Threat Category: APT, KE3CHANG Group, Backdoor

Threat Description: The YARA rule is designed to detect strings left in temporary files created by the KE3CHANG group's Ketrican backdoor. This rule specifically targets artifacts left within TMP files, which are indicative of the Ketrican backdoor's activity.

Indicators of Compromise (IoCs):

hash1 = "4ef11e84d5203c0c425d1a76d4bf579883d40577c2e781cdccc2cc4c8a8d346f"

strings:

$pps1 = "PSParentPath: Microsoft.PowerShell.Core\\Registry::HKEY_CURRENT_USE" fullword ascii

$pps2 = "PSPath: Microsoft.PowerShell.Core\\Registry::HKEY_CURRENT_USE" fullword ascii

$psp1 = ": Microsoft.PowerShell.Core\\Registry" ascii

$s4 = "PSChildName : PhishingFilter" fullword ascii

$s1 = "DisableFirstRunCustomize : 2" fullword ascii

$s7 = "PSChildName : 3" fullword ascii

$s8 = "2500 : 3" fullword ascii

Detection Mechanism:

This rule identifies suspicious TMP files using the following conditions:

The file must start with the signature 0x5350.

The file size must be less than 1KB.

The file must contain the string ": Microsoft.PowerShell.Core\Registry".

The file must contain at least one of the PowerShell Registry Path strings.

The file must contain at least one of the specific strings.

Possible Attribution & Use Cases:

The presence of these specific strings in TMP files is indicative of activity associated with the KE3CHANG group and their Ketrican backdoor.

KE3CHANG group is known for targeting various sectors for espionage.

This detection can be used to identify potential infections and investigate compromised systems.

Recommended Actions:

Monitor and Investigate: Examine TMP files on systems for the presence of these indicators. Investigate processes creating these files.

Containment & Mitigation: Remove identified malicious TMP files and investigate the source of the infection.

Threat Hunting & Intelligence Sharing: Implement this rule to proactively hunt for Ketrican backdoor activity. Share findings with the security community.

Author & Attribution:

Rule Author: Markus Neis, Swisscom

Rule Date: 2020-06-18

Reference: https://app.any.run/tasks/a96f4f9d-c27d-490b-b5d3-e3be0a1c93e9/

Hash: 4ef11e84d5203c0c425d1a76d4bf579883d40577c2e781cdccc2cc4c8a8d346f

Rule ID: 84d411af-ea3d-5862-8c2f-7caca60c1b66