

Malcat

Renaud Tabary (www.malcat.fr)

OSSIR - 8 Octobre 2024





1 Malcat

- Présentation
- Aperçu rapide
- Points forts



Figure: Pourquoi Malcat ?



- Analyste SOC
 - **Triage**
 - Création de règles de détection
- Antivirus
 - RE léger
 - **Triage**
- Réponse à incident
 - **Triage**
 - Carving
- Ingénierie inverse
 - Analyse de **données**
 - Identification de patterns



- Début du developement: depuis 2020
- Commercialisation: depuis 2022
- Environ 200 utilisateurs journaliers:
 - Antivirus
 - SOCs
 - CERTs (nationaux / externes / internes)
 - Labs
 - Formation
 - etc.



1 Malcat

- Présentation
- Aperçu rapide
- Points forts

SUMMARY & ANOMALIES

10101

The screenshot displays the Malcat Professional interface for analyzing a PE file. The main window is titled "4539a7a77cc8afd531a6164e27afde755326a8061c6c23d7d81c88147a0b61".

File Analysis View: Shows a tree view of the file's internal structure, including sections like .text (48.0 KB), .rdata (12.0 KB), and .data (09 + 0 + 0). The left sidebar shows a search result for "code (703)" with various sub-sections.

Metadata: Provides details about the file's origin and version. Key information includes:

- Company Name: Microsoft Corporation
- Product Name: Messenger
- Version: 4.7.3001
- Internal Name: #msggr
- Product Version: Version 4.7.3001

Yara Signatures: Displays three categories of signatures:

- Suspicious:** Includes a signature for "tampering" (ChangeRouterPreference).
- Odd:** Includes signatures for "network" (CustomUserAgent), "fingerprint" (FingerprintEnvironment), "lateral movement" (ElevatePrivileges, RunShell).
- Other:** Includes a "coaplier" signature with sub-signatures like MSVC_6_linker, MSVC_6_rich, MSVC (msvc_uv_55), and MSVC (msvc_60_07).

Anomalies: Lists detected anomalies such as "xorInLoop(2)", "StackArrayInitialisationX86", "ManyUniqueImmediateBytes(2)", and "SequentialFunction".

Legend: Provides a key for symbols used in the anomalies list: R (Register), M (Memory), RM (Register/Memory), RX (Register/Execute), and RMX (Register/Memory/Execute).

Bottom Bar: Shows the current file path "0x004139e0 (<Resources.ICO.7.zh-cn.Data>)", architecture "PE", and CPU architecture "x86".

Figure: Summary view with anomalies

HEXA & STRUCTURES



The screenshot displays the Malcat Professional interface. The main window shows a hexadecimal view of a file named 'vbpcode'. The left sidebar shows a file tree with folders like 'data (65 + 0 + 0)', 'BoundPortTable', 'VBForm0', and 'VBObjForm1'. The main area shows hex data with corresponding ASCII characters. The right sidebar shows a disassembly view with instructions like 'Jmp', 'Mov', and 'Call'.

Figure: Hexadecimal view

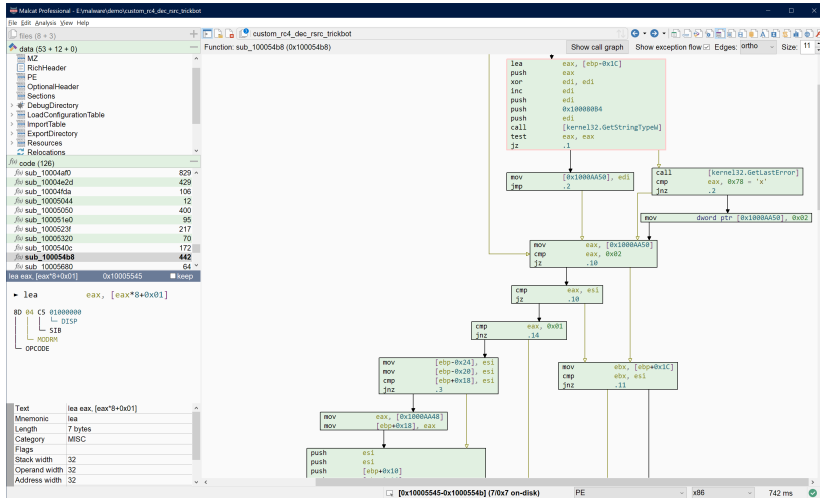
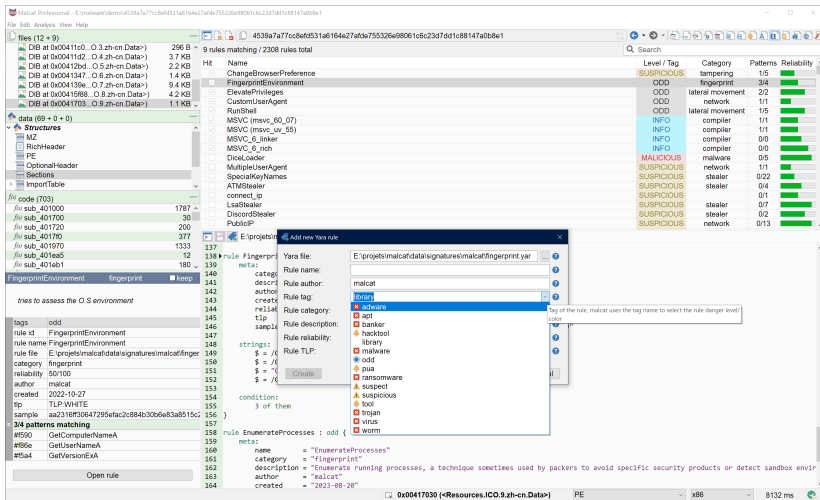


Figure: Desassembleur



Malcat Professional - E:\malware\demo\4539a7a77cc8bf4531a6164427af4e755326e98061c623d7dd1c88147a1b8e1

File Edit Analysis View Help

4539a7a77cc8bf4531a6164427af4e755326e98061c623d7dd1c88147a1b8e1

9 rules matching / 2308 rules total

HR	Name	Level / Tag	Category	Patterns	Reliability
	ChangeBrowserPreference	SUSPICIOUS	tampering	1/5	████████
	FingerprintEnvironment	ODD	fingerprint	3/4	██████
	ElevatePrivileges	ODD	lateral movement	2/2	██████
	CustomUserAgent	ODD	network	1/1	██████
	RunShell	ODD	lateral movement	1/5	██████
	MSVC (msvc_60_07)	INFO	compiler	1/1	██████
	MSVC (msvc_uv_55)	INFO	compiler	1/1	██████
	MSVC_6_linker	INFO	compiler	0/0	██████
	MSVC_6_rich	INFO	compiler	0/0	██████
	Dicel.loader	MALICIOUS	malware	0/5	██████
	MultipleUserAgent	SUSPICIOUS	network	1/1	██████
	SpecialKeyNames	SUSPICIOUS	stealer	0/22	██████
	ATMSStealer	SUSPICIOUS	stealer	0/4	██████
	connect_ip	SUSPICIOUS	stealer	0/1	██████
	LsaStealer	SUSPICIOUS	stealer	0/7	██████
	DiscordStealer	SUSPICIOUS	stealer	0/2	██████
	PublicIP	SUSPICIOUS	network	0/13	██████

Yara file: E:\projects\malcat\data\signatures\malcat\fingerprint.yar

Rule name: malcat

Rule author: malcat

Rule tag: library

Rule category: adware

Rule description: apt, banker, backtool, library, malware, odd, pua, ransomware, suspect, suspicious, tool, trojan, virus, worm

Rule reliability: 1/5

Rule TLP: \$ = /C/ \$ = /C/ \$ = /C/ \$ = /C/

condition: 3 of then

rule EnumerateProcesses : odd {
 meta:
 name = "EnumerateProcesses"
 category = "fingerprint"
 description = "Enumerate running processes, a technique sometimes used by packers to avoid specific security products or detect sandbox enviro"
 author = "malcat"
 created = "2023-08-28"

Figure: Yara editor

Malcat Professional - E:\malcat\demo\pnd\VERSUS E:\malcat\demo\panda_2_2_5_dump

File Edit Analysis View Help

File: panda_2_2_5_dump -- pnd

Address	Field	Value	Field	Value
header: #00000016:	InitialCS:	0x0	header: #00000016:	InitialCS:
header: #00000018:	RelocPosition:	0x40	header: #00000018:	RelocPosition:
header: #0000001a:	OverlayNumber:	0x0	header: #0000001a:	OverlayNumber:
header: #0000001c:	Reserved:	0x0	header: #0000001c:	Reserved:
header: #00000024:	OEMId:	0x0	header: #00000024:	OEMId:
header: #00000026:	OEMInfos:	0x0	header: #00000026:	OEMInfos:
header: #00000028:	Reserved2:	0x0	header: #00000028:	Reserved2:
header: #00000038:	AddressOfPE:	0x40	header: #00000038:	AddressOfPE:
header: #0000003c:	PE:		header: #0000003c:	PE:
header: #00000040:	Signature:	"PE\x00\x00"	header: #00000040:	Signature:
header: #00000044:	Machine:	IMAGE_FILE_MACHINE_I386 (0x14)	header: #00000044:	Machine:
header: #00000046:	NumberOfSections:	0x4	header: #00000046:	NumberOfSections:
header: #00000048:	TimeDateStamp:	Tue Jun 28 21:44:49 2016 (0x5)	header: #00000048:	TimeDateStamp:
header: #0000004c:	PointerToSymbolTable:	0x0	header: #0000004c:	PointerToSymbolTable:
header: #00000050:	NumberOfSymbols:	0x0	header: #00000050:	NumberOfSymbols:
header: #00000054:	SizeOfOptionalHeader:	0xe0	header: #00000054:	SizeOfOptionalHeader:
header: #00000056:	Characteristics:	32bitsMachine(100) + Executab	header: #00000056:	Characteristics:
header: #00000058:	OptionsHeader:	PE32 (0x10b)	header: #00000058:	OptionsHeader:
header: #0000005a:	MajorLinkerVersion:	0x0	header: #0000005a:	MajorLinkerVersion:
header: #0000005b:	MinorLinkerVersion:	0x0	header: #0000005b:	MinorLinkerVersion:
header: #0000005c:	SizeOfCode:	0x0	header: #0000005c:	SizeOfCode:
header: #0000005d:	SizeOfInitializedData:	0x0	header: #0000005d:	SizeOfInitializedData:
header: #00000064:	SizeOfUninitializedData:	0x0	header: #00000064:	SizeOfUninitializedData:
header: #00000068:	AddressOfEntryPoint:	0x0c98e	header: #00000068:	AddressOfEntryPoint:
header: #0000006c:	BaseOfCode:	0x0	header: #0000006c:	BaseOfCode:
header: #00000070:	BaseOfData:	0x0	header: #00000070:	BaseOfData:
header: #00000074:	ImageBase:	0x400000	header: #00000074:	ImageBase:
header: #00000078:	SectionAlignment:	0x1000	header: #00000078:	SectionAlignment:
header: #0000007c:	FileAlignment:	0x200	header: #0000007c:	FileAlignment:
header: #00000080:	MajorOperatingSystemVersion:	0x5	header: #00000080:	MajorOperatingSystemVersion:
header: #00000082:	MinorOperatingSystemVersion:	0x1	header: #00000082:	MinorOperatingSystemVersion:
header: #00000084:	MajorImageVersion:	0x0	header: #00000084:	MajorImageVersion:
header: #00000086:	MinorImageVersion:	0x0	header: #00000086:	MinorImageVersion:
header: #00000088:	MajorSubsystemVersion:	0x5	header: #00000088:	MajorSubsystemVersion:
header: #0000008a:	MinorSubsystemVersion:	0x1	header: #0000008a:	MinorSubsystemVersion:
header: #0000008c:	Win32VersionValue:	0x0	header: #0000008c:	Win32VersionValue:
header: #00000090:	SizeOfImage:	0x21000	header: #00000090:	SizeOfImage:
header: #00000094:	SizeOfHeaders:	0x200	header: #00000094:	SizeOfHeaders:
header: #00000098:	Checksum:	0x0	header: #00000098:	Checksum:
header: #0000009c:	Subsystem:	IMAGE_SUBSYSTEM_WINDOWS_GUI	header: #0000009c:	Subsystem:
header: #0000009e:	DllCharacteristics:	TerminalServerAware(800) + k	header: #0000009e:	DllCharacteristics:
header: #000000a0:	SizeOfStackReserve:	0x100000	header: #000000a0:	SizeOfStackReserve:
header: #000000a4:	SizeOfStackCommit:	0x10000	header: #000000a4:	SizeOfStackCommit:
header: #000000a8:	SizeOfHeapReserve:	0x100000	header: #000000a8:	SizeOfHeapReserve:
header: #000000ac:	SizeOfHeapCommit:	0x10000	header: #000000ac:	SizeOfHeapCommit:
header: #000000b0:	LoaderFlags:	0x0	header: #000000b0:	LoaderFlags:
header: #000000b4:	NumberOfRvaAndSizes:	0x10	header: #000000b4:	NumberOfRvaAndSizes:

RichHeader:

- Signature: 0x536e5144
- Padding: 4(4c+4c+4c)
- ToolList:

 - ToolList[0]:
 - Version: 0x7809
 - Tool: C (0x03)
 - ToolList[1]:
 - Version: 0x7809
 - Tool: ImpLib (0x03)
 - ToolList[2]:
 - Version: 0x0
 - Tool: Import (0x1)
 - ToolList[3]:
 - Version: 0x20fc
 - Tool: Mass (0x12)
 - ToolList[4]:
 - Version: 0x9eb5
 - Tool: LTC_CPP (0x05)
 - ToolList[5]:
 - Version: 0x9eb5
 - Tool: Linker (0x0e)

Rich: "Rich"

XorKey: 0x88d828c1

PE:

- Signature: "PE\x00\x00"
- Machine: IMAGE_FILE_MACHINE_I386 (0x14)
- NumberOfSections: 0x4
- TimeDateStamp: Tue Oct 25 18:54:46 2016 (0x5)
- PointerToSymbolTable: 0x0
- NumberOfSymbols: 0x0
- SizeOfOptionalHeader: 0xe0

size of optional header #16 (-MZ+16) PE x86 4 ms

Figure: Binary diffing

TRANSFORMS



Malcat Professional - E:\malware\demos\js_cobalt (MODIFIED)

File Edit Analysis View Help

js_cobalt

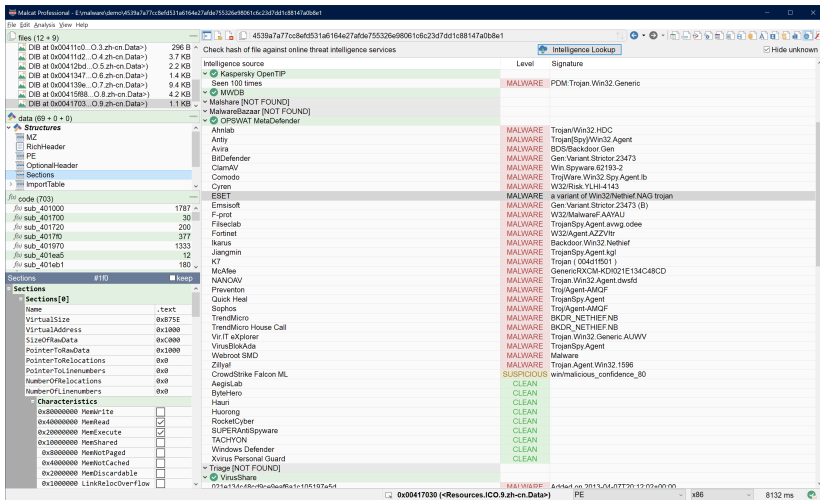
Transforms chain New template Preview Auto preview

- lzma decompress
 - raw_mode:
 - lzma2:
 - max_length: -0x1 (decimal | hexa)
- aes decrypt
 - mode: ecb
 - key: 'Whitelat5myneig'
 - iv: '00000000000000000000000000000000'
 - unpad:
- xor8
 - key: 'FBDD89CE'

Output size: 307168 bytes

```
00 00 00 48 80 1D EA FF FF FF FF 48 89 DF 48 81 C3 ] C
D4 88 01 00 FF 03 41 88 F0 B5 A2 56 68 04 00 00
00 5A 48 89 F9 FF D0 00 00 00 00 00 00 00 00
00 81 00 00 0E F1 BA 9E 00 84 00 CD 21 B8 91 4C
CD 21 54 68 69 73 87 20 70 72 6F 67 72 61 D0 28 63
61 6E 6E 6F 74 20 62 65 28 72 75 6E 20 69 6E 28
44 4F 53 20 60 6F 64 65 2E 00 00 0A 24 00 00 00
00 00 00 85 A6 2D 1C C1 C7 43 4F C1 C7 43 4F
C1 C7 43 4F A7 29 89 4F C0 C7 43 4F E2 28 91 4F
59 C7 43 4F 5F 87 94 4F C0 C7 43 4F 00 81 8C 4F
EB C7 43 4F 30 81 80 4F 48 C7 43 4F 30 81 8E 4F
CB C7 43 4F CB 8F 00 4F CA C7 43 4F C1 C7 42 4F
16 C7 43 4F E2 28 80 4F FB C7 43 4F A7 29 8E 4F
CB C7 43 4F A7 29 89 4F C0 C7 43 4F A7 29 8F 4F
C0 C7 43 4F 52 69 63 68 C1 C7 43 4F 00 00 00 00
00 00 00 50 45 00 00 64 86 95 00 7F 8C F8 64
00 00 00 00 00 00 F0 00 22 A0 08 02 00 00
00 02 03 00 4E 02 00 00 00 00 48 18 02 00
```

Figure: Transforms



The screenshot displays the Malcat Professional interface. The main pane shows a file named `4539a7a77cc8efcd531a6164e27af9c755326e80616c23d7dd1c88147ab8e1` with a size of 296 B. The file is analyzed against online threat intelligence services. The Intelligence Lookup table on the right provides a detailed view of the findings.

Intelligence source	Level	Signature
Seen 100 times	MALWARE	PDM.Trojan.Win32.Generic
Malshare [NOT FOUND]		
MalwareBazaar [NOT FOUND]		
OPSWAT MetaDefender		
Ahlab	MALWARE	Trojan/Win32_HDC
Antiy	MALWARE	Trojan/Spy/Win32.Agent
Avira	MALWARE	BDS/Backdoor.Gen
BitDefender	MALWARE	Gen.Variant.Strictor.23473
ClamAV	MALWARE	Win.Spyware.62.193-2
Comodo	MALWARE	TrojWare.Win32.Spy.Agent.lb
Cyren	MALWARE	W32/Risk.YLH-4143
ESET	MALWARE	a variant of Win32/Nethef.NAG.trojan
Emisoft	MALWARE	Gen.Variant.Strictor.23473 (B)
F-prot	MALWARE	W32/MalwareF.AAYAU
Filseclab	MALWARE	Trojan/Spy.Agent.awwg.odee
Fortinet	MALWARE	W32/Agent.AZZYlr
Ikarus	MALWARE	Backdoor/Win32.Nethef
Jiangmin	MALWARE	Trojan/Spy.Agent.kgl
K7	MALWARE	Trojan (004d1501)
McAfee	MALWARE	GenericRXCX-KD021E134C8CD
NANOV	MALWARE	Trojan/Win32.Agent.dwsfd
Phevention	MALWARE	TrojAgent.40QF
Quick Heal	MALWARE	Trojan/Spy.Agent
Sophos	MALWARE	TrojAgent-AMQF
TrendMicro	MALWARE	BKDR_NETHIEF.NB
TrendMicro House Call	MALWARE	BKDR_NETHIEF.NB
VirIT eXplorer	MALWARE	Trojan/Win32.Generic.AUWV
VirusBlokAda	MALWARE	Trojan/Spy.Agent
Webroot SMD	MALWARE	Malware
Webroot SMD	MALWARE	Trojan.Agent.Win32.1586
Zillya	MALWARE	win/malicious_confidence_80
CrowdStrike Falcon ML	SUSPICIOUS	
Aegislab	CLEAN	
ByteHero	CLEAN	
Huarr	CLEAN	
Huorong	CLEAN	
RocketCyber	CLEAN	
SUPERAntiSpyware	CLEAN	
TACHYON	CLEAN	
Windows Defender	CLEAN	
Xvirus Personal Guard	CLEAN	
Triage [NOT FOUND]		
VirusShare	CLEAN	

Figure: Threat intelligence

The screenshot displays the Malcat Professional interface with two windows open. The left window shows a file analysis of '0f5c3f56d2271570b752304726f744e4d894e7f74302ae'. The right window shows an analysis of '333361510546430426c0eaf'. Both windows feature a table of file entries with columns for Name, Address, User, Danger, Type, and Codec. The entries are color-coded: green for safe files, yellow for suspicious files, and red for dangerous files. The right window also includes a hex dump view on the far right.

Name	Address	User	Danger	Type	Codec	
140 strings found (25474 bytes / 13.27% of file) SCAN META UACSR DYN Search						
eventvwr.exe	0x14002448 (rdta.b3f8)	USER	CLEAN	USER	UHF16	
winlogon.exe	0x14002440 (rdta.b400)	USER	CLEAN	USER	UHF16	
Wolfram.exe	0x14002478 (rdta.b378)	USER	CLEAN	USER	UHF16	
MWEXE.nls	0x14002480 (rdta.b378)	USER	CLEAN	USER	UHF16	
taskhost.exe	0x14002470 (rdta.b370)	USER	CLEAN	USER	UHF16	
explorer.exe	0x14002580 (rdta.b050)	USER	CLEAN	USER	UHF16	
(3AD05F78-8857-4850-9277-118B80B8E069)	0x14002540 (rdta.b120)	UACME	USER	UHF16		
OcsSupport.dll	0x14002478 (rdta.b378)	USER	CLEAN	USER	UHF16	
wiremon.dll	0x14002408 (rdta.b3c8)	USER	CLEAN	USER	UHF16	
explorer.exe	0x14002480 (rdta.b378)	USER	CLEAN	USER	UHF16	
mscorrc.dll	0x140019a8 (rdta.ae8)	USER	CLEAN	USER	UHF16	
Clamp.exe	0x14002560 (rdta.c60)	USER	CLEAN	USER	UHF16	
pcadm.dll	0x14002480 (rdta.b378)	USER	CLEAN	USER	UHF16	
rgen.log	0x14002438 (rdta.b3e8)	USER	CLEAN	USER	UHF16	
(3E5FC7F9-9A51-4367-9063-A120244FBE7)	0x14002430 (rdta.b390)	MediaLocker	USER	UHF16		
(40111E08-CBF7-4112-A926-2C720FA9F2FC)	0x14002470 (rdta.b378)	UACME	USER	UHF16		
system32	0x140009f1 (rsa_1400065d+21)	DYN	USER	UHF16		
wol6log.dll	0x14002420 (rdta.b200)	CLEAN	USER	UHF16		
msconfig.exe	0x14002560 (rdta.c60)	USER	CLEAN	USER	UHF16	
Software/Classes	0x14002480 (rdta.b378)	USER	CLEAN	USER	UHF16	
results.cab	0x14002580 (rdta.c00)	CLEAN	USER	UHF16		
fusion.dll	0x14002428 (rdta.b218)	USER	CLEAN	USER	UHF16	
msd.exe	0x14002528 (rdta.c16)	USER	CLEAN	USER	UHF16	
mscorrc.dll	0x14002528 (rdta.c16)	UACME	USER	UHF16		
sdclt.exe	0x14002510 (rdta.c150)	CLEAN	USER	UHF16		
sk.exe	0x14002508 (rdta.c138)	CLEAN	USER	UHF16		
shel32.dll	0x14002538 (rdta.c108)	USER	CLEAN	USER	UHF16	
comctl32.dll	0x14002460 (rdta.b3c0)	CLEAN	USER	UHF16		
comctl32.dll	0x14002460 (rdta.b3c0)	CLEAN	USER	UHF16		
comctl32.dll	0x14002480 (rdta.b378)	CLEAN	USER	UHF16		
rdshost.exe	0x14002480 (rdta.b378)	USER	CLEAN	USER	UHF16	
rsd-rsh-win-core-kernel32-legacy+1.DLL	0x14002480 (rdta.b378)	SCAN	USER	UHF16		
GalPas.dll	0x14002510 (rdta.c110)	CLEAN	USER	UHF16		
Software/Classes/CLSID	0x14002508 (rdta.c138)	CLEAN	USER	UHF16		
0x14002560 (rdta.c60)	0x14002560 (rdta.c60)	CLEAN	USER	UHF16		
docx.exe	0x14002488 (rdta.b3f8)	CLEAN	USER	UHF16		
D:\PA\AOC\FAC\WD	0x14002460 (rdta.b3c0)	CLEAN	USER	UHF16		
msc.exe	0x14002488 (rdta.b3f8)	CLEAN	USER	UHF16		
eventvwr.msc	0x14002170 (rdta.b170)	USER	CLEAN	USER	UHF16	
readme.html	0x14002438 (rdta.b3e8)	CLEAN	USER	UHF16		
plgprog.exe	0x14002460 (rdta.b3c0)	CLEAN	USER	UHF16		
Services/Active	0x14002468 (rdta.b3d8)	CLEAN	USER	UHF16		
Accessibility	0x14002448 (rdta.b3d8)	CLEAN	USER	UHF16		
DiagHost.Execls	0x14002438 (rdta.b3e8)	CLEAN	USER	UHF16		
(?)	0x14002450 (rdta.b3d0)	CLEAN	USER	UHF16		
URL_Msc-Window-store	0x14002478 (rdta.b378)	USER	CLEAN	USER	UHF16	
ost.exe	0x14002428 (rdta.b3e8)	CLEAN	USER	UHF16		
update.msu	0x14002568 (rdta.c68)	USER	CLEAN	USER	UHF16	

Figure: Kesakode: coloring



1 Malcat

- Présentation
- Aperçu rapide
- Points forts



- Rapide!
- Plus de 50 formats de fichiers supportés:
 - Programmes, images, archives, FS, documents, Office, etc.
 - Parsers en python
 - Extraction de fichiers / carving
- Multi-architecture:
 - x86/x64, .NET, .PYC, VB p-code
 - Mais aussi: VBA, NSIS VM, InnoScript, macros Excel, tables MSI
 - ...
- Reconnaissances de patterns:
 - Plus de 300 anomalies
 - Support signatures FLIRT
 - Plus de 400k constantes (hash API, crypto, GUIDs, etc.)
 - Kesakode (function/string/constants online lookup)



Moteur d'analyse en C++, décoré de la GUI:

- Bindings en python
- Documentation complète
- Possibilité de lancer des analyse depuis la CLI ou depuis python
- Traitements en batch / multi-threading
- Rapport / templates



Interaction entre les outils:

- Désassembleur / editeur hexa -> Yara
- Transforms -> file carving
- Désassembleur -> script / émulation, Yara
- Késakode -> Strings, Yara, désassembleur
- etc.



- Adapté à tout niveau de compétence
 - Débutant: rapport d'analyse, anomalies, threat intel
 - Intermédiaire: editeur Yara, désassembleur
 - Avancé: scripting, intégration OEM
- Gain de temps pour l'analyste
 - Analyse rapide
 - Beaucoup d'outils en un
 - Support de 99% des types de fichiers "malveillants"
- Gain d'argent pour l'entreprise