

Table of contents

Overview

● Description	4
● Confidence	4
● Content	5

Entities

● Attack-Pattern	6
● Indicator	10
● Intrusion-Set	12
● Malware	13

Observables

● StixFile	14
------------	----



External References

-
- External References

15

Overview

Description

On January 20th the Cactus ransomware group attacked a number of victims across varying industries. The attacks were disclosed on their leak site with the accompanying victim data. The ransomware group has routinely put pressure on victims by releasing personal information about employees of the victim organization; this has included drivers licenses, passports, pictures and other personal identification.

Confidence

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

15 / 100

Content

N/A

Attack-Pattern

Name

Scheduled Task/Job

ID

T1053

Description

Adversaries may abuse task scheduling functionality to facilitate initial or recurring execution of malicious code. Utilities exist within all major operating systems to schedule programs or scripts to be executed at a specified date and time. A task can also be scheduled on a remote system, provided the proper authentication is met (ex: RPC and file and printer sharing in Windows environments). Scheduling a task on a remote system typically may require being a member of an admin or otherwise privileged group on the remote system.(Citation: TechNet Task Scheduler Security) Adversaries may use task scheduling to execute programs at system startup or on a scheduled basis for persistence. These mechanisms can also be abused to run a process under the context of a specified account (such as one with elevated permissions/privileges). Similar to [System Binary Proxy Execution](<https://attack.mitre.org/techniques/T1218>), adversaries have also abused task scheduling to potentially mask one-time execution under a trusted system process. (Citation: ProofPoint Serpent)

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 Manipulation

ID

T1565

Description

Adversaries may insert, delete, or manipulate data in order to influence external outcomes or hide activity, thus threatening the integrity of the data. By manipulating data, adversaries may attempt to affect a business process, organizational understanding, or decision making. The type of modification and the impact it will have depends on the target application and process as well as the goals and objectives of the adversary. For complex systems, an adversary would likely need special expertise and possibly access to specialized software related to the system that would typically be gained through a prolonged information gathering campaign in order to have the desired impact.

Name

Create or Modify System Process

ID

T1543

Description

Adversaries may create or modify system-level processes to repeatedly execute malicious payloads as part of persistence. When operating systems boot up, they can start processes that perform background system functions. On Windows and Linux, these system processes are referred to as services.(Citation: TechNet Services) On macOS, launchd processes known as [Launch Daemon](<https://attack.mitre.org/techniques/T1543/004>) and [Launch Agent](<https://attack.mitre.org/techniques/T1543/001>) are run to finish system initialization and load user specific parameters.(Citation: AppleDocs Launch Agent Daemons) Adversaries may install new services, daemons, or agents that can be configured to execute at startup or a repeatable interval in order to establish persistence. Similarly, adversaries may modify existing services, daemons, or agents to achieve the same effect. Services, daemons, or agents may be created with administrator privileges but executed under root/SYSTEM privileges. Adversaries may leverage this functionality to create or modify system processes in order to escalate privileges.(Citation: OSX Malware Detection)

Name

File and Directory Discovery

ID

T1083

Description

Adversaries may enumerate files and directories or may search in specific locations of a host or network share for certain information within a file system. Adversaries may use the information from [File and Directory Discovery](<https://attack.mitre.org/techniques/T1083>) during automated discovery to shape follow-on behaviors, including whether or not the adversary fully infects the target and/or attempts specific actions. Many command shell utilities can be used to obtain this information. Examples include ``dir``, ``tree``, ``ls``, ``find``, and ``locate``.(Citation: Windows Commands JPCERT) Custom tools may also be used to gather file and directory information and interact with the [Native API](<https://attack.mitre.org/techniques/T1106>). Adversaries may also leverage a [Network Device CLI](<https://attack.mitre.org/techniques/T1059/008>) on network devices to gather file and directory information (e.g. ``dir``, ``show flash``, and/or ``nvram``). (Citation: US-CERT-TA18-106A)

Name

T1022

ID

T1022

Indicator

Name

9ec6d3bc07743d96b723174379620dd56c167c58a1e04dbfb7a392319647441a

Pattern Type

stix

Pattern

```
[file:hashes:'SHA-256' =  
'9ec6d3bc07743d96b723174379620dd56c167c58a1e04dbfb7a392319647441a']
```

Name

CactusRansomware

Description

CactusRansomware rule to detect Cactus Ransomware

Pattern Type

yara

Pattern

```
/* MIT License Copyright 2023 ShadowStackRe.com Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions: The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE. */ rule CactusRansomware { meta: description = "rule to detect Cactus Ransomware" author = "ShadowStackRe.com" date = "2024-01-18" Rule_Version = "v1" malware_type = "ransomware" malware_family = "Cactus" License = "MIT License, https://opensource.org/license/mit/" Hash = "9ec6d3bc07743d96b723174379620dd56c167c58a1e04dbfb7a392319647441a,c49b4faa6ac7b5c207410ed1e86d0f21c00f47a78c531a0a736266c436cc1c0a" strings: $strReadMe = "cAcTuS.readme.txt" wide $strLockExt = ".cts" wide $strTskName = "Updates Check Task" wide $strTskName2 = "Google Service Update" $strNTUSer = "ntuser.dat" wide $strNTUSer2 = "ntuser.log" wide $strBuilderName = "cactusbuilder" condition: uint16(0) == 0x5A4D and ($strReadMe and $strLockExt) and (1 of ($strTskName*)) and (1 of ($strNTUSer*)) or ($strBuilderName) }
```

Name

c49b4faa6ac7b5c207410ed1e86d0f21c00f47a78c531a0a736266c436cc1c0a

Pattern Type

stix

Pattern

```
[file:hashes:'SHA-256' = 'c49b4faa6ac7b5c207410ed1e86d0f21c00f47a78c531a0a736266c436cc1c0a']
```

Intrusion-Set

Name

Cactus

Malware

Name

Cactus

StixFile

Value

c49b4faa6ac7b5c207410ed1e86d0f21c00f47a78c531a0a736266c436cc1c0a

9ec6d3bc07743d96b723174379620dd56c167c58a1e04dbfb7a392319647441a

External References

-
- <https://otx.alienvault.com/pulse/65b14ba5f8a32510362fc172>
-
- <https://www.shadowstackre.com/analysis/cactus>