ID: 532838
Sample Name: Solicitud urgente de Quotaion_U1197,pdf.exe
Cookbook: default.jbs
Time: 18:37:09
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report Solicitud urgente de Quotaion_U1197,pdf.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: FormBook 4
Yara Overview 5
Memory Dumps 5
Unpacked PEs 6
Sigma Overview 7
System Summary: 7
Jbx Signature Overview 7
AV Detection: 7
Networking: 7
E-Banking Fraud: 7
System Summary: 7
Data Obfuscation: 7
Hooking and other Techniques for Hiding and Protection: 7
Malware Analysis System Evasion: 7
HIPS / PFW / Operating System Protection Evasion: 7
Stealing of Sensitive Information: 8
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 10
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 11
Contacted IPs 11
Public 11
General Information 11
Simulations 12
Behavior and APIs 12
Joe Sandbox View / Context 12
IPs 12
Domains 15
ASN 15
JA3 Fingerprints 16
Dropped Files 16
Created / dropped Files 16
Static File Info 17
General 17
File Icon 17
Static PE Info 17
General 17
Entrypoint Preview 17
Data Directories 17
Sections 17
Resources 18
Imports 18
Version Infos 18
Network Behavior 18
Snort IDS Alerts 18
Network Port Distribution 18
TCP Packets 18
UDP Packets 18
DNS Queries 18
DNS Answers 18
HTTP Request Dependency Graph 18
HTTP Packets 19
Code Manipulations 20
User Modules 20

Hook Summary 20
Processes 20
Statistics 20
Behavior 20
System Behavior 20
Analysis Process: Solicitud urgente de Quotaion_U1197,pdf.exe PID: 6204 Parent PID: 5052 20
General 20
File Activities 21
File Created 21
File Written 21
File Read 21
Analysis Process: Solicitud urgente de Quotaion_U1197,pdf.exe PID: 3560 Parent PID: 6204 21
General 21
Analysis Process: Solicitud urgente de Quotaion_U1197,pdf.exe PID: 6120 Parent PID: 6204 21
General 21
File Activities 22
File Read 22
Analysis Process: explorer.exe PID: 3352 Parent PID: 6120 22
General 22
File Activities 23
Analysis Process: msdt.exe PID: 6516 Parent PID: 3352 23
General 23
File Activities 23
File Read 23
Analysis Process: cmd.exe PID: 6960 Parent PID: 6516 24
General 24
File Activities 24
Analysis Process: conhost.exe PID: 6020 Parent PID: 6960 24
General 24
Disassembly 24
Code Analysis 24

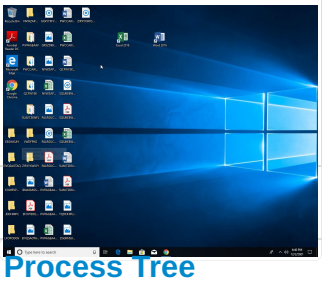
Windows Analysis Report Solicitud urgente de Quotaio…

Overview

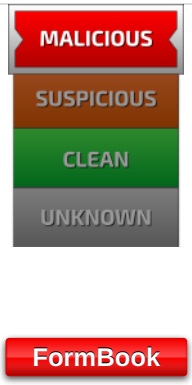
General Information

Sample Name:	Solicitud urgente de Quotaion_U1197,pdf.exe
Analysis ID:	532838
MD5:	985db7fdfcf2aa3…
SHA1:	5f51dec30f3a649..
SHA256:	6e4323460316f29.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



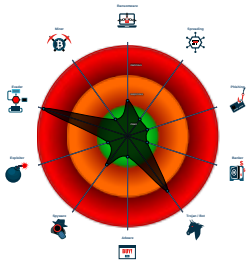
FormBook

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Yara detected AntiVM3
- System process connects to networ…
- Antivirus detection for URL or domain
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Tries to detect sandboxes and other…
- Modifies the prolog of user mode fun…

Classification



Process Tree

- **System is w10x64**
- Solicitud urgente de Quotaion_U1197,pdf.exe (PID: 6204 cmdline: "C:\Users\user\Desktop\Solicitud urgente de Quotaion_U1197,pdf.exe" MD5: 985DB7FDFCF2AA38A0B75C22F06B2756)
  - Solicitud urgente de Quotaion_U1197,pdf.exe (PID: 3560 cmdline: C:\Users\user\Desktop\Solicitud urgente de Quotaion_U1197,pdf.exe MD5: 985DB7FDFCF2AA38A0B75C22F06B2756)
  - Solicitud urgente de Quotaion_U1197,pdf.exe (PID: 6120 cmdline: C:\Users\user\Desktop\Solicitud urgente de Quotaion_U1197,pdf.exe MD5: 985DB7FDFCF2AA38A0B75C22F06B2756)
    - explorer.exe (PID: 3352 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - msdt.exe (PID: 6516 cmdline: C:\Windows\SysWOW64\msdt.exe MD5: 7F0C51DBA69B9DE5DDF6AA04CE3A69F4)
        - cmd.exe (PID: 6960 cmdline: /c del "C:\Users\user\Desktop\Solicitud urgente de Quotaion_U1197,pdf.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6020 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.coralxlix.com/c1h5/"
  ],
  "decoy": [
    "ui4dev.com",
    "horrycountyrealtor.com",
    "abivz.icu",
    "toxicwokeness.com",
    "fillthegap.site",
    "surprisessinside.com",
    "metaversefinder.xyz",
    "freeshipflowers.com",
    "apacheicon.com",
    "greenfootprintpros.com",
    "topauonlinecasino.com",
    "weqffg.site",
    "bountylux.com",
    "eedrvheyn.sbs",
    "whiskeybentmobile.com",
    "yupeg.xyz",
    "thenorthwesthome.com",
    "cyril.ventures",
    "zukunsmart.com",
    "1l7kng51j4nm.site",
    "nigeldavies.net",
    "8sscal.icu",
    "8wngeu.icu",
    "paramountnewtwork.com",
    "homehelperscalifornia.com",
    "tropicalbooking.com",
    "samsungwr.com",
    "gravityarchive.com",
    "hatdieuhoanglinhlinh.com",
    "masterysystemsinternational.com",
    "handandstoneparma.com",
    "tucsongolfacademy.com",
    "wholesalepoolkits.com",
    "2lovit.com",
    "calista-platinum.com",
    "dark9a.com",
    "sextremeboudoir.com",
    "dalmonello.com",
    "gyqfnc.com",
    "wqbz1.com",
    "kentuckyductless.com",
    "automotive-forensic.com",
    "metacityelves.com",
    "yckzy.com",
    "therobotians.com",
    "38qp2.com",
    "xqibit.site",
    "xn--o39a00am61aa311e3tj68d.com",
    "theb8szsk5vkv.com",
    "blackfridaypromoamericanas5.com",
    "4746390.win",
    "binkybones.com",
    "bridalhuich.com",
    "marceanahata.com",
    "kostense.email",
    "wellingboroughbid.com",
    "afxwn.icu",
    "nofrdictrack.com",
    "smohjs.com",
    "yjefcalg1p.top",
    "haseeb-wp.site",
    "analytics-at-scale.com",
    "adqc3.icu",
    "berekende.ink"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000006.00000000.298321821.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000006.00000000.298321821.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000006.00000000.298321821.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$sqlite3step: 68 34 1C 7B E1 • 0x1895c:$sqlite3step: 68 34 1C 7B E1 • 0x18878:$sqlite3text: 68 38 2A 90 C5 • 0x1899d:$sqlite3text: 68 38 2A 90 C5 • 0x1888b:$sqlite3blob: 68 53 D8 7F 8C • 0x189b3:$sqlite3blob: 68 53 D8 7F 8C
0000000A.00000002.560174409.0000000000770000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
0000000A.00000002.560174409.0000000000770000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 31 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
6.0.Solicitud urgente de Quotaion_U1197,pdf.exe.400000.8.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
6.0.Solicitud urgente de Quotaion_U1197,pdf.exe.400000.8.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
6.0.Solicitud urgente de Quotaion_U1197,pdf.exe.400000.8.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$sqlite3step: 68 34 1C 7B E1 • 0x1895c:$sqlite3step: 68 34 1C 7B E1 • 0x18878:$sqlite3text: 68 38 2A 90 C5 • 0x1899d:$sqlite3text: 68 38 2A 90 C5 • 0x1888b:$sqlite3blob: 68 53 D8 7F 8C • 0x189b3:$sqlite3blob: 68 53 D8 7F 8C
6.0.Solicitud urgente de Quotaion_U1197,pdf.exe.400000.6.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
6.0.Solicitud urgente de Quotaion_U1197,pdf.exe.400000.6.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8b08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x148b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x143a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x149b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x979a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1361c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa493:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab27:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bb2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 17 entries				

Sigma Overview

System Summary:

Sigma detected: Possible Applocker Bypass

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

System process connects to network (likely due to code injection or exploit)

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

Modifies the prolog of user mode functions (user mode inline hooks)

Self deletion via cmd delete

Malware Analysis System Evasion:

Yara detected AntiVM3

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

System process connects to network (likely due to code injection or exploit)

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Queues an APC in another process (thread injection)

Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information:

Yara detected FormBook

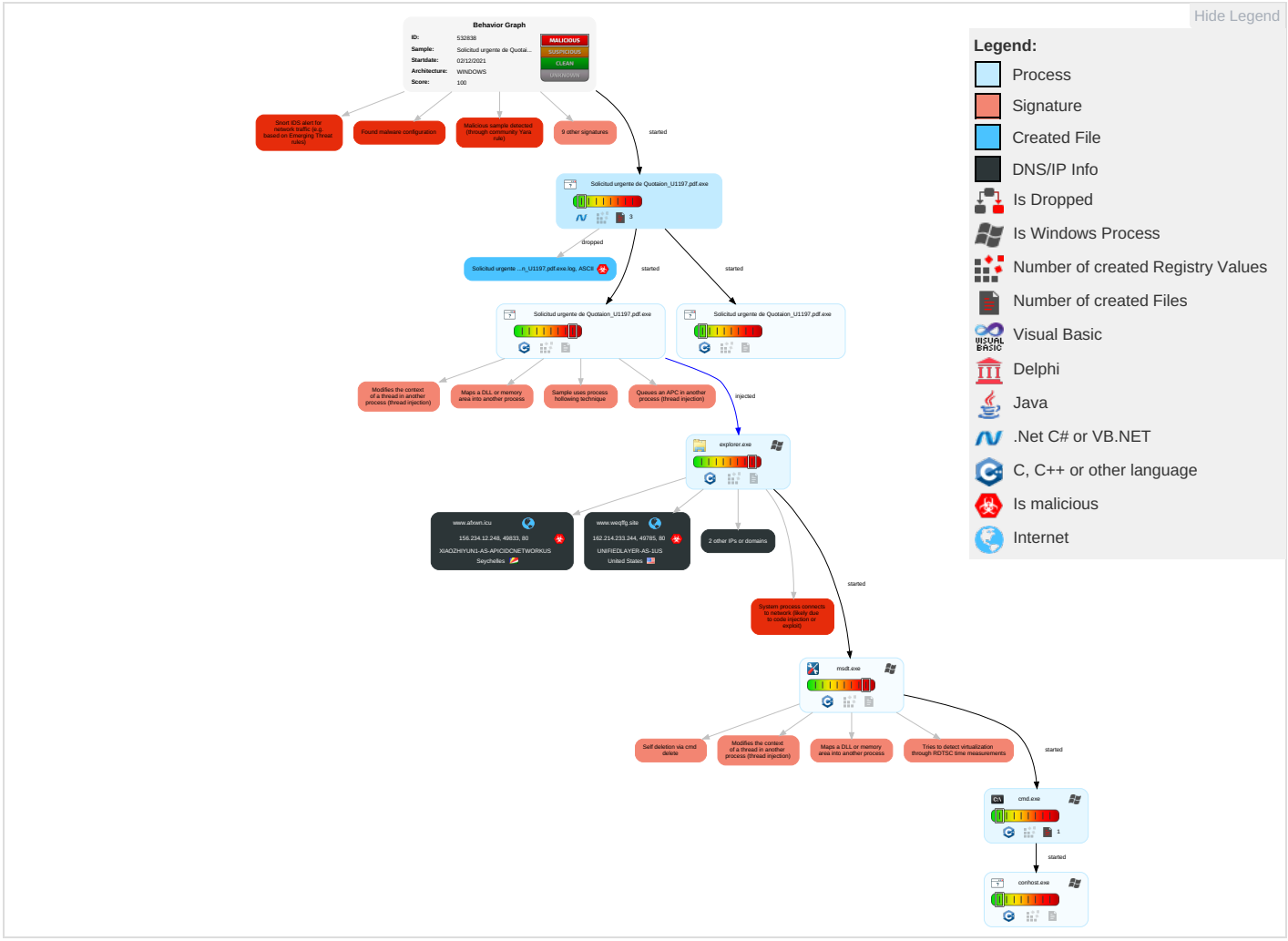
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 5 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 2 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 3 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 5 1 2	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3	DCSync	Network Sniffing	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	Software Packing 1 3	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Timestomp 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	File Deletion 1	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Transfer Protocols

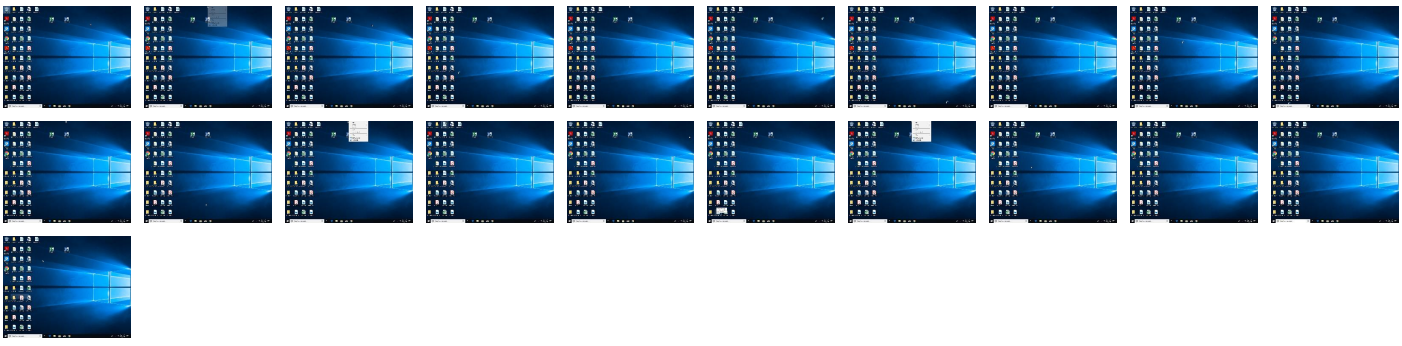
Behavior Graph



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

Source	Detection	Scanner	Label	Link
Solicitud urgente de Quotaion_U1197,pdf.exe	40%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.0.Solicitud urgente de Quotaion_U1197,pdf.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
6.0.Solicitud urgente de Quotaion_U1197,pdf.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
6.0.Solicitud urgente de Quotaion_U1197,pdf.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
6.2.Solicitud urgente de Quotaion_U1197,pdf.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
analytics-at-scale.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
www.coralxlix.com/c1h5/	0%	Avira URL Cloud	safe	
http://www.afxwn.icu/c1h5/?2do4nxu0=dDVdw41TThH+tglXdiSPLe9aGuOwvr9FdRXdYLI3Qef1kwVllG2roDseQXIwgkVkVQDX&q4Y4=kvWdz	0%	Avira URL Cloud	safe	
http://www.weqffg.site/c1h5/?2do4nxu0=xDzgA/AT2jMmjnlrkj7rt3ckDtoX4QGQrpVL2KD3Bff+aUtt+S7+kl+hKb5L2UO+/CvD&q4Y4=kvWdz	100%	Avira URL Cloud	phishing	
http://www.analytics-at-scale.com/c1h5/?2do4nxu0=eCqut3pLTAp695DvAk1SvvQ7mDNC6PWTA4g6LTP2Tz9bKaOndJvYlqsLJ7dAZrG7pLSW&q4Y4=kvWdz	0%	Avira URL Cloud	safe	
http://https://www.analytics-at-scale.com/c1h5/?2do4nxu0=eCqut3pLTAp695DvAk1SvvQ7mDNC6PWTA4g6LTP2Tz9bKaOndJ	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.afxwn.icu	156.234.12.248	true	true		unknown
www.weqffg.site	162.214.233.244	true	true		unknown
analytics-at-scale.com	192.0.78.24	true	true	• 1%, Virustotal, Browse	unknown
www.analytics-at-scale.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.coralxlix.com/c1h5/	true	• Avira URL Cloud: safe	low
http://www.afxwn.icu/c1h5/?2do4nxu0=dDVdw41TThH+tglXdiSPLe9aGuOwvr9FdRXdYLI3Qef1kwVllG2roDseQXIwgkVkVQDX&q4Y4=kvWdz	true	• Avira URL Cloud: safe	unknown
http://www.weqffg.site/c1h5/?2do4nxu0=xDzgA/AT2jMmjnlrkj7rt3ckDtoX4QGQrpVL2KD3Bff+aUtt+S7+kl+hKb5L2UO+/CvD&q4Y4=kvWdz	true	• Avira URL Cloud: phishing	unknown
http://www.analytics-at-scale.com/c1h5/?2do4nxu0=eCqut3pLTAp695DvAk1SvvQ7mDNC6PWTA4g6LTP2Tz9bKaOndJvYlqsLJ7dAZrG7pLSW&q4Y4=kvWdz	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.0.78.24	analytics-at-scale.com	United States		2635	AUTOMATTICUS	true
162.214.233.244	www.weqffg.site	United States		46606	UNIFIEDLAYER-AS-1US	true
156.234.12.248	www.afxwn.icu	Seychelles		136800	XIAOZHIYUN1-AS-APICIDCNETWORKUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532838
Start date:	02.12.2021
Start time:	18:37:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 53s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Solicitud urgente de Quotaion_U1197,pdf.exe

Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	23
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@9/1@3/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 15% (good quality ratio 13.5%) • Quality average: 73.8% • Quality standard deviation: 31.1%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
18:38:08	API Interceptor	1x Sleep call for process: Solicitud urgente de Quotaion_U1197,pdf.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
192.0.78.24	RFQ-18072 QPHN .doc	Get hash	malicious	Browse	• www.eminkoy.com/t3t2/?YTX8m6=X/AHJ1G8CzET27bRNAkcy2zo056pG+X2bUgtrIM6Usdw2LVzhx3zymRQr/cABPSK+z/Wow==&GZS=5jiXYnvXE6
	mtW2HRnhqB.exe	Get hash	malicious	Browse	• www.kgv-lachswehr.com/ea0r/?fHhDa=c9rlrwb5l0PsvCqZfPZLJ32YxU7lPLK2cV3voPHeBiJjRGf36/O5Za+oFiQ/bs3zoxiOdKVauQ==&2d=SFNDF0m

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	hNfqWik7qw.exe	Get hash	malicious	Browse	• www.amandaznaprawa.com/rht9/?NTiPcP=i488q&2d=oSEpyrDN2jpFtLPZR+/YFKSBf/v8Miz39LE5/YRv+zM0Krg9SxOGQM2eCbJi8hWE+L+z
	BL_CI_PL.exe	Get hash	malicious	Browse	• www.talkingpoint.tours/n8ds/?lZOD=wE3cJZPNojFXEHzVtPzLvjQgQ8siWlvoMBTDgMX5y9SxEB5bNYsjP9rL8bMOP+2FRUIW&E0Dpk=l8hHaF
	Dumak Order.xlsx	Get hash	malicious	Browse	• www.cletechsolutions.com/yrcy/?n2M4s4o=6oj+cRAcOTuW+xdHLRHF0KzLhmFT0afQnvz1X6yVwGfVu9zh+SVYblJ6SqTa14lOVkDkCg==&zbO=wpf8lJJX
	AWB_SHIPPING DOCS.exe	Get hash	malicious	Browse	• www.talkingpoint.tours/n8ds/?9rJT=wE3cJZPNojFXEHzVtPzLvjQgQ8siWlvoMBTDgMX5y9SxEB5bNYsjP9rL8bMOP+2FRUIW&v4VDH=WHU8k4m
	DuxgwH47QB.exe	Get hash	malicious	Browse	• www.magaliverdonck.com/cfn8/?7ntP2=G2JlCZwhJ8t&wZEhNtn=EAmfM1bZJ66AiKX05l3TaYUgrsfuP/gkLWzderYzqwcOOYaogkVBhIhYz1vuz5d9mKCz
	ORDER.doc	Get hash	malicious	Browse	• www.magaliverdonck.com/cfn8/?r0Dpfv=PV84qbppmxMhmF&etxxAzu=EAmfM1bcJ96Eiab47l3TaYUgrsfuP/gkLWrNCoEyuQcPOp2un0EN3MZawTjo4IJ2zs2EYw==
	Ordre de virement.exe	Get hash	malicious	Browse	• www.sammamotivation.com/wrcb/?i6=JRZY7R8EpGxMvUxoU9FjXImHM9r6be3CVb1cEdmzJ1+o3zoDrIbVKOVdp4L7IUQXVHQZ&Vn=5joLnT60H6Utl

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ja71FJcG4X.exe	Get hash	malicious	Browse	• www.fourjmedia.com/w8n5/?6lPx=Krsevr0fcKdFVj2db+BCLUY6buAyCdOHDU7bdlcHSmOR3oywPLLv+weEBRgOZ5y0K3R+&i2=bZ-LgDohxn7
	31hGtwI4CD.exe	Get hash	malicious	Browse	• www.givepy.info/s18y/?SF=697MTAEVXvVEXUyAJF20F132oezl1lQlpw2PkmQS81lH+yWLjKrG7SsVWH+sEO7fSxwKD9xmsQ==&7nT=4hfP1hlXyPvt5d80
	rfq.exe	Get hash	malicious	Browse	• www.faithtruthresolve.com/unzn/?m8a=YX6yD3qjkEh06A43Kvlzsqa1IJGgtNpO3VOCMHkgx/DYA63i6lhcxQdv+JiPSxcNqo3A&-Z=B0G8W4pHG
	sample02.exe	Get hash	malicious	Browse	• www.practicalmalwareanalysis.com/cc.htm
	6aA9bRxfnl.exe	Get hash	malicious	Browse	• www.cletechsolutions.com/yrcy/?1bxX=6oj+cRAZOUuS+hRLJRHF0KzLhmFT0afQnvrlL5uU0mfUuMfn5CEUNMx4RP/MxoM9eneU&5j=8pqxuZ4Prl2
	Remittance_advice.exe	Get hash	malicious	Browse	• www.baroquefolke.com/snr6/?mTZDVrwX=cbil4dbQ85/EoogyOScyzPrFGpGYEkh7zEyo7+xlFpBsIXqPkX0ip4hj/fSsceuRUxVF&lp=5jUHiDu8uBc
	AWB [EXTERNAL] RFQ-RVS QUOTATION .doc	Get hash	malicious	Browse	• www.fourjmedia.com/w8n5/?c45dyZs=Krsevr0acNdBVz6RZ+BCLUY6buAyCdOHDUjLBmAGWGOQ3Ze2Ibajo0mGC0MYdp2HB0MOmQ==&c8itZ=wRJxjZzxmlSHP2Hp

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	ELEGANT MARINE.exe	Get hash	malicious	Browse	• www.fourjmedia.com/w8n5/?o2JdMD=Krsevr0fcKdFVj2db+BCLUY6buAyCdOHDU7bdlcHSmOR3oywPLLv+weEBRgkGJC0O1Z+&q2JL=nZKHsDQPhRVD1D
	URGENT RFQ.doc	Get hash	malicious	Browse	• www.givepy.info/s18y/?2dGT=697MTAEQXoVAXE+MLF20F132oezl1lQlpwuf4lMT4VlG+D6Nka6KtWUXVh+qcvjXeHEraA==&aL0lqZ=h0G02VRHXrsHxf
	Ekol_LOG_00914,pdf.exe	Get hash	malicious	Browse	• www.flatironstreeservice.com/dgt9/?bH=DN9ti628iJ60&j4=9BOhy8kblAyJide7ynQBLE+qFSLeuxc/qvallqSEtgcGhdWxOk07eomuMpMdU/GfV2RowavF0Q==
	v54ueAmr6D.exe	Get hash	malicious	Browse	• www.mainponsel.com/n8cr/?nL0DH=mVFDnNjLroOTVY/e2vMB3+FXNX8eexEZxlQPv7nMWghAxegu28tS6Ss7v6+WYlySqVct&c48dyT=rPYXgR

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	OSCBLUS33XXX1032021110200150939.exe	Get hash	malicious	Browse	• 192.185.224.36
	RFQ - SST#2021111503.exe	Get hash	malicious	Browse	• 162.241.253.162
	ufKi6DmWMQCuEb4.exe	Get hash	malicious	Browse	• 192.185.16.241
	counter-1248368226.xls	Get hash	malicious	Browse	• 108.179.192.98
	counter-1248368226.xls	Get hash	malicious	Browse	• 108.179.192.98
	counter-1248368226.xls	Get hash	malicious	Browse	• 108.179.192.98
	counter-1248368226.xls	Get hash	malicious	Browse	• 108.179.192.98
	CU-6431 report.xlsm	Get hash	malicious	Browse	• 162.240.9.126
	CU-6431 report.xlsm	Get hash	malicious	Browse	• 162.240.9.126
	DkX9HVJTmi.exe	Get hash	malicious	Browse	• 108.167.135.122
	Shipping report -17420.xlsx	Get hash	malicious	Browse	• 162.241.169.32
	SCAN_7295943480515097.xlsm	Get hash	malicious	Browse	• 162.240.9.126
	SCAN_7295943480515097.xlsm	Get hash	malicious	Browse	• 162.240.9.126
	INVOICE.exe	Get hash	malicious	Browse	• 162.214.80.6
	img20048901738_Pago.pdf.exe	Get hash	malicious	Browse	• 192.185.115.3
	PaCJ39hC4R.xlsx	Get hash	malicious	Browse	• 162.241.126.156
	PaCJ39hC4R.xlsx	Get hash	malicious	Browse	• 162.241.126.156
	New order documents. pdf.....exe	Get hash	malicious	Browse	• 108.179.232.76

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	part-1500645108.xlsb	Get hash	malicious	Browse	• 162.241.62.201
	img20048901740_Pago.pdf.exe	Get hash	malicious	Browse	• 192.185.115.3
AUTOMATTICUS	RFQ-18072 QPHN .doc	Get hash	malicious	Browse	• 192.0.78.24
	mtW2HRnhqB.exe	Get hash	malicious	Browse	• 192.0.78.24
	IM-87678A-1A.msi	Get hash	malicious	Browse	• 192.0.77.32
	hNfqWik7qw.exe	Get hash	malicious	Browse	• 192.0.78.24
	forensic_challenge(1).html	Get hash	malicious	Browse	• 192.0.77.32
	BL_CI_PL.exe	Get hash	malicious	Browse	• 192.0.78.24
	PilHb37Gmt.exe	Get hash	malicious	Browse	• 74.114.154.22
	2A9E7BC07BD4EC39C2BEAA42FF35352BBE6400F899F70.exe	Get hash	malicious	Browse	• 74.114.154.18
	0A7D966E66CBD260C909DE1D79038C86A071F2F10A810.exe	Get hash	malicious	Browse	• 74.114.154.18
	6DFD902231E6AA1301C11ECA21F5A29456AA020BFE1EB.exe	Get hash	malicious	Browse	• 74.114.154.22
	B10274561191CEDB0B16D2A69FDCD4E5062EDFE262184.exe	Get hash	malicious	Browse	• 74.114.154.18
	Dumak Order.xlsx	Get hash	malicious	Browse	• 192.0.78.24
	uSD1d8nRJ0.exe	Get hash	malicious	Browse	• 192.0.78.248
	PO P232-2111228.xlsx	Get hash	malicious	Browse	• 192.0.78.25
	PROFORMA INVOICE.xlsx	Get hash	malicious	Browse	• 192.0.78.25
	fpvN6iDp5r.msi	Get hash	malicious	Browse	• 192.0.77.32
	Zr26f1rL6r.exe	Get hash	malicious	Browse	• 192.0.78.25
	2sX7IceYWM.msi	Get hash	malicious	Browse	• 192.0.77.32
	vbc.exe	Get hash	malicious	Browse	• 192.0.78.25
	162AB00C0E943F9548B04F343786750865648058 5369C.exe	Get hash	malicious	Browse	• 74.114.154.18

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Solicitud urgente de Quotaion_U1197,pdf.exe.log	
Process:	C:\Users\user\Desktop\Solicitud urgente de Quotaion_U1197,pdf.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1310
Entropy (8bit):	5.345651901398759
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE47mE4Ko88:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKz6
MD5:	D918C6A765EDB90D2A227FE23A3FEC98
SHA1:	8BA802AD8D740F114783F0DADC407CBFD2A209B3
SHA-256:	AB0E9F716E31502A4C6786575C5E64DFD9D24AF99056BBE2640A2FA322CFF4D6
SHA-512:	A937ABD8294BB32A612F8B3A376C94111D688379F0A4DB9FAA2FCEB71C25E18D621EEBCFDA5706B71C8473A4F38D8B3C4005D1589B564F9B1C9C441B6D33784
Malicious:	**true**
Reputation:	moderate, 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

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.69240335411092
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Solicitud urgente de Quotaion_U1197,pdf.exe
File size:	456192
MD5:	985db7fdfcf2aa38a0b75c22f06b2756
SHA1:	5f51dec30f3a649fc49e95e3421bc247cf9c40c7
SHA256:	6e4323460316f29ecdaa2b49fbe733c11ea3a040cf7336e177ac9345ddac21c1
SHA512:	469037a46ca39a8540b81bc18016058d170f99ba98707883b3a4c0a1c9a3a4b84fe2f849765b17c7e8387db13ca1d96148abda2a676d688b6b1f0a1c062a063d
SSDEEP:	6144:h3j2kQqvZRHs/KTAva0AfvzIBOU5LrBhtIMiHDrH03S0NJQeEv6si/c5U/TU1zN1:101NBxRrPtIhjrUi+QzRoTU1zNBjf
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....H.....J.....N.... .....@.. .....`.....@.....

File Icon

Icon Hash:	94ba3a92e98cb6c8

Static PE Info

General

Entrypoint:	0x46c94e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0xD47F48BF [Mon Dec 21 20:44:47 2082 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x6a954	0x6aa00	False	0.877765973036	data	7.76378455521	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.rsrc	0x6e000	0x47ac	0x4800	False	0.258192274306	data	4.85061345991	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x74000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
12/02/21-18:39:50.928609	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49833	156.234.12.248	192.168.2.3
12/02/21-18:40:11.587934	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49872	80	192.168.2.3	192.0.78.24
12/02/21-18:40:11.587934	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49872	80	192.168.2.3	192.0.78.24
12/02/21-18:40:11.587934	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49872	80	192.168.2.3	192.0.78.24

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 2, 2021 18:39:27.422539949 CET	192.168.2.3	8.8.8.8	0x8b16	Standard query (0)	www.weqffg.site	A (IP address)	IN (0x0001)
Dec 2, 2021 18:39:50.271529913 CET	192.168.2.3	8.8.8.8	0x96ce	Standard query (0)	www.afxwn.icu	A (IP address)	IN (0x0001)
Dec 2, 2021 18:40:11.538088083 CET	192.168.2.3	8.8.8.8	0x50a3	Standard query (0)	www.analytics-at-scale.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Dec 2, 2021 18:39:27.569787979 CET	8.8.8.8	192.168.2.3	0x8b16	No error (0)	www.weqffg.site		162.214.233.244	A (IP address)	IN (0x0001)
Dec 2, 2021 18:39:50.446052074 CET	8.8.8.8	192.168.2.3	0x96ce	No error (0)	www.afxwn.icu		156.234.12.248	A (IP address)	IN (0x0001)
Dec 2, 2021 18:40:11.569740057 CET	8.8.8.8	192.168.2.3	0x50a3	No error (0)	www.analytics-at-scale.com	analytics-at-scale.com		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 18:40:11.569740057 CET	8.8.8.8	192.168.2.3	0x50a3	No error (0)	analytics-at-scale.com		192.0.78.24	A (IP address)	IN (0x0001)
Dec 2, 2021 18:40:11.569740057 CET	8.8.8.8	192.168.2.3	0x50a3	No error (0)	analytics-at-scale.com		192.0.78.25	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.weqffg.site
- www.afxwn.icu
- www.analytics-at-scale.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49785	162.214.233.244	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 18:39:27.749593019 CET	9660	OUT	GET /c1h5/?2do4nxu0=xDzgA/AT2jMmjnlrkj7rt3ckDtoX4QGQrpVL2KD3Bff+aUtt+S7+kl+hKb5L2UO+/CvD&q4Y4=kvWdz HTTP/1.1 Host: www.weqffg.site Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 2, 2021 18:39:27.910689116 CET	9770	IN	HTTP/1.1 404 Not Found Server: nginx Date: Thu, 02 Dec 2021 17:39:27 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>404 Not Found</title></head><body> 404 Not Found <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.3	49833	156.234.12.248	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 18:39:50.688074112 CET	9884	OUT	GET /c1h5/?2do4nxu0=dDVdw41TThH+tglXdiSPLe9aGuOwvr9FdRXdYLI3Qef1kwVllG2roDseQXIwgkVkVQDX&q4Y4=kvWdz HTTP/1.1 Host: www.afxwn.icu Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 2, 2021 18:39:50.928608894 CET	9885	IN	HTTP/1.1 403 Forbidden Server: nginx Date: Thu, 02 Dec 2021 17:39:50 GMT Content-Type: text/html Content-Length: 146 Connection: close Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body> 403 Forbidden <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.3	49872	192.0.78.24	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 18:40:11.587934017 CET	9976	OUT	GET /c1h5/?2do4nxu0=eCqut3pLTAp695DvAk1SvvQ7mDNC6PWTA4g6LTP2Tz9bKaOndJvYlqsLJ7dAZrG7pLSW&q4Y4=kvWdz HTTP/1.1 Host: www.analytics-at-scale.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 18:40:11.604665041 CET	9976	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Thu, 02 Dec 2021 17:40:11 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.analytics-at-scale.com/c1h5/?2do4nxu0=eCqut3pLTAp695DvAk1SvvQ7mDNC6PWTA4g6LTP2Tz9bKaOndJvYlqsLJ7dAZrG7pLSW&q4Y4=kvWdz X-ac: 2.hhn _dfw Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
PeekMessageA	INLINE	explorer.exe
PeekMessageW	INLINE	explorer.exe
GetMessageW	INLINE	explorer.exe
GetMessageA	INLINE	explorer.exe

Processes

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Solicitud urgente de Quotaion_U1197,pdf.exe PID: 6204 Parent PID: 5052

General

Start time:	18:38:06
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\Solicitud urgente de Quotaion_U1197,pdf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\Solicitud urgente de Quotaion_U1197,pdf.exe"
Imagebase:	0xf20000
File size:	456192 bytes
MD5 hash:	985DB7FDFCF2AA38A0B75C22F06B2756
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.300643719.0000000003301000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.300683350.000000000333D000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.301296785.0000000004309000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.301296785.0000000004309000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.301296785.0000000004309000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: Solicitud urgente de Quotaion_U1197,pdf.exe PID: 3560 Parent PID: 6204

General

Start time:	18:38:08
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\Solicitud urgente de Quotaion_U1197,pdf.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\Solicitud urgente de Quotaion_U1197,pdf.exe
Imagebase:	0x90000
File size:	456192 bytes
MD5 hash:	985DB7FDFCF2AA38A0B75C22F06B2756
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: Solicitud urgente de Quotaion_U1197,pdf.exe PID: 6120 Parent PID: 6204

General

Start time:	18:38:09
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\Solicitud urgente de Quotaion_U1197,pdf.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Solicitud urgente de Quotaion_U1197,pdf.exe
Imagebase:	0xd50000
File size:	456192 bytes
MD5 hash:	985DB7FDFCF2AA38A0B75C22F06B2756
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.298321821.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.298321821.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.298321821.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.372897742.0000000001730000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.372897742.0000000001730000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.372897742.0000000001730000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.298732907.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.298732907.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.298732907.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.372402095.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.372402095.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.372402095.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.373637862.000000001A90000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.373637862.000000001A90000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.373637862.000000001A90000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3352 Parent PID: 6120

General

Start time:	18:38:12
Start date:	02/12/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff720ea0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000000.338321770.00000000100B5000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.338321770.00000000100B5000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.338321770.00000000100B5000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000000.354531059.00000000100B5000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000000.354531059.00000000100B5000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000000.354531059.00000000100B5000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: msdt.exe PID: 6516 Parent PID: 3352

General

Start time:	18:38:39
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\msdt.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msdt.exe
Imagebase:	0xeb0000
File size:	1508352 bytes
MD5 hash:	7F0C51DBA69B9DE5DDF6AA04CE3A69F4
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.560174409.0000000000770000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.560174409.0000000000770000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.560174409.0000000000770000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.563987618.00000000007C0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.563987618.00000000007C0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.563987618.00000000007C0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.558246949.0000000000120000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.558246949.0000000000120000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.558246949.0000000000120000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 6960 Parent PID: 6516

General

Start time:	18:38:47
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\Solicitud urgente de Quotaion_U1197,pdf.exe"
Imagebase:	0xd80000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 6020 Parent PID: 6960

General

Start time:	18:38:48
Start date:	02/12/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis