ID: 452668
Sample Name:
6LS4xS6TKn.exe
Cookbook: default.jbs
Time: 17:43:18
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report 6LS4xS6TKn.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Agenttesla 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
Jbx Signature Overview 5
AV Detection: 5
Data Obfuscation: 5
Boot Survival: 5
Hooking and other Techniques for Hiding and Protection: 5
Malware Analysis System Evasion: 5
HIPS / PFW / Operating System Protection Evasion: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 6
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 9
Domains and IPs 10
Contacted Domains 10
URLs from Memory and Binaries 10
Contacted IPs 10
General Information 10
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASN 11
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
Static File Info 14
General 14
File Icon 14
Static PE Info 15
General 15
Entrypoint Preview 15
Data Directories 15
Sections 15
Resources 15
Imports 15
Version Infos 15
Network Behavior 15
Code Manipulations 15
Statistics 15
Behavior 15
System Behavior 15
Analysis Process: 6LS4xS6TKn.exe PID: 4260 Parent PID: 5556 16
General 16
File Activities 16
File Created 16
File Deleted 16
File Written 16
File Read 16
Analysis Process: schtasks.exe PID: 4300 Parent PID: 4260 16
General 16
File Activities 16
File Read 16
Analysis Process: conhost.exe PID: 4604 Parent PID: 4300 16
General 16

Analysis Process: 6LS4xS6TKn.exe PID: 6048 Parent PID: 4260 17
General 17
File Activities 17
File Created 17
File Written 17
File Read 17
Registry Activities 17
Key Value Created 17
Analysis Process: MLdAu.exe PID: 6108 Parent PID: 3388 17
General 17
File Activities 18
File Created 18
File Deleted 18
File Written 18
File Read 18
Analysis Process: MLdAu.exe PID: 5432 Parent PID: 3388 18
General 18
File Activities 18
File Created 18
File Read 18
Analysis Process: schtasks.exe PID: 3148 Parent PID: 6108 18
General 18
File Activities 19
File Read 19
Analysis Process: conhost.exe PID: 1328 Parent PID: 3148 19
General 19
Analysis Process: MLdAu.exe PID: 1392 Parent PID: 6108 19
General 19
File Activities 19
File Read 19
Disassembly 19
Code Analysis 19

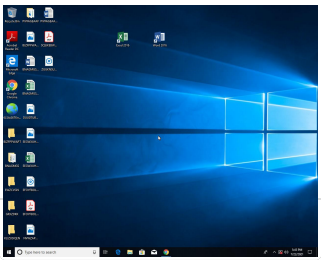
Windows Analysis Report 6LS4xS6TKn.exe

Overview

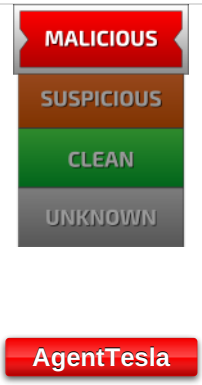
General Information

Sample Name:	6LS4xS6TKn.exe
Analysis ID:	452668
MD5:	118f0e5d6a1c91a.
SHA1:	933d498bf7eea29.
SHA256:	16d0e36df66a1ba.
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection

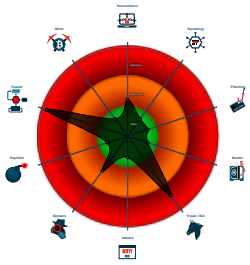


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains potentia…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …

Classification



Process Tree

- **System is w10x64**
- 6LS4xS6TKn.exe (PID: 4260 cmdline: 'C:\Users\user\Desktop\6LS4xS6TKn.exe' MD5: 118F0E5D6A1C91A5B820741669C495D7)
  - schtasks.exe (PID: 4300 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\yuNCTcaeT' /XML 'C:\Users\user\AppData\Local\Temp\tmp74F3.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4604 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - 6LS4xS6TKn.exe (PID: 6048 cmdline: {path} MD5: 118F0E5D6A1C91A5B820741669C495D7)
- MLdAu.exe (PID: 6108 cmdline: 'C:\Users\user\AppData\Roaming\MLdAu\MLdAu.exe' MD5: 118F0E5D6A1C91A5B820741669C495D7)
  - schtasks.exe (PID: 3148 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\yuNCTcaeT' /XML 'C:\Users\user\AppData\Local\Temp\tmpAB9F.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 1328 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - MLdAu.exe (PID: 1392 cmdline: {path} MD5: 118F0E5D6A1C91A5B820741669C495D7)
- MLdAu.exe (PID: 5432 cmdline: 'C:\Users\user\AppData\Roaming\MLdAu\MLdAu.exe' MD5: 118F0E5D6A1C91A5B820741669C495D7)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "account@jiqdyi.com",
  "Password": "Emotion22",
  "Host": "mail.spamora.net"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000001F.00000002.490664959.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
0000001F.00000002.490664959.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000017.00000002.484767094.000000000399B000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000017.00000002.484767094.000000000399B000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.313750267.0000000003FAB000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 5 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.6LS4xS6TKn.exe.406f160.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.6LS4xS6TKn.exe.406f160.2.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
31.2.MLdAu.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
31.2.MLdAu.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
23.2.MLdAu.exe.3a5f160.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 5 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

Yara detected AntiVM3

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

Yara detected AgentTesla

Remote Access Functionality:

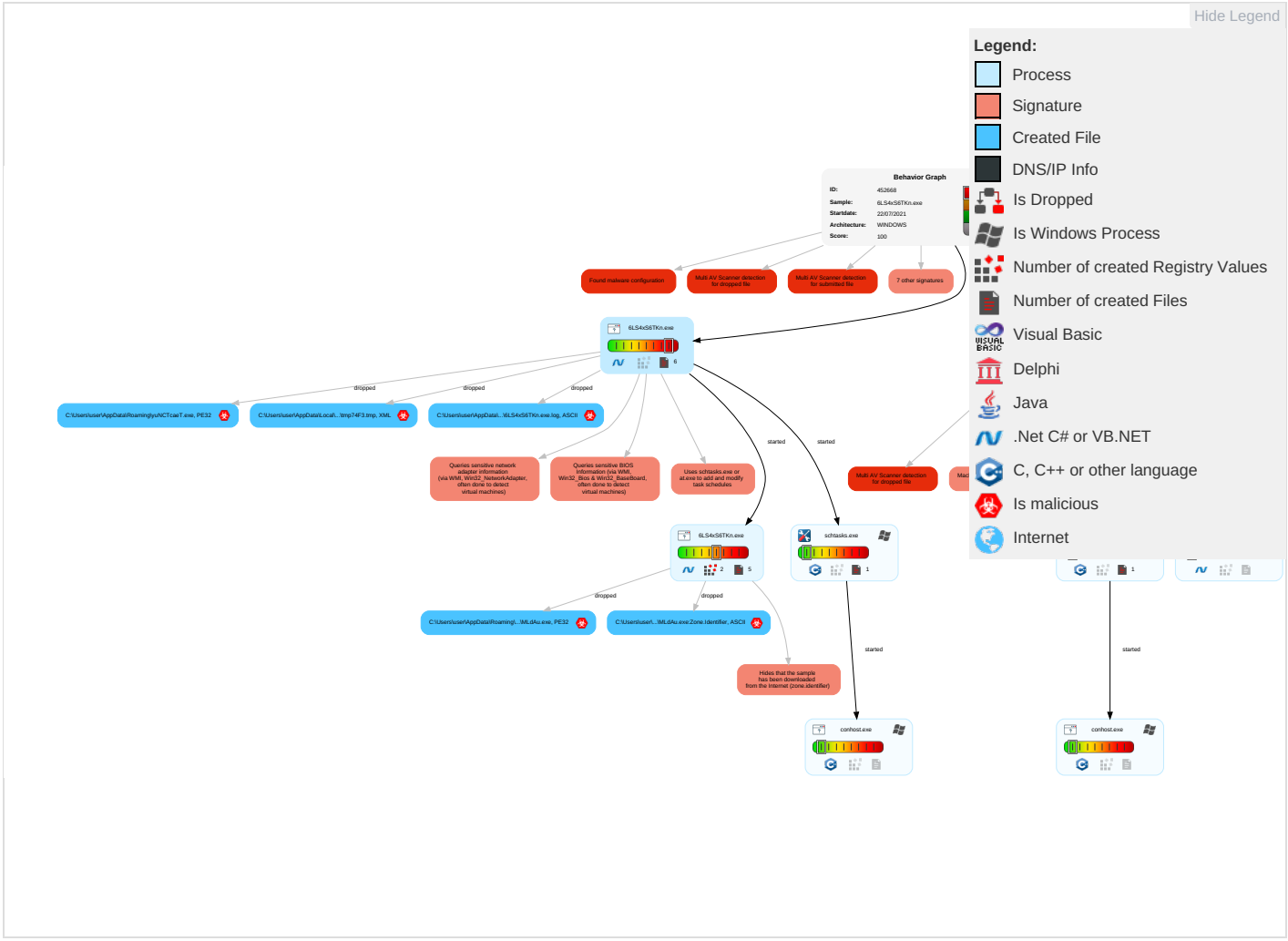
Yara detected AgentTesla

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	N E
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Process Injection 1 1 2	Masquerading 1	Input Capture 1	Security Software Discovery 3 1 1	Remote Services	Input Capture 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	E I N C
Default Accounts	Scheduled Task/Job 1	Registry Run Keys / Startup Folder 1	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Junk Data	E F C
Domain Accounts	At (Linux)	Logon Script (Windows)	Registry Run Keys / Startup Folder 1	Virtualization/Sandbox Evasion 1 3 1	Security Account Manager	Virtualization/Sandbox Evasion 1 3 1	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Steganography	E T L
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Application Window Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	S S
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Hidden Files and Directories 1	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	N D C
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	System Information Discovery 1 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	J D S
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	F A

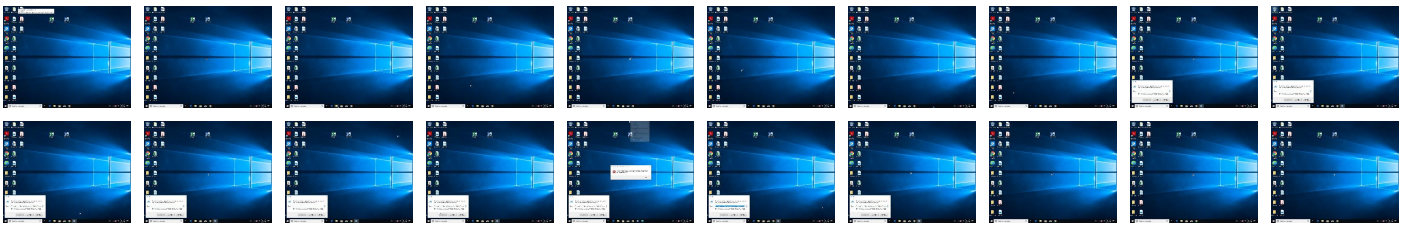
Behavior Graph



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
6LS4xS6TKn.exe	37%	Virustotal		Browse
6LS4xS6TKn.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\yuNCTcaeT.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\MLdAu\MLdAu.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\MLdAu\MLdAu.exe	30%	ReversingLabs	ByteCode-MSIL.Trojan.Heracles	
C:\Users\user\AppData\Roaming\yuNCTcaeT.exe	30%	ReversingLabs	ByteCode-MSIL.Trojan.Heracles	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
31.2.MLdAu.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.founder.com.cn/cner	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Q9	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnze	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/j9	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/ltt	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/j9	0%	Avira URL Cloud	safe	
http://www.carterandcone.coman	0%	Avira URL Cloud	safe	
http://www.carterandcone.comva	0%	URL Reputation	safe	
http://www.carterandcone.comva	0%	URL Reputation	safe	
http://www.carterandcone.comva	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0r	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.fontbureau.comiona	0%	URL Reputation	safe	
http://www.fontbureau.comiona	0%	URL Reputation	safe	
http://www.fontbureau.comiona	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.fontbureau.comFc9	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.fontbureau.comgrita	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://BGwprh.com	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.carterandcone.como.	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htmS	0%	Avira URL Cloud	safe	
http://www.fontbureau.comalsj9	0%	Avira URL Cloud	safe	
http://www.fontbureau.comalsd	0%	URL Reputation	safe	
http://www.fontbureau.comalsd	0%	URL Reputation	safe	
http://www.fontbureau.comalsd	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/29	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/X	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/X	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/X	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.founder.com.cn/cnvan	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0P	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/oi	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/oi	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/oi	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond

Analysis ID:	452668
Start date:	22.07.2021
Start time:	17:43:18
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	6LS4xS6TKn.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	32
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
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@13/7@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 1.4% (good quality ratio 1%) • Quality average: 48.7% • Quality standard deviation: 37.3%
HCA Information:	• Successful, ratio: 96% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
17:45:11	API Interceptor	512x Sleep call for process: 6LS4xS6TKn.exe modified
17:45:25	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run MLdAu C:\Users\user\AppData\Roaming\MLdAu\MLdAu.exe
17:45:33	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run MLdAu C:\Users\user\AppData\Roaming\MLdAu\MLdAu.exe

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\6LS4xS6TKn.exe.log	
Process:	C:\Users\user\Desktop\6LS4xS6TKn.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\MLdAu.exe.log	
Process:	C:\Users\user\AppData\Roaming\MLdAu\MLdAu.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\tmp74F3.tmp	
Process:	C:\Users\user\Desktop\6LS4xS6TKn.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.1850889851927615
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBvBtn:cbh47TlNQ//rydbz9I3YODOLNdq3t
MD5:	71359811BDEC23A8C3EB4B94E71DC270

C:\Users\user\AppData\Local\Temp\tmp74F3.tmp	
SHA1:	05F286BA3C3CCF4BF106BDF8447A94A82AB93A8A
SHA-256:	290E797D6A26CE3C5B18A020D5A21BCF45A723DEC403AC08C9106FF53B4160BA
SHA-512:	09B62C1C6B194F793CE80EB01EE2FC12048CC87C882ED614B0EEAED834FE24E7E604EA4FEE9FA09EC923724163A580D325967488B60F10486037776C93586AA
Malicious:	**true**
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmpAB9F.tmp	
Process:	C:\Users\user\AppData\Roaming\MLdAu\MLdAu.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.1850889851927615
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBvBtn:cbh47TlNQ//rydbz9I3YODOLNdq3t
MD5:	71359811BDEC23A8C3EB4B94E71DC270
SHA1:	05F286BA3C3CCF4BF106BDF8447A94A82AB93A8A
SHA-256:	290E797D6A26CE3C5B18A020D5A21BCF45A723DEC403AC08C9106FF53B4160BA
SHA-512:	09B62C1C6B194F793CE80EB01EE2FC12048CC87C882ED614B0EEAED834FE24E7E604EA4FEE9FA09EC923724163A580D325967488B60F10486037776C93586AA
Malicious:	false
Reputation:	unknown
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\MLdAu\MLdAu.exe	
Process:	C:\Users\user\Desktop\6LS4xS6TKn.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	883200
Entropy (8bit):	7.017055708276543
Encrypted:	false
SSDEEP:	12288:nwRHMJfTDAe9AVLYy6t4XlJIT7652mgkSMPQipP5q:nwRsdT19qMy6tIsnipQ
MD5:	118F0E5D6A1C91A5B820741669C495D7
SHA1:	933D498BF7EEA29D1DEDD4B597692D62C6DC53D4
SHA-256:	16D0E36DF66A1BA451C25A5F5C1FCCCCA5CB415A81CB8820F89811232C4FC3B3
SHA-512:	C9EA9BF3ADB6324A8AD565ED3B7CD14C56AD2370DAE79FE9FF0637E0D8D0291A22363182E72DAEF7C16FA666FCBE3CEC9A9ECF83BAEAFAC23F8DD275AC4BCF38
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 30%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...zk.`.....0..... .....@.. ..... ..@.....S..... ..... ..... ..H.....text..... ..... ..`.rsrc... .....@..@.reloc..... .....x.....@..B.....H.....(.....L,....9....<Iu.<k.....`...v...cU$[so.`z..W9.j... F.g\Pu.B.....,.-.b.....3.?..vt....kU0.!?.n.'...E<v..|G7...B.{.PW..2....OH..w...U.....WCF..*.].../.....4A?...&.4.krV_....~<n.....4.....N.....`.K@....u..?...O....p.-.6...^.....$F.$..d..P.....^O.+..7g.....DWE.....#2.....r.....;L9..M.BL...G~.lxf*..3..' .Xr.S..Q..O.=.:....O...L.ga.....A.j.\m.~..$D....^...s...J.=A44..%@.

C:\Users\user\AppData\Roaming\MLdAu\MLdAu.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\6LS4xS6TKn.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64

C:\Users\user\AppData\Roaming\MLdAu\MLdAu.exe:Zone.Identifier	
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\yuNCTcaeT.exe	
Process:	C:\Users\user\Desktop\6LS4xS6TKn.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	883200
Entropy (8bit):	7.017055708276543
Encrypted:	false
SSDEEP:	12288:nwRHMJfTDAe9AVLYy6t4XlJIT7652mgkSMPQipP5q:nwRsdT19qMy6tIsnipQ
MD5:	118F0E5D6A1C91A5B820741669C495D7
SHA1:	933D498BF7EEA29D1DEDD4B597692D62C6DC53D4
SHA-256:	16D0E36DF66A1BA451C25A5F5C1FCCCCA5CB415A81CB8820F89811232C4FC3B3
SHA-512:	C9EA9BF3ADB6324A8AD565ED3B7CD14C56AD2370DAE79FE9FF0637E0D8D0291A22363182E72DAEF7C16FA666FCBE3CEC9A9ECF83BAEAFAC23F8DD275AC4E CF38
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 30%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...zk.`.....0..... .....@.. ..... ..@.....S..... ..... ..H.....text..... ..... ..`.rsrc... .....@..@.reloc..... .....x.....@..B.....H.....(.....L,....9....<Iu.<k.....`...v...cU$[so.`z..W9.j... F.g\Pu.B.....,-.b.....3.?..vt....kU0.!?.n.'...E< v..|G7...B.{.PW..2....OH..w...U.....WCF..*.].../.....4A?...&.4.krV_....~<n.....4.....N.....`.K@....u..?...O....p.-.6...^.....$F.$..d..P.....^O.+..7g.....DWE.....#2.....r.....;L9..M.BL ...G~.lxf*..3..' .Xr.S..Q..O.=.:....O...L.ga.....A.j.\m.~..$D....^...s...J.=A44..%@.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.017055708276543
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	6LS4xS6TKn.exe
File size:	883200
MD5:	118f0e5d6a1c91a5b820741669c495d7
SHA1:	933d498bf7eea29d1dedd4b597692d62c6dc53d4
SHA256:	16d0e36df66a1ba451c25a5f5c1fcccca5cb415a81cb8820f89811232c4fc3b3
SHA512:	c9ea9bf3adb6324a8ad565ed3b7cd14c56ad2370dae79fe9ff0637e0d8d0291a22363182e72daef7c16fa666fcbe3cec9a9ecf83baeafac23f8dd275ac4ecf38
SSDEEP:	12288:nwRHMJfTDAe9AVLYy6t4XlJIT7652mgkSMPQipP5q:nwRsdT19qMy6tIsnipQ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...zk.`.....0..... .....@.. ..... .@.....

File Icon

Icon Hash:	f0debeffdffeec70

Static PE Info

General

Entrypoint:	0x47affe
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60F96B7A [Thu Jul 22 12:58:34 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x79004	0x79200	False	0.847881998194	data	7.70847292155	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x7c000	0x5e320	0x5e400	False	0.167331523541	data	5.64058505063	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xdc000	0xc	0x200	False	0.041015625	data	0.0815394123432	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 6LS4xS6TKn.exe PID: 4260 Parent PID: 5556

General

Start time:	17:44:11
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\6LS4xS6TKn.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\6LS4xS6TKn.exe'
Imagebase:	0xb80000
File size:	883200 bytes
MD5 hash:	118F0E5D6A1C91A5B820741669C495D7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.313750267.0000000003FAB000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.313750267.0000000003FAB000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 4300 Parent PID: 4260

General

Start time:	17:44:54
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\yuNCTcaeT' /XML 'C:\Users\user\AppData\Local\Temp\tmp74F3.tmp'
Imagebase:	0xab0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 4604 Parent PID: 4300

General

General

Start time:	17:44:54
Start date:	22/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: 6LS4xS6TKn.exe PID: 6048 Parent PID: 4260

General

Start time:	17:44:55
Start date:	22/07/2021
Path:	C:\Users\user\Desktop\6LS4xS6TKn.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x880000
File size:	883200 bytes
MD5 hash:	118F0E5D6A1C91A5B820741669C495D7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: MLdAu.exe PID: 6108 Parent PID: 3388

General

Start time:	17:45:33
Start date:	22/07/2021
Path:	C:\Users\user\AppData\Roaming\MLdAu\MLdAu.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\MLdAu\MLdAu.exe'
Imagebase:	0x4f0000
File size:	883200 bytes
MD5 hash:	118F0E5D6A1C91A5B820741669C495D7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000017.00000002.484767094.000000000399B000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000017.00000002.484767094.000000000399B000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 30%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: MLdAu.exe PID: 5432 Parent PID: 3388

General

Start time:	17:45:46
Start date:	22/07/2021
Path:	C:\Users\user\AppData\Roaming\MLdAu\MLdAu.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\MLdAu\MLdAu.exe'
Imagebase:	0x7a0000
File size:	883200 bytes
MD5 hash:	118F0E5D6A1C91A5B820741669C495D7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Analysis Process: schtasks.exe PID: 3148 Parent PID: 6108

General

Start time:	17:46:13
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\yuNCTcaeT' /XML 'C:\Users\user\AppData\Local\Temp\tmpAB9F.tmp'
Imagebase:	0xab0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities | Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 1328 Parent PID: 3148

General

Start time:	17:46:14
Start date:	22/07/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: MLdAu.exe PID: 1392 Parent PID: 6108

General

Start time:	17:46:15
Start date:	22/07/2021
Path:	C:\Users\user\AppData\Roaming\MLdAu\MLdAu.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x4a0000
File size:	883200 bytes
MD5 hash:	118F0E5D6A1C91A5B820741669C495D7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001F.00000002.490664959.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000001F.00000002.490664959.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000001F.00000002.496038864.00000000029F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000001F.00000002.496038864.00000000029F1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities | Show Windows behavior

File Read

Disassembly

Code Analysis