Threat Category: Malware, CloudDuke

Threat Description: The YARA rule rule5_h is designed to detect CloudDuke malware. This rule identifies specific strings and opcode patterns associated with CloudDuke samples.

The detection mechanism focuses on identifying 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 720KB.

The file must contain at least four of the following strings:

"ProcDataWrap" (fullword ascii)

"imagehlp.dll" (fullword ascii)

"dnlibsh" (fullword ascii)

"%ws_out%ws" (fullword wide)

"Akernel32.dll" (fullword wide)

The file must contain one of the following opcode sequences:

0f b6 80 68 0e 41 00 0b c8 c1 e1 08 0f b6 c2 8b

8b ce e8 f8 01 00 00 85 c0 74 41 83 7d f8 00 0f

e8 2f a2 ff ff 83 20 00 83 c8 ff 5f 5e 5d c3 55

Indicators of Compromise (IoCs):

MZ Header: 0x5A4D

File size: < 720KB

Specific strings:

$s1 = "ProcDataWrap" fullword ascii

$s2 = "imagehlp.dll" fullword ascii

$s3 = "dnlibsh" fullword ascii

$s4 = "%ws_out%ws" fullword wide

$s5 = "Akernel32.dll" fullword wide

Specific opcode sequences:

$op0 = { 0f b6 80 68 0e 41 00 0b c8 c1 e1 08 0f b6 c2 8b }

$op1 = { 8b ce e8 f8 01 00 00 85 c0 74 41 83 7d f8 00 0f }

$op2 = { e8 2f a2 ff ff 83 20 00 83 c8 ff 5f 5e 5d c3 55 }

Hashes:

97d8725e39d263ed21856477ed09738755134b5c0d0b9ae86ebb1cdd4cdc18b7

88a40d5b679bccf9641009514b3d18b09e68b609ffaf414574a6eca6536e8b8f

1d4ac97d43fab1d464017abb5d57a6b4601f99eaa93b01443427ef25ae5127f7

ed7abf93963395ce9c9cba83a864acb4ed5b6e57fd9a6153f0248b8ccc4fdb46

ee5eb9d57c3611e91a27bb1fc2d0aaa6bbfa6c69ab16e65e7123c7c49d46f145

a713982d04d2048a575912a5fc37c93091619becd5b21e96f049890435940004

56ac764b81eb216ebed5a5ad38e703805ba3e1ca7d63501ba60a1fb52c7ebb6e

Possible Attribution & Use Cases:

The rule is designed to detect CloudDuke malware.

CloudDuke is known for cyber espionage activities.

Detection of this malware can indicate potential targeting by the CloudDuke group.

Recommended Actions:

Investigation: If this rule is triggered, investigate the affected system for signs of compromise and further CloudDuke activity.

Containment: Isolate affected systems to prevent lateral movement.

Remediation: Remove the identified malware and any related malicious artifacts.

Enhanced Monitoring: Implement enhanced monitoring and logging to detect potential follow-on activity.

Intelligence Sharing: Share information about the CloudDuke activity with relevant security communities.

Author & Attribution:

Rule Author: Florian Roth (Nextron Systems)

Rule Reference: https://www.f-secure.com/weblog/archives/00002822.html

Rule Date: 2015-07-22

Rule Identifier: 902ef68b-7ed1-5622-b796-4e3bb2388124