bdiivxpzbhlny4ybz75dpxckqd.onion

Pattern Type

stix

Pattern

[domain-name:value = 'cloak7jpvcb73rtx2ff7kaw2kholu7bdiivxpzbhlny4ybz75dpxckqd.onion']

Name

wwwieqvblhnel7wsb6jpxeen3dbmsqyozj2gzl2oyn6swrkq27jtusqd.onion

Pattern Type

stix

Pattern

[domain-name:value = 'wwwieqvblhnel7wsb6jpxeen3dbmsqyozj2gzl2oyn6swrkq27jtusqd.onion']

Attack-Pattern

Name

Abuse Elevation Control Mechanism

ID

T1548

Description

Adversaries may circumvent mechanisms designed to control elevate privileges to gain higher-level permissions. Most modern systems contain native elevation control mechanisms that are intended to limit privileges that a user can perform on a machine. Authorization has to be granted to specific users in order to perform tasks that can be considered of higher risk. An adversary can perform several methods to take advantage of built-in control mechanisms in order to escalate privileges on a system.

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)

Name

Inhibit System Recovery

ID

T1490

Description

Adversaries may delete or remove built-in data and turn off services designed to aid in the recovery of a corrupted system to prevent recovery.(Citation: Talos Olympic Destroyer 2018)(Citation: FireEye WannaCry 2017) This may deny access to available backups and recovery options. Operating systems may contain features that can help fix corrupted systems, such as a backup catalog, volume shadow copies, and automatic repair features. Adversaries may disable or delete system recovery features to augment the effects of [Data Destruction](https://attack.mitre.org/techniques/T1485) and [Data Encrypted for Impact](https://attack.mitre.org/techniques/T1486).(Citation: Talos Olympic Destroyer 2018)(Citation: FireEye WannaCry 2017) Furthermore, adversaries may disable recovery notifications, then corrupt backups.(Citation: disable_notif_synology_ransom) A number of native Windows utilities have been used by adversaries to disable or delete system recovery features: * `vssadmin.exe` can be used to delete all volume shadow copies on a system - `vssadmin.exe delete shadows /all /quiet` * [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047) can be used to delete volume shadow copies - `wmic shadowcopy delete` * `wbadmin.exe` can be used to delete the Windows Backup Catalog - `wbadmin.exe delete catalog -quiet` * `bcdedit.exe` can be used to disable automatic Windows recovery features by modifying boot configuration data - `bcdedit.exe /set {default} bootstatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no` * `REAgentC.exe` can be used to disable Windows Recovery Environment (WinRE) repair/recovery options of an infected system On network devices, adversaries may leverage [Disk Wipe](https://attack.mitre.org/techniques/T1561) to delete backup firmware images and reformat the file system, then [System Shutdown/Reboot](https://attack.mitre.org/techniques/T1529) to reload the device. Together this activity may leave network devices completely inoperable and inhibit recovery operations. Adversaries may also delete “online” backups that are connected to their network – whether via network storage media or through folders that sync to cloud services.(Citation: ZDNet Ransomware Backups 2020) In cloud environments, adversaries may disable versioning and backup policies and delete snapshots, machine images, and prior versions of objects designed to be used in disaster recovery scenarios.(Citation: Dark Reading Code Spaces Cyber Attack)(Citation: Rhino Security Labs AWS S3 Ransomware)

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)

Domain-Name

Value
cloak7jpvcb73rtx2ff7kaw2kholu7bdiivxpzbhlny4ybz75dpxckqd.onion
47h4pwve4scndaneljfnxdhzoulgsyfzbgayyonbwztfz74gsdprz5qd.onion
dcpuyivlbzx56hqwsvey33bxobxw3timjgljjy3index6qvdls5bjoad.onion
wwwieqvblhnel7wsb6jpxeen3dbmsqyozj2gzl2oyn6swrkq27jtusqd.onion
zxzs677rphmjznqgqzlsmjtqwqlydq47rwjesrt4dkkh6cc2ftlfhuqd.onion

External References

- https://otx.alienvault.com/pulse/64ef6e79f617dd47a15b55a8
- https://www.sentinelone.com/blog/threat-actor-interplay-good-days-victim-portals-and-their-ties-to-cloak/