Threat Category: Malware, Destructive Malware

Threat Description: The YARA rule is designed to detect suspicious malware that utilizes ElRawDisk. This rule is specifically crafted to identify malware associated with destructive attacks, such as the DUSTMAN campaign.

The rule focuses on identifying executable files that meet the following criteria:

The file must be a valid Portable Executable (PE) file, indicated by the MZ header (0x5A4D).

The file size must be less than or equal to 2000KB.

The file must contain either one of the following ASCII strings:

"\drv\agent.plain.pdb"

" * ********** Down With Saudi Kingdom, Down With Bin Salman ********** "

Or the file must contain four of the following strings:

".?AVERDError@@" (fullword ascii)

"b4b615c28ccd059cf8ed1abf1c71fe03c0354522990af63adf3c911e2287a4b906d47d" (fullword wide)

"\\?\ElRawDisk" (fullword wide)

"\??\c:" (wide)

And optionally, it can also contain any of the following byte sequences:

e9 3d ff ff ff 33 c0 48 89 05 0d ff 00 00 48 8b

0f b6 0c 01 88 48 34 48 8b 8d a8

Indicators of Compromise (IoCs):

MZ Header: 0x5A4D

File size: <= 2000KB

Specific strings: (See Threat Description)

Specific byte sequences: (See Threat Description)

MD5 Hash: 44100c73c6e2529c591a10cd3668691d92dc0241152ec82a72c6e63da299d3a2

Possible Attribution & Use Cases:

This rule detects malware using ElRawDisk, a tool that can be used for direct disk access, often employed in destructive attacks.

The rule is specifically referenced in connection with the Saudi National Cybersecurity Authority report on the DUSTMAN destructive attack.

Detection of this malware indicates a high risk of data destruction or system compromise.

Recommended Actions:

Immediate Response: If this rule is triggered, initiate immediate incident response procedures due to the destructive potential of the detected malware.

Isolation: Isolate the affected system to prevent further spread of the malware.

Forensic Analysis: Perform a thorough forensic analysis to determine the extent of the damage and identify the attack vector.

Recovery: Implement recovery procedures to restore affected systems and data from clean backups.

Prevention: Strengthen security measures to prevent similar attacks, including restricting access to raw disk devices and implementing robust endpoint detection and response solutions.

Intelligence Sharing: Share details of the incident with relevant cybersecurity authorities and communities.

Author & Attribution:

Rule Author: Florian Roth (Nextron Systems)

Rule Reference: Saudi National Cybersecurity Authority - Destructive Attack DUSTMAN

Rule Date: 2020-01-02, Modified: 2022-12-21

Rule Identifier: 0efaae51-1407-5039-9e5a-9c2f13d6a971