ID: 755986
Sample Name: Copie a bonului de plata.exe
Cookbook: default.jbs
Time: 12:47:07
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Copyright Joe Security LLC 2022

Copyright Joe Security LLC 2022

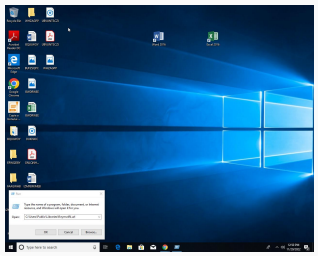
Windows Analysis Report

Copie a bonului de plata.exe

Overview

General Information

Sample Name:	Copie a bonului de plata.exe
Analysis ID:	755986
MD5:	eb8c68c29d6131..
SHA1:	61dfb557d2e792..
SHA256:	d1798c288b2960..
Tags:	exe ModiLoader
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

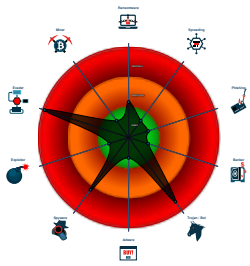
FormBook, DBatLoader

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

Signatures

- Detected FormBook malware
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- Sigma detected: Steal Google chrom…
- Antivirus / Scanner detection for sub…
- Yara detected DBatLoader
- System process connects to networ…
- Antivirus detection for URL or domain
- Antivirus detection for dropped file
- Multi AV Scanner detection for drop…
- Sample uses process hollowing tech…

Classification



Process Tree

- **System is w10x64**
- Copie a bonului de plata.exe (PID: 5152 cmdline: C:\Users\user\Desktop\Copie a bonului de plata.exe MD5: EB8C68C29D6131D6B903DD268D6FF0EF)
  - colorcpl.exe (PID: 3556 cmdline: C:\Windows\System32\colorcpl.exe MD5: 746F3B5E7652EA0766BA10414D317981)
    - explorer.exe (PID: 3452 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - Ndvmyrkf.exe (PID: 5252 cmdline: "C:\Users\Public\Libraries\Ndvmyrkf.exe" MD5: EB8C68C29D6131D6B903DD268D6FF0EF)
        - wscript.exe (PID: 4648 cmdline: C:\Windows\System32\wscript.exe MD5: 7075DD7B9BE8807FCA93ACD86F724884)
      - raserver.exe (PID: 3868 cmdline: C:\Windows\SysWOW64\raserver.exe MD5: 2AADF65E395BFBD0D9B71D7279C8B5EC)
        - cmd.exe (PID: 3672 cmdline: /c copy "C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data" "C:\Users\user\AppData\Local\Temp\DB1" /V MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 1808 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
      - msdt.exe (PID: 632 cmdline: C:\Windows\SysWOW64\msdt.exe MD5: 7F0C51DBA69B9DE5DDF6AA04CE3A69F4)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.xctech.world/3nop/"
  ],
  "decoy": [
    "slot999.site",
    "hagsahoy.com",
    "howdyart.com",
    "orders-marketplace.com",
    "ranaa.email",
    "masterlink.guru",
    "archershut.com",
    "weikumcommunications.com",
    "dphardmoney.com",
    "shjyutie.com",
    "vivaberlin.net",
    "mycto.today",
    "curvygirlugc.com",
    "otnmp.cfd",
    "alwrists.com",
    "propercandlecompany.com",
    "allindustry-bg.com",
    "theyoungbizacademy.com",
    "expand658170.com",
    "leslainesdumouchon.com",
    "suptisa.com",
    "picnic-in-andong.com",
    "wanligui.com",
    "cesarjunaro.com",
    "kuxita.xyz",
    "simpkecpr.com",
    "microsoftsecuritys.com",
    "responsefactor.com",
    "polyggroup.com",
    "talonxmfg.biz",
    "jam-nins.com",
    "picuar.com",
    "familysafehidingplaces.com",
    "centericehockey.com",
    "appleidd.info",
    "igctsansculottism.sbs",
    "guiaestilosaude.online",
    "happysscribe.com",
    "tizzbizz.com",
    "qcorretor.com",
    "baremaster.online",
    "liputanlima.com",
    "ontherighttrack.systems",
    "zzza002.xyz",
    "k-aashirwaad.com",
    "stillwatersagawork.com",
    "skindoze.com",
    "asdjmhfg.xyz",
    "refaccionariafgnogales.com",
    "hunn.pro",
    "tlland.group",
    "homebizen.com",
    "newszi.xyz",
    "nicetimecafe.net",
    "qdbs.cloud",
    "ebtl.wtf",
    "dchasss.com",
    "kijangjantan.tech",
    "elegant-story.com",
    "glimtmedia.com",
    "1dot.online",
    "neatneighborncclean.com",
    "marionarzel.com",
    "app-arthrex.com"
  ]
}
```


Copyright Joe Security LLC 2022

Threatname: DBatLoader


```
{
  "Download Url": "https://onedrive.live.com/download?cid=E0CF7F9E6AAF27EF&resid=E0CF7F9E6AAF27EF%21845&authkey=AIl8u0Az19Gihis"
}
```


Yara Signatures

Dropped Files

Source	Rule	Description	Author	Strings
C:\Users\Public\Libraries\fkrymvdN.url	Methodology_Shortcut_HotKey	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0x58:$hotkey: \x0AHotKey=3 • 0x0:$url_explicit: [InternetShortcut]
C:\Users\Public\Libraries\fkrymvdN.url	Methodology_Contains_Shortcut_OtherURIhandlers	Detects possible shortcut usage for .URL persistence	@itsreallynick (Nick Carr)	• 0x14:$file: URL= • 0x0:$url_explicit: [InternetShortcut]

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.368934423.0000000010410000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000001.00000002.368934423.0000000010410000.00000040.00000400.00020000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x6251:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1cb90:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xa9bf:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x158a7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
00000001.00000002.368934423.0000000010410000.00000040.00000400.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1591f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa58a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1440c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb283:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b8e7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c8fa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000001.00000002.368934423.0000000010410000.00000040.00000400.00020000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18809:$sqlite3step: 68 34 1C 7B E1 • 0x1891c:$sqlite3step: 68 34 1C 7B E1 • 0x18838:$sqlite3text: 68 38 2A 90 C5 • 0x1895d:$sqlite3text: 68 38 2A 90 C5 • 0x1884b:$sqlite3blob: 68 53 D8 7F 8C • 0x18973:$sqlite3blob: 68 53 D8 7F 8C
00000006.00000000.300982694.0000000010410000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Click to see the 91 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
6.0.wscript.exe.10410000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
6.0.wscript.exe.10410000.1.unpack	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x5451:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1bd90:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0x9bbf:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x14aa7:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
6.0.wscript.exe.10410000.1.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8b08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d72:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x148a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14391:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x149a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b1f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x978a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 8 3 E3 0F C1 EA 06 • 0x1360c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa483:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1aae7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bafa:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
6.0.wscript.exe.10410000.1.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x17a09:$sqlite3step: 68 34 1C 7B E1 • 0x17b1c:$sqlite3step: 68 34 1C 7B E1 • 0x17a38:$sqlite3text: 68 38 2A 90 C5 • 0x17b5d:$sqlite3text: 68 38 2A 90 C5 • 0x17a4b:$sqlite3blob: 68 53 D8 7F 8C • 0x17b73:$sqlite3blob: 68 53 D8 7F 8C
1.0.colorcpl.exe.10410000.1.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 78 entries				

Sigma Signatures

Stealing of Sensitive Information

Sigma detected: Steal Google chrome login data

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Detected FormBook malware

Malicious sample detected (through community Yara rule)

Data Obfuscation

Yara detected DBatLoader

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)

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Writes to foreign memory regions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

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

Creates a thread in another existing process (thread injection)

Stealing of Sensitive Information

Yara detected FormBook

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality

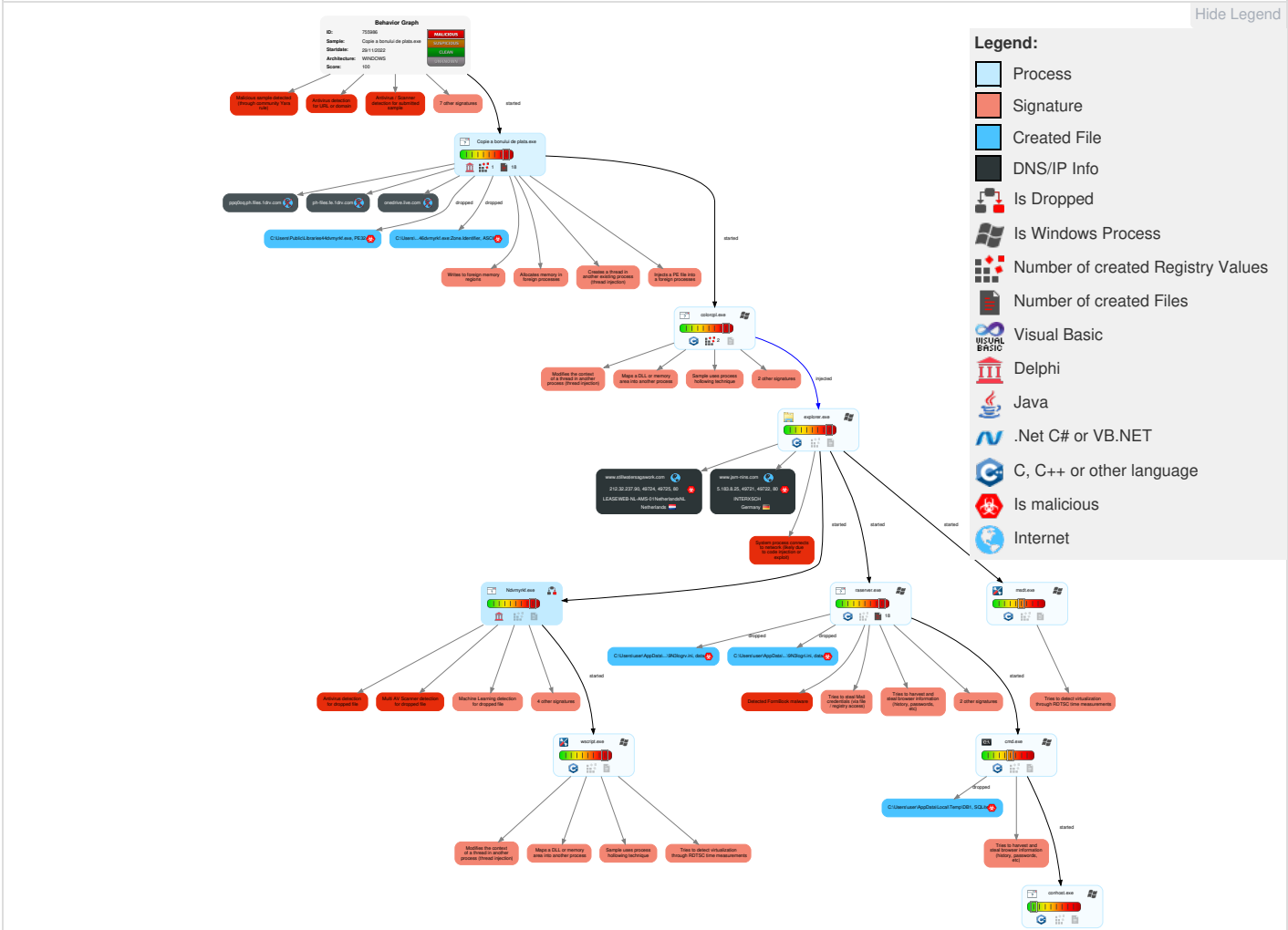
Yara detected FormBook

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 Native API	1 DLL Side-Loading	1 DLL Side-Loading	1 Deobfuscate/Decode Files or Information	1 OS Credential Dumping	1 System Time 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
Default Accounts	1 Shared Modules	1 Registry Run Keys / Startup Folder	9 1 2 Process Injection	2 Obfuscated Files or Information	1 Credential API Hooking	3 File and Directory Discovery	Remote Desktop Protocol	1 Data from Local System	Exfiltration Over Bluetooth	1 Encrypted Channel	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Domain Accounts	At (Linux)	Logon Script (Windows)	1 Registry Run Keys / Startup Folder	1 Software Packing	1 Input Capture	1 1 5 System Information Discovery	SMB/Windows Admin Shares	1 Email Collection	Automated Exfiltration	4 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)	1 DLL Side-Loading	NTDS	2 2 1 Security Software Discovery	Distributed Component Object Model	1 Credential API Hooking	Scheduled Transfer	1 1 4 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Rootkit	LSA Secrets	2 Virtualization/Sandbox Evasion	SSH	1 Input Capture	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 Masquerading	Cached Domain Credentials	3 Process 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	2 Virtualization/Sandbox Evasion	DCSync	1 Remote System 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	9 1 2 Process Injection	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

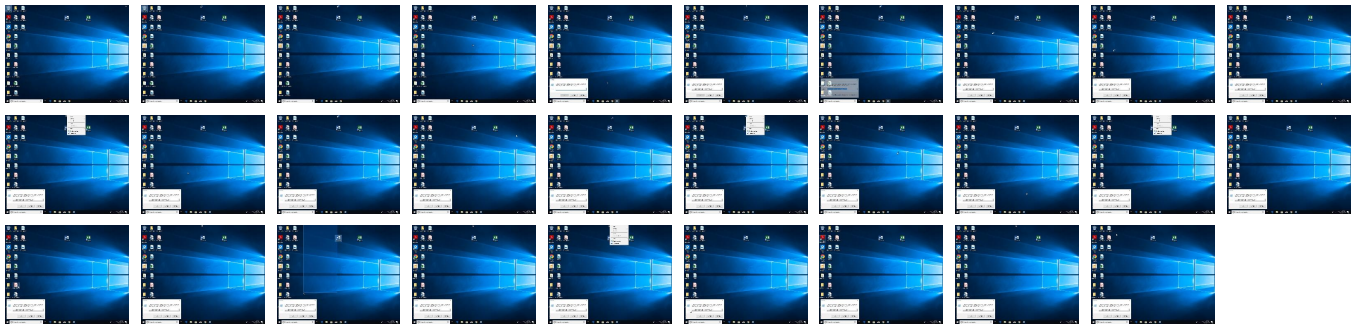
Behavior Graph



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
Copie a bonului de plata.exe	20%	ReversingLabs	Win32.Trojan.Generic	
Copie a bonului de plata.exe	26%	Virustotal		Browse

Source	Detection	Scanner	Label	Link
Copie a bonului de plata.exe	100%	Avira	HEUR/AGEN.1214697	
Copie a bonului de plata.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\Libraries\Ndvmyrkf.exe	100%	Avira	HEUR/AGEN.1214697	
C:\Users\Public\Libraries\Ndvmyrkf.exe	100%	Joe Sandbox ML		
C:\Users\Public\Libraries\Ndvmyrkf.exe	20%	ReversingLabs	Win32.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.0.wscript.exe.10410000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.0.Copie a bonului de plata.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1214697		Download File
3.2.Ndvmyrkf.exe.2268248.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
6.0.wscript.exe.10410000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.colorcpl.exe.10410000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
6.0.wscript.exe.10410000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.0.colorcpl.exe.10410000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.Copie a bonului de plata.exe.23c8248.2.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
1.0.colorcpl.exe.10410000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.Copie a bonului de plata.exe.22b0000.0.unpack	100%	Avira	TR/Hijacker.Gen		Download File
6.2.wscript.exe.10410000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
1.2.colorcpl.exe.10410000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.Copie a bonului de plata.exe.2381218.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.0.colorcpl.exe.10410000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
6.0.wscript.exe.10410000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
0.2.Copie a bonului de plata.exe.2a4eed8.3.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://survey-smiles.com	0%	URL Reputation	safe	
http://www.jam-nins.com/3nop/?IR-DA=FNGt6FUR7BoC+Wk2mT/OXzHG9rfZBcl/fjySAuf4KaFOaHLtldhTTP3Ojf6osS08NYIgkgrbcw==&5j=6leTg0VPe4i	100%	Avira URL Cloud	malware	
http://www.stillwatersagawork.com	0%	Avira URL Cloud	safe	
http://www.stillwatersagawork.com/3nop/?IR-DA=uizPEf3ZCIKf+0vjz41ZIbJXQmeLMi3XcgBA4XxBdLh6ZlOYX2KmQQVjEXygOMnK9OyVSVhb/w==&5j=6leTg0VPe4i	100%	Avira URL Cloud	malware	
http://www.stillwatersagawork.com/3nop/	100%	Avira URL Cloud	malware	
www.xctech.world/3nop/	100%	Avira URL Cloud	malware	
http://www.jam-nins.com/3nop/	100%	Avira URL Cloud	malware	

Copyright Joe Security LLC 2022

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.jam-nins.com	5.183.8.25	true	true		unknown
www.stillwatersagawork.com	212.32.237.90	true	true		unknown
onedrive.live.com	unknown	unknown	false		high
ppq0oq.ph.files.1drv.com	unknown	unknown	false		high

Contacted URLs

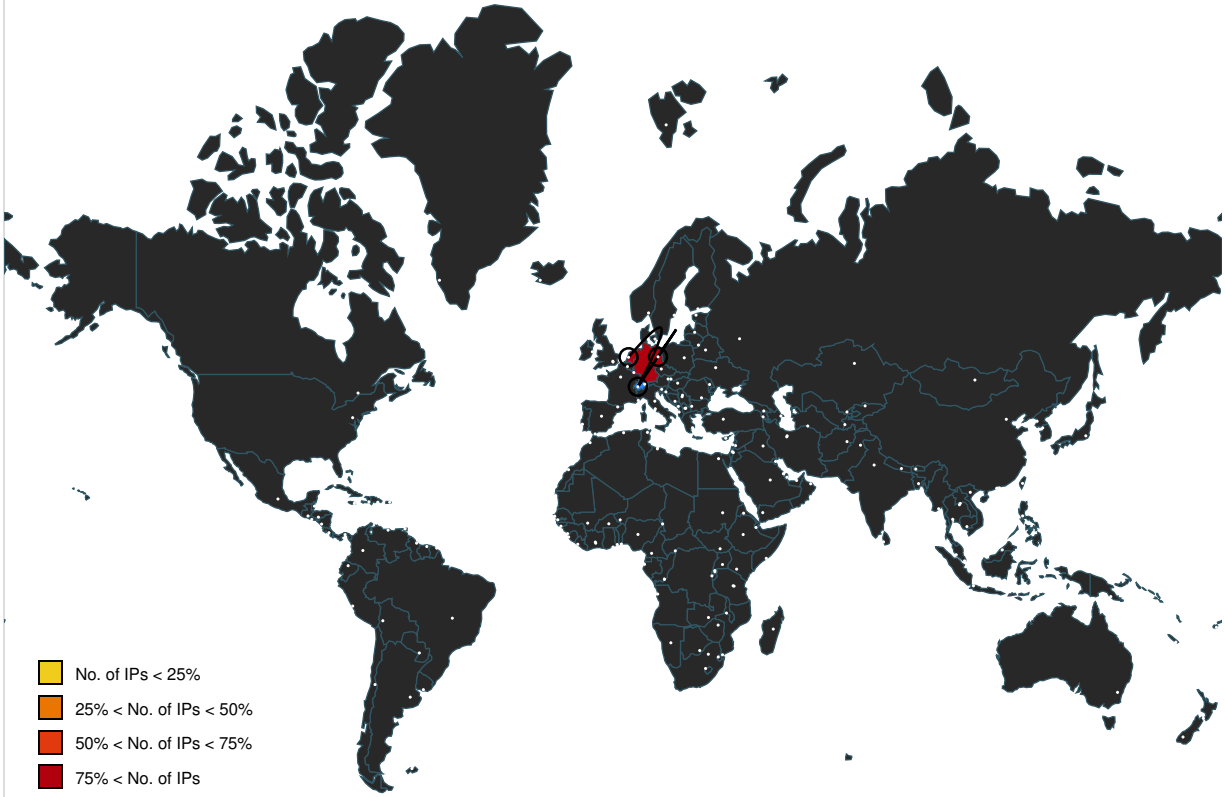
Name	Malicious	Antivirus Detection	Reputation
www.xctech.world/3nop/	true	• Avira URL Cloud: malware	low
http://www.stillwatersagawork.com/3nop/	true	• Avira URL Cloud: malware	unknown
http://https://onedrive.live.com/download?cid=E0CF7F9E6AAF27EF&resid=E0CF7F9E6AAF27EF%21845&authkey=AII8u0Az19Gihis	false		high
http://www.jam-nins.com/3nop/?IR-DA=FNGt6FUR7BoC+Wk2mT/OXzHG9rfZBcl/fjySAuf4KaFOaHLtldhTTP3Ojf6osS08NYIgkgrbcw==&5j=6leTg0VPe4i	true	• Avira URL Cloud: malware	unknown
http://www.jam-nins.com/3nop/	true	• Avira URL Cloud: malware	unknown
http://www.stillwatersagawork.com/3nop/?IR-DA=uizPEf3ZCIKf+0vjz41ZIbJXQmeLMi3XcgBA4XxBdLh6ZlOYX2KmQQVjEXygOMnK9OyVSVhb/w==&5j=6leTg0VPe4i	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000002.00000000.33939165 7.0000000000AC8000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 002.00000000.265456363.0000000000AC8000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000002.00000000.325519457.000000 0000AC8000.00000004.00000020.00020000.00 000000.sdmp, explorer.exe, 00000002.0000 0000.307576033.0000000000AC8000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 00000002.00000000.327025987.00000000084420 00.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000002.00000000.300998928.000 0000008442000.00000004.00000001.00020000 .00000000.sdmp	false		high
http://https://ppq0oq.ph.files.1drv.com/y	Copie a bonului de plata.exe, 00000000.00000003.25 3118024.0000000000888000.00000004.000000 20.00020000.00000000.sdmp	false		high
http://https://onedrive.live.com/download?cid=E0CF7F9E6AAF27EF&resid=E0CF7F9E6AAF27EF%21845&authkey=AII8u0A	Copie a bonului de plata.exe, 00000000.00000002.26 1332912.000000000082F000.00000004.000000 20.00020000.00000000.sdmp	false		high
http://https://ppq0oq.ph.files.1drv.com/y4mTq5RZ8ohnMX6xf7NDPAPVNhWu7XDJIy7fluYHyTqr4rWZJ8CBMittNjykZHXcnJ_	Copie a bonului de plata.exe, 00000000.00000003.25 4351119.000000000089D000.00000004.000000 20.00020000.00000000.sdmp, Copie a bonului de plata.exe, 00000000.00000002.261332912.00000 0000082F000.00000004.00000020.00020000.0 0000000.sdmp, Copie a bonului de plata.exe, 000000 00.00000002.261941242.00000000008CC000.0 0000004.00000020.00020000.00000000.sdmp, Copie a bonului de plata.exe, 00000000.00000003.2 53162647.00000000008D7000.00000004.00000 020.00020000.00000000.sdmp	false		high
http://www.stillwatersagawork.com	raserver.exe, 0000000C.00000002.51755999 8.0000000005879000.00000004.10000000.000 40000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ppq0oq.ph.files.1drv.com/	Copie a bonului de plata.exe, 00000000.00000003.25 4351119.000000000089D000.00000004.000000 20.00020000.00000000.sdmp	false		high
http://https://ppq0oq.ph.files.1drv.com/y4mSOYNl8PReN028zDgtLGTbNYcgZC2HyHGQN3fPTRemBgwyzYyJn9Rzn0pByB78UZm	Copie a bonului de plata.exe, 00000000.00000002.26 1332912.000000000082F000.00000004.000000 20.00020000.00000000.sdmp, Copie a bonului de plata.exe, 00000000.00000002.261941242.00000 000008CC000.00000004.00000020.00020000.0 0000000.sdmp	false		high
http://https://onedrive.live.com/	Copie a bonului de plata.exe, 00000000.00000002.26 1332912.000000000082F000.00000004.000000 20.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://survey-smiles.com	raserver.exe, 0000000C.00000002.51796960 2.0000000005BEF000.00000004.10000000.000 40000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://ppq0oq.ph.files.1drv.com/t	Copie a bonului de plata.exe, 00000000.00000003.25 4351119.000000000089D000.00000004.000000 20.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
5.183.8.25	www.jam-nins.com	Germany		64463	INTERXSCH	true
212.32.237.90	www.stillwatersagawork.com	Netherlands		60781	LEASEWEB-NL-AMS-01NetherlandsNL	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	755986
Start date and time:	2022-11-29 12:47:07 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 41s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Copie a bonului de plata.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	17
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

Copyright Joe Security LLC 2022

Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@11/10@4/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 99% (good quality ratio 86.8%) • Quality average: 75.1% • Quality standard deviation: 33.7%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 13.107.42.13, 13.107.42.12
- Excluded domains from analysis (whitelisted): www.bing.com, l-0004.l-msedge.net, odc-web-brs.onedrive.akadns.net, client.wns.windows.com, odwebpl.trafficmanager.net.l-0004.dc-msedge.net.l-0004.l-msedge.net, fs.microsoft.com, l-0003.l-msedge.net, odc-web-geo.onedrive.akadns.net, ph-files.ha.1drv.com.l-0003.dc-msedge.net.l-0003.l-msedge.net, ctldl.windowsupdate.com, odc-ph-files-geo.onedrive.akadns.net, odc-ph-files-brs.onedrive.akadns.net
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtOpenFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
12:48:03	API Interceptor	1x Sleep call for process: Copie a bonului de plata.exe modified
12:48:10	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run Ndvmyrkf C:\Users\Public\Libraries\fkrymvdN.url
12:48:18	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run Ndvmyrkf C:\Users\Public\Libraries\fkrymvdN.url
12:48:25	API Interceptor	1x Sleep call for process: Ndvmyrkf.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\Public\Libraries\Ndvmyrkf

Process:	C:\Users\user\Desktop\Copie a bonului de plata.exe
File Type:	data
Category:	dropped
Size (bytes):	189867
Entropy (8bit):	7.833666236780806
Encrypted:	false
SSDEEP:	3072:nB2d+y45Gxp9NXbfTblfaPMC0fItwxWNy28GYkYXu9wr/BbI8BbWvo5AUKm8hT4S:HytzNXbNXhQ+28GYX3r/BFEvo5fEq+4U
MD5:	DA1820F2023CBA0621F8254315D73304
SHA1:	B4A80EE400DA24420B1D8FBDC347998609E2DAE2
SHA-256:	0BEC5D05261F1EEDF5D49ADAD928AF68D2020F77632F6641E88C1DBFCE7DD516
SHA-512:	A5D705E50FA467BD4631A527F488A60559F167181D72910B94BACBB9A8DBBA528A8E2EACFF180AEDC744BF4070B2FF63D11538F1F511CA5789DA4F4DA728C9C2
Malicious:	false
Preview:	....4.e.4..kk.4........kk.4.......4.mo..s....o..w.m.s}w....wu.........y.{..........w......4.e.4..kk.4........kk.4.......4B..y..w.{.y....4.e.4..kk.4........kk.4.......4'..)+.%!%../+./.....11)!....%.'..1#.3.).).%"%.+..3'..)+.%!%../+./.....11)!....%.'..1#.3.).).%"%.+..3'..)+.%!%../+./.....11)!....%.'..1#.3.).).%"%.+..3'..)+.%!%../+./.....11)!....%.'..1#.3.).).%"%.+..3'..)+.%!%../+./.....11)!....%.'..1#.3.).).%"%.+..3'..)+.%!%../+./.....11)!....%.'..1#.3.).).%"%.+..3'..)+.%!%../+./.....11)!....%.'..1#.3.).).%"%.+..3'..)+.%!%../+./.....11)!....%.'..1#.3.).).%"%.+..3'..)+.%!%../+./.....11)!....%.'..1#.3.).).%"%.+..3'..)+.%!%../+./.....11)!....%.'..1#.3.).).%"%.+..3'..)+.%!%../+./.....11)!....%.'..1#.3.).).%"%.+..3'..)+.%!%../+./.....11)!....%.'..1#.3.).).%"%.+..3'..)+.%!%../+./.....11)!....%.'..1#.3.).).%"%.+..3'..)+.%!%../+./.....11)!....%.'..1#.3.).).%"%.+..3'..)+.%!%../+.

C:\Users\Public\Libraries\Ndvmyrkf.exe

Process:	C:\Users\user\Desktop\Copie a bonului de plata.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	750592
Entropy (8bit):	6.8799839274072205
Encrypted:	false
SSDEEP:	12288:i1qMhtVLzLypCggIh36+O9dvjpQVeri4O2qKk/RqIkr:WFhHzmQgn6+8T/r7JaqI
MD5:	EB8C68C29D6131D6B903DD268D6FF0EF
SHA1:	61DFB557D2E792229060BDEB21285F65DAF48492
SHA-256:	D1798C288B296009D8049CA5364B29B079D59FADC870AF65E92FE5FA23BDCEC5
SHA-512:	077A05F65709382D70C1FED0836125854AE56802EB2BBFE3D3B1ECD1958F9F3C35DFAA8C91058BA6248B15E4BDD8C3A35AFF8D20F302996609B0D0CAE9B51F D
Malicious:	**true**
Antivirus:	- Antivirus: Avira, Detection: 100% - Antivirus: Joe Sandbox ML, Detection: 100% - Antivirus: ReversingLabs, Detection: 20%
Preview:	MZP....................@...!..L.!..This program must be run under Win32..$7..PE..L....^B*....................b.......&.......0....@...@.......................... ...%.......$..................p...n..........................`....................$'...............................text...,............................ ..`.itext..$.... ....`.data........0.....................@....bss....`6...............................idata...%... ...&..................@....tls....4....P..........................rdata.......`......................@..@.reloc...n...p...p.................@..B.rsrc....$.......$...N.............@..@.....................r..............@..@..

C:\Users\Public\Libraries\Ndvmyrkf.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\Copie a bonului de plata.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309

SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD6 E
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\Public\Libraries\fkrymvdN.url

Process:	C:\Users\user\Desktop\Copie a bonului de plata.exe
File Type:	MS Windows 95 Internet shortcut text (URL=<file:"C:\\Users\\Public\\Libraries\\Ndvmyrkf.exe">), ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	100
Entropy (8bit):	5.049624409749107
Encrypted:	false
SSDEEP:	3:HRAbABGQYmTWAX+rSF55i0XMBTTiysGKd9bvfAK:HRYFVmTWDyzmTTbsb9sK
MD5:	85066F050D1866BA30287E98DCC58140
SHA1:	750CA5CA86A51911268B2E8FD2E41C40E2B625B4
SHA-256:	F153472DC20C71C16BEF5ECE734331A061176ABF864F21108753E948F4B99ABF
SHA-512:	688A2E665AFEE3C6F4B3C71B44D927B23F350628EB64E07AB623CD8BB1695C9C9558BCCD0F6355ECCCA8141CE896A8D456DF04ABEC2A832A39A840ADA43C 01C
Malicious:	false
Yara Hits:	• Rule: Methodology_Shortcut_HotKey, Description: Detects possible shortcut usage for .URL persistence, Source: C:\Users\Public\Libraries\fkrymvdN.url, Author: @itsreallynick (Nick Carr) • Rule: Methodology_Contains_Shortcut_OtherURIhandlers, Description: Detects possible shortcut usage for .URL persistence, Source: C:\Users\Public\Libraries\fkrymvdN.url, Author: @itsreallynick (Nick Carr)
Preview:	[InternetShortcut]..URL=file:"C:\\Users\\Public\\Libraries\\Ndvmyrkf.exe"..IconIndex=57..HotKey=37..

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\Ndvmyrkfoxm[1]

Process:	C:\Users\user\Desktop\Copie a bonului de plata.exe
File Type:	data
Category:	dropped
Size (bytes):	189867
Entropy (8bit):	7.833666236780806
Encrypted:	false
SSDEEP:	3072:nB2d+y45Gxp9NXbfTblfaPMC0fltwxWNy28GYkYXu9wr/BbI8BbWvo5AUKm8hT4S:HytzNXbNXhQ+28GYX3r/BFEvo5fEq+4U
MD5:	DA1820F2023CBA0621F8254315D73304
SHA1:	B4A80EE400DA24420B1D8FBDC347998609E2DAE2
SHA-256:	0BEC5D05261F1EEDF5D49ADAD928AF68D2020F77632F6641E88C1DBFCE7DD516
SHA-512:	A5D705E50FA467BD4631A527F488A60559F167181D72910B94BACBB9A8DBBA528A8E2EACFF180AEDC744BF4070B2FF63D11538F1F511CA5789DA4F4DA728C9 C2
Malicious:	false
Preview:	....4.e.4..kk.4........kk.4.......4.mo..s....o..w.m.s}w....wu.........y.{..........w......4.e.4..kk.4........kk.4.......4B..y..w.{.y....4.e.4..kk.4........kk.4.......4'..)+.%!%../+./.....11)!....%.'..1#.3.).).%"%.+..3'..)+.%!%../+./.....11)!....%.'..1#.3.).).%"%.+..3'..)+.%!%../+./.....11)!....%.'..1#.3.).).%"%.+..3'..)+.%!%../+./.....11)!....%.'..1#.3.).).%"%.+..3'..)+.%!%../+./.....11)!....%.'..1#.3.).).%"%.+..3'..)+.%!%../+./.....11)!....%.'..1#.3.).).%"%.+..3'..)+.%!%../+./.....11)!....%.'..1#.3.).).%"%.+..3'..)+.%!%../+./.....11)!....%.'..1#.3.).).%"%.+..3'..)+.%!%../+./.....11)!....%.'..1#.3.).).%"%.+..3'..)+.%!%../+./.....11)!....%.'..1#.3.).).%"%.+..3'..)+.%!%../+./.....11)!....%.'..1#.3.).).%"%.+..3'..)+.%!%../+./.....11)!....%.'..1#.3.).).%"%.+..3'..)+.%!%../+./.....11)!....%.'..1#.3.).).%"%.+..3'..)+.%!%../+./.....11)!....%.'..1#.3.).).%"%.+..3'..)+.%!%../+./.....11)!....%.'..1#.3.).).%"%.+..3'..)+.%!%../+./.....11)!....%.'..1#.3.).).%"%.+..3'..)+.%!%../+.

C:\Users\user\AppData\Local\Temp\DB1

Process:	C:\Windows\SysWOW64\cmd.exe
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 2, database pages 23, cookie 0x19, schema 4, UTF-8, version-valid-for 2
Category:	dropped
Size (bytes):	49152
Entropy (8bit):	0.7876734657715041
Encrypted:	false
SSDEEP:	48:43KzOIIY3HzrkNSs8LKvUf9KnmlG0UX9q4lCm+KLka+yJqhM0ObVEq8Ma0D0HOlx:Sq0NFeymDlGD9qlm+KL2y0Obn8MouO
MD5:	CF7758A2FF4A94A5D589DEBAED38F82E
SHA1:	D3380E70D0CAEB9AD78D14DD970EA480E08232B8
SHA-256:	6CA783B84D01BFCF9AA7185D7857401D336BAD407A182345B97096E1F2502B7F
SHA-512:	1D0C49B02A159EEB4AA971980CCA02751973E249422A71A0587EE63986A4A0EB8929458BCC575A9898CE3497CC5BDFB7050DF33DF53F5C88D110F386A0804C F
Malicious:	**true**

Preview:	SQLite format 3......@ ....[5.. ....

C:\Users\user\AppData\Roaming\9N30RODQ\9N3logim.jpeg	
Process:	C:\Windows\SysWOW64\raserver.exe
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 96x96, segment length 16, baseline, precision 8, 1280x1024, components 3
Category:	dropped
Size (bytes):	92472
Entropy (8bit):	7.902093016473941
Encrypted:	false
SSDEEP:	1536:CCZLHVw9ZbCsdphPEYcJ7I4dWv3AGwqLpeKAk8KqbP4vlapwDOzzz29syF625N98:3Rw9ldbncJlvpwqL7KKmhvzzz295U2S
MD5:	D01609AB857EFA37ABA10FB4F3A23A87
SHA1:	F4F43737962C5C7E2DEE4E45632B088F911D2A50
SHA-256:	7DD08CD44AB64552BFE79A54E20E20AA108E6ED547446A522A836DC9882304F0
SHA-512:	2AA66E428BADE8CBC611566A02B5BF490873C18AD434F9876BFE2977CD2773D761645CF812B383838C10C2B1D18B89F45B9E59C502C6399B25F5E9D5CAE7A9E 5
Malicious:	false
Preview:	......JFIF.....`.`.....C.................................. $.' ",#..(7),01444.'9=82<.342...C...........2!.!22222222222222222222222222222222222222222222222222...........".................... ....}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.. ....w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz... ....?..01KK...lq\....xcS.m..#Hm.....T......<!...wq5...v1.?S.....rHj-.U:...5............\|..+.......}...<.>...H.......Wo.CK`/l.1./...C...W.....,1....R.0.W.M.!.l7.~S....."SW.^..c......^s........u,- n....A..?.2.....l.(.?....7..~.q$.f..1\.q[.....oS:.gOY".....f-%.P.b.Z....>.....4+..b.Y&..F...)Pq.L....... .....H.#.|..).?.H.'.|....).?m.....h.t......|4.%...d....

C:\Users\user\AppData\Roaming\9N30RODQ\9N3logrg.ini	
Process:	C:\Windows\SysWOW64\raserver.exe
File Type:	Targa image data - RGB - RLE 109 x 101 x 32 +114 +111 "R"
Category:	dropped
Size (bytes):	38
Entropy (8bit):	2.7883088224543333
Encrypted:	false
SSDEEP:	3:rFGQJhIl:RGQPY
MD5:	4AADF49FED30E4C9B3FE4A3DD6445EBE
SHA1:	1E332822167C6F351B99615EADA2C30A538FF037
SHA-256:	75034BEB7BDED9AEAB5748F4592B9E1419256CAEC474065D43E531EC5CC21C56
SHA-512:	EB5B3908D5E7B43BA02165E092F05578F45F15A148B4C3769036AA542C23A0F7CD2BC2770CF4119A7E437DE3F681D9E398511F69F66824C516D9B451BB95F945
Malicious:	false
Preview:	....C.h.r.o.m.e. .R.e.c.o.v.e.r.y.....

C:\Users\user\AppData\Roaming\9N30RODQ\9N3logri.ini	
Process:	C:\Windows\SysWOW64\raserver.exe
File Type:	data
Category:	dropped
Size (bytes):	40
Entropy (8bit):	2.8420918598895937
Encrypted:	false
SSDEEP:	3:+slXllAGQJhIl:dlIGQPY
MD5:	D63A82E5D81E02E399090AF26DB0B9CB
SHA1:	91D0014C8F54743BBA141FD60C9D963F869D76C9
SHA-256:	EAECE2EBA6310253249603033C744DD5914089B0BB26BDE6685EC9813611BAAE
SHA-512:	38AFB05016D8F3C69D246321573997AAAC8A51C34E61749A02BF5E8B2B56B94D9544D65801511044E1495906A86DC2100F2E20FF4FCBED09E01904CC780FDBAI
Malicious:	**true**
Preview:	....I.e.x.p.l.o.r. .R.e.c.o.v.e.r.y.....

C:\Users\user\AppData\Roaming\9N30RODQ\9N3logrv.ini	
Process:	C:\Windows\SysWOW64\raserver.exe
File Type:	data
Category:	dropped
Size (bytes):	40

Entropy (8bit):	2.96096404744368
Encrypted:	false
SSDEEP:	3:AJlbeGQJhII:tGQPY
MD5:	BA3B6BC807D4F76794C4B81B09BB9BA5
SHA1:	24CB89501F0212FF3095ECC0ABA97DD563718FB1
SHA-256:	6EEBF968962745B2E9DE2CA969AF7C424916D4E3FE3CC0BB9B3D414ABFCE9507
SHA-512:	ECD07E601FC9E3CFC39ADDD7BD6F3D7F7FF3253AFB40BF536E9EAAC5A4C243E5EC40FBFD7B216CB0EA29F2517419601E335E33BA19DEA4A46F65E38694D46 5BF
Malicious:	**true**
Preview:	...._._.V.a.u.l.t. .R.e.c.o.v.e.r.y.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.8799839274072205
TrID:	• Win32 Executable (generic) a (10002005/4) 99.38% • InstallShield setup (43055/19) 0.43% • Windows Screen Saver (13104/52) 0.13% • Win16/32 Executable Delphi generic (2074/23) 0.02% • Generic Win/DOS Executable (2004/3) 0.02%
File name:	Copie a bonului de plata.exe
File size:	750592
MD5:	eb8c68c29d6131d6b903dd268d6ff0ef
SHA1:	61dfb557d2e792229060bdeb21285f65daf48492
SHA256:	d1798c288b296009d8049ca5364b29b079d59fadc870af65e92fe5fa23bdcec5
SHA512:	077a05f65709382d70c1fed0836125854ae56802eb2bbfe3d3b1ecd1958f9f3c35dfaa8c91058ba6248b15e4bdd8c3a35aff8d20f302996609b0d0cae9b51fad
SSDEEP:	12288:i1qMhtVLzLypCgglh36+O9dvjpQVeri4O2qKk/RqIkr:WFhHzmQgn6+8T/r7Jaql
TLSH:	48F47D6771E04633D0262535DC5BA7A8692FBEE02F14B8562BE03DDC1F783CA742916B
File Content Preview:	MZP.....@.....!..L.!..This program must be run under Win32..$7.....

File Icon

Icon Hash:	2321270727090923

Static PE Info

General

Entrypoint:	0x4626e8
Entrypoint Section:	.itext
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, BYTES_REVERSED_LO, 32BIT_MACHINE, BYTES_REVERSED_HI
DLL Characteristics:	
Time Stamp:	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	5a047051636dce23e36a7dceaf1507c0

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
add esp, FFFFFFF0h
mov eax, 0046105Ch
call 00007FA2049FCBF5h
mov ecx, dword ptr [0046D410h]
mov eax, dword ptr [0046D324h]
mov eax, dword ptr [eax]
mov edx, dword ptr [00460A90h]
call 00007FA204A4F5CDh
mov eax, dword ptr [0046D324h]
mov eax, dword ptr [eax]
call 00007FA204A4F641h
call 00007FA2049FACF8h
lea eax, dword ptr [eax+00h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x72000	0x25ac	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x7e000	0x42400	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x77000	0x6eec	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x76000	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x72724	0x5e4	.idata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6022c	0x60400	False	0.5191025771103897	data	6.531038724700122	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.itext	0x62000	0x724	0x800	False	0.57373046875	data	5.847823102407548	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.data	0x63000	0xa49c	0xa600	False	0.08553746234939759	data	6.4911792818920375	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.bss	0x6e000	0x3660	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.idata	0x72000	0x25ac	0x2600	False	0.32452713815789475	data	5.139331879404015	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.tls	0x75000	0x34	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.rdata	0x76000	0x18	0x200	False	0.05078125	data	0.2108262677871819	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x77000	0x6eec	0x7000	False	0.6196986607142857	data	6.6810323966616	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0x7e000	0x42400	0x42400	False	0.4435620577830189	data	6.403601787519998	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0x7ef0c	0x134	Targa image data - Map 64 x 65536 x 1 +32 "\001"	English	United States
RT_CURSOR	0x7f040	0x134	data	English	United States
RT_CURSOR	0x7f174	0x134	data	English	United States
RT_CURSOR	0x7f2a8	0x134	data	English	United States
RT_CURSOR	0x7f3dc	0x134	data	English	United States
RT_CURSOR	0x7f510	0x134	data	English	United States
RT_CURSOR	0x7f644	0x134	Targa image data - RGB 64 x 65536 x 1 +32 "\001"	English	United States
RT_BITMAP	0x7f778	0x128	Device independent bitmap graphic, 21 x 16 x 4, image size 192	English	United States
RT_BITMAP	0x7f8a0	0x128	Device independent bitmap graphic, 19 x 16 x 4, image size 192	English	United States
RT_BITMAP	0x7f9c8	0x128	Device independent bitmap graphic, 21 x 16 x 4, image size 192	English	United States
RT_BITMAP	0x7faf0	0xe8	Device independent bitmap graphic, 13 x 16 x 4, image size 128	English	United States
RT_BITMAP	0x7fbd8	0x128	Device independent bitmap graphic, 17 x 16 x 4, image size 192	English	United States
RT_BITMAP	0x7fd00	0x128	Device independent bitmap graphic, 20 x 16 x 4, image size 192	English	United States
RT_BITMAP	0x7fe28	0xd0	Device independent bitmap graphic, 13 x 13 x 4, image size 104	English	United States
RT_BITMAP	0x7fef8	0x128	Device independent bitmap graphic, 21 x 16 x 4, image size 192	English	United States
RT_BITMAP	0x80020	0x128	Device independent bitmap graphic, 17 x 16 x 4, image size 192	English	United States
RT_BITMAP	0x80148	0x128	Device independent bitmap graphic, 21 x 16 x 4, image size 192	English	United States
RT_BITMAP	0x80270	0x128	Device independent bitmap graphic, 19 x 16 x 4, image size 192	English	United States
RT_BITMAP	0x80398	0x128	Device independent bitmap graphic, 21 x 16 x 4, image size 192	English	United States
RT_BITMAP	0x804c0	0xe8	Device independent bitmap graphic, 12 x 16 x 4, image size 128	English	United States
RT_BITMAP	0x805a8	0x128	Device independent bitmap graphic, 17 x 16 x 4, image size 192	English	United States
RT_BITMAP	0x806d0	0x128	Device independent bitmap graphic, 20 x 16 x 4, image size 192	English	United States
RT_BITMAP	0x807f8	0xd0	Device independent bitmap graphic, 13 x 13 x 4, image size 104	English	United States
RT_BITMAP	0x808c8	0x128	Device independent bitmap graphic, 21 x 16 x 4, image size 192	English	United States
RT_BITMAP	0x809f0	0x128	Device independent bitmap graphic, 17 x 16 x 4, image size 192	English	United States
RT_BITMAP	0x80b18	0x128	Device independent bitmap graphic, 21 x 16 x 4, image size 192	English	United States
RT_BITMAP	0x80c40	0x128	Device independent bitmap graphic, 19 x 16 x 4, image size 192	English	United States

Copyright Joe Security LLC 2022

Name	RVA	Size	Type	Language	Country
RT_BITMAP	0x80d68	0x128	Device independent bitmap graphic, 21 x 16 x 4, image size 192	English	United States
RT_BITMAP	0x80e90	0xe8	Device independent bitmap graphic, 13 x 16 x 4, image size 128	English	United States
RT_BITMAP	0x80f78	0x128	Device independent bitmap graphic, 17 x 16 x 4, image size 192	English	United States
RT_BITMAP	0x810a0	0x128	Device independent bitmap graphic, 20 x 16 x 4, image size 192	English	United States
RT_BITMAP	0x811c8	0xd0	Device independent bitmap graphic, 13 x 13 x 4, image size 104	English	United States
RT_BITMAP	0x81298	0x128	Device independent bitmap graphic, 21 x 16 x 4, image size 192	English	United States
RT_BITMAP	0x813c0	0x128	Device independent bitmap graphic, 17 x 16 x 4, image size 192	English	United States
RT_ICON	0x814e8	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096		
RT_ICON	0x82590	0x25a8	Device independent bitmap graphic, 48 x 96 x 32, image size 9216		
RT_ICON	0x84b38	0x5488	Device independent bitmap graphic, 72 x 144 x 32, image size 20736		
RT_ICON	0x89fc0	0x94a8	Device independent bitmap graphic, 96 x 192 x 32, image size 36864		
RT_STRING	0x93468	0x200	data		
RT_STRING	0x93668	0x188	data		
RT_STRING	0x937f0	0xc8	data		
RT_STRING	0x938b8	0x350	data		
RT_STRING	0x93c08	0x3d8	data		
RT_STRING	0x93fe0	0x388	data		
RT_STRING	0x94368	0x418	data		
RT_STRING	0x94780	0x140	data		
RT_STRING	0x948c0	0xcc	data		
RT_STRING	0x9498c	0x1ec	data		
RT_STRING	0x94b78	0x3b0	data		
RT_STRING	0x94f28	0x354	data		
RT_STRING	0x9527c	0x2a4	data		
RT_RCDATA	0x95520	0x10	data		
RT_RCDATA	0x95530	0x2a7c2	GIF image data, version 89a, 300 x 168	English	United States
RT_RCDATA	0xbfcf4	0x254	data		
RT_RCDATA	0xbff48	0x3e0	Delphi compiled form 'TForm1'		
RT_GROUP_CURSOR	0xc0328	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xc033c	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xc0350	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xc0364	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xc0378	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xc038c	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_CURSOR	0xc03a0	0x14	Lotus unknown worksheet or configuration, revision 0x1	English	United States
RT_GROUP_ICON	0xc03b4	0x3e	data		

Imports

DLL	Import
oleaut32.dll	SysFreeString, SysReAllocStringLen, SysAllocStringLen
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey
user32.dll	GetKeyboardType, DestroyWindow, LoadStringA, MessageBoxA, CharNextA
kernel32.dll	GetACP, Sleep, VirtualFree, VirtualAlloc, GetCurrentThreadId, InterlockedDecrement, InterlockedIncrement, VirtualQuery, WideCharToMultiByte, MultiByteToWideChar, lstrlenA, lstrcpynA, LoadLibraryExA, GetThreadLocale, GetStartupInfoA, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetCommandLineA, FreeLibrary, FindFirstFileA, FindClose, ExitProcess, CompareStringA, WriteFile, UnhandledExceptionFilter, RtlUnwind, RaiseException, GetStdHandle
kernel32.dll	TlsSetValue, TlsGetValue, LocalAlloc, GetModuleHandleA

Copyright Joe Security LLC 2022

DLL	Import
user32.dll	CreateWindowExA, WindowFromPoint, WaitMessage, UpdateWindow, UnregisterClassA, UnhookWindowsHookEx, TranslateMessage, TranslateMDISysAccel, TrackPopupMenu, SystemParametersInfoA, ShowWindow, ShowScrollBar, ShowOwnedPopups, SetWindowsHookExA, SetWindowPos, SetWindowPlacement, SetWindowLongW, SetWindowLongA, SetTimer, SetScrollRange, SetScrollPos, SetScrollInfo, SetRect, SetPropA, SetParent, SetMenuItemInfoA, SetMenu, SetForegroundWindow, SetFocus, SetCursor, SetClassLongA, SetCapture, SetActiveWindow, SendMessageW, SendMessageA, ScrollWindow, ScreenToClient, RemovePropA, RemoveMenu, ReleaseDC, ReleaseCapture, RegisterWindowMessageA, RegisterClipboardFormatA, RegisterClassA, RedrawWindow, PtInRect, PostQuitMessage, PostMessageA, PeekMessageW, PeekMessageA, OffsetRect, OemToCharA, MessageBoxA, MapWindowPoints, MapVirtualKeyA, LoadStringA, LoadKeyboardLayoutA, LoadIconA, LoadCursorA, LoadBitmapA, KillTimer, IsZoomed, IsWindowVisible, IsWindowUnicode, IsWindowEnabled, IsWindow, IsRectEmpty, IsIconic, IsDialogMessageW, IsDialogMessageA, IsChild, InvalidateRect, IntersectRect, InsertMenuItemA, InsertMenuA, InflateRect, GetWindowThreadProcessId, GetWindowTextA, GetWindowRect, GetWindowPlacement, GetWindowLongW, GetWindowLongA, GetWindowDC, GetTopWindow, GetSystemMetrics, GetSystemMenu, GetSysColorBrush, GetSysColor, GetSubMenu, GetScrollRange, GetScrollPos, GetScrollInfo, GetPropA, GetParent, GetWindow, GetMessagePos, GetMenuStringA, GetMenuState, GetMenuItemInfoA, GetMenuItemID, GetMenuItemCount, GetMenu, GetLastActivePopup, GetKeyboardState, GetKeyboardLayoutNameA, GetKeyboardLayoutList, GetKeyboardLayout, GetKeyState, GetKeyNameTextA, GetIconInfo, GetForegroundWindow, GetFocus, GetDlgItem, GetDesktopWindow, GetDCEx, GetDC, GetCursorPos, GetCursor, GetClientRect, GetClassLongA, GetClassInfoA, GetCapture, GetActiveWindow, FrameRect, FindWindowA, FillRect, EqualRect, EnumWindows, EnumThreadWindows, EnumChildWindows, EndPaint, EnableWindow, EnableScrollBar, EnableMenuItem, DrawTextA, DrawMenuBar, DrawIconEx, DrawIcon, DrawFrameControl, DrawFocusRect, DrawEdge, DispatchMessageW, DispatchMessageA, DestroyWindow, DestroyMenu, DestroyIcon, DestroyCursor, DeleteMenu, DefWindowProcA, DefMDIChildProcA, DefFrameProcA, CreatePopupMenu, CreateMenu, CreateIcon, ClientToScreen, CheckMenuItem, CallWindowProcA, CallNextHookEx, BeginPaint, CharNextA, CharLowerA, CharToOemA, AdjustWindowRectEx, ActivateKeyboardLayout
gdi32.dll	UnrealizeObject, StretchBlt, SetWindowOrgEx, SetViewportOrgEx, SetTextColor, SetStretchBltMode, SetROP2, SetPixel, SetDIBColorTable, SetBrushOrgEx, SetBkMode, SetBkColor, SelectPalette, SelectObject, SaveDC, RestoreDC, RectVisible, RealizePalette, Polyline, PatBlt, MoveToEx, MaskBlt, LineTo, IntersectClipRect, GetWindowOrgEx, GetTextMetricsA, GetTextExtentPoint32A, GetSystemPaletteEntries, GetStockObject, GetRgnBox, GetPixel, GetPaletteEntries, GetObjectA, GetDeviceCaps, GetDIBits, GetDIBColorTable, GetDCOrgEx, GetCurrentPositionEx, GetClipBox, GetBrushOrgEx, GetBitmapBits, ExcludeClipRect, DeleteObject, DeleteDC, CreateSolidBrush, CreatePenIndirect, CreatePalette, CreateHalftonePalette, CreateFontIndirectA, CreateDIBitmap, CreateDIBSection, CreateCompatibleDC, CreateCompatibleBitmap, CreateBrushIndirect, CreateBitmap, BitBlt
version.dll	VerQueryValueA, GetFileVersionInfoSizeA, GetFileVersionInfoA
kernel32.dll	lstrcpyA, lstrcatA, _lread, _lopen, _llseek, _lclose, WriteFile, WaitForSingleObject, VirtualQuery, VirtualProtect, VirtualAlloc, SizeofResource, SetThreadLocale, SetFilePointer, SetEvent, SetErrorMode, SetEndOfFile, ResetEvent, ReadFile, MulDiv, LockResource, LoadResource, LoadLibraryA, LeaveCriticalSection, InitializeCriticalSection, GlobalFindAtomA, GlobalDeleteAtom, GlobalAddAtomA, GetVersionExA, GetVersion, GetTickCount, GetThreadLocale, GetStdHandle, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetLocalTime, GetLastError, GetFullPathNameA, GetDiskFreeSpaceA, GetDateFormatA, GetCurrentThreadId, GetCurrentProcessId, GetCPInfo, FreeResource, InterlockedExchange, FreeLibrary, FormatMessageA, FindResourceA, EnumCalendarInfoA, EnterCriticalSection, DeleteCriticalSection, CreateThread, CreateFileA, CreateEventA, CompareStringA, CloseHandle
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegFlushKey, RegCloseKey, IsValidSid
kernel32.dll	Sleep
oleaut32.dll	SafeArrayPtrOfIndex, SafeArrayGetUBound, SafeArrayGetLBound, SafeArrayCreate, VariantChangeType, VariantCopy, VariantClear, VariantInit
comctl32.dll	_TrackMouseEvent, ImageList_SetIconSize, ImageList_GetIconSize, ImageList_Write, ImageList_Read, ImageList_DragShowNolock, ImageList_DragMove, ImageList_DragLeave, ImageList_DragEnter, ImageList_EndDrag, ImageList_BeginDrag, ImageList_Remove, ImageList_DrawEx, ImageList_Draw, ImageList_GetBkColor, ImageList_SetBkColor, ImageList_Add, ImageList_GetImageCount, ImageList_Destroy, ImageList_Create
comdlg32.dll	GetOpenFileNameA
URL	AutodialHookCallback

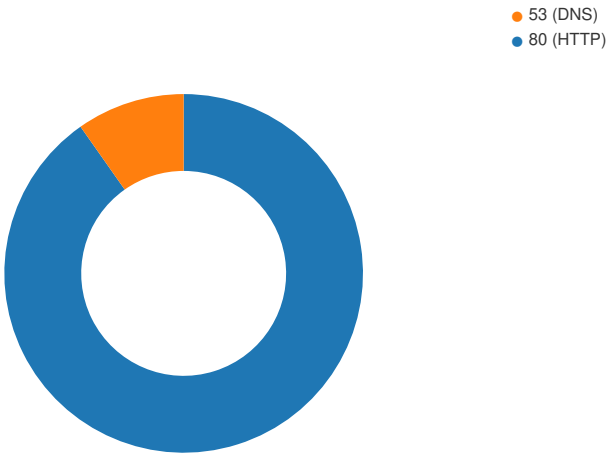
Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Network Port Distribution

Total Packets: 41



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 12:49:31.618283033 CET	49721	80	192.168.2.6	5.183.8.25
Nov 29, 2022 12:49:31.740262985 CET	80	49721	5.183.8.25	192.168.2.6
Nov 29, 2022 12:49:31.741211891 CET	49721	80	192.168.2.6	5.183.8.25
Nov 29, 2022 12:49:31.741300106 CET	49721	80	192.168.2.6	5.183.8.25
Nov 29, 2022 12:49:31.871023893 CET	80	49721	5.183.8.25	192.168.2.6
Nov 29, 2022 12:49:31.947927952 CET	80	49721	5.183.8.25	192.168.2.6
Nov 29, 2022 12:49:31.948004961 CET	80	49721	5.183.8.25	192.168.2.6
Nov 29, 2022 12:49:31.948185921 CET	49721	80	192.168.2.6	5.183.8.25
Nov 29, 2022 12:49:31.948242903 CET	49721	80	192.168.2.6	5.183.8.25
Nov 29, 2022 12:49:32.070991039 CET	80	49721	5.183.8.25	192.168.2.6
Nov 29, 2022 12:49:34.019376040 CET	49722	80	192.168.2.6	5.183.8.25
Nov 29, 2022 12:49:34.143007040 CET	80	49722	5.183.8.25	192.168.2.6
Nov 29, 2022 12:49:34.143212080 CET	49722	80	192.168.2.6	5.183.8.25
Nov 29, 2022 12:49:34.146193027 CET	49722	80	192.168.2.6	5.183.8.25
Nov 29, 2022 12:49:34.268577099 CET	80	49722	5.183.8.25	192.168.2.6
Nov 29, 2022 12:49:34.268805027 CET	49722	80	192.168.2.6	5.183.8.25
Nov 29, 2022 12:49:34.392867088 CET	80	49722	5.183.8.25	192.168.2.6
Nov 29, 2022 12:49:34.392991066 CET	49722	80	192.168.2.6	5.183.8.25
Nov 29, 2022 12:49:34.393543959 CET	80	49722	5.183.8.25	192.168.2.6
Nov 29, 2022 12:49:34.393878937 CET	49722	80	192.168.2.6	5.183.8.25
Nov 29, 2022 12:49:34.394963026 CET	80	49722	5.183.8.25	192.168.2.6
Nov 29, 2022 12:49:34.395057917 CET	49722	80	192.168.2.6	5.183.8.25
Nov 29, 2022 12:49:34.516290903 CET	80	49722	5.183.8.25	192.168.2.6
Nov 29, 2022 12:49:34.516545057 CET	49722	80	192.168.2.6	5.183.8.25
Nov 29, 2022 12:49:34.517843008 CET	80	49722	5.183.8.25	192.168.2.6
Nov 29, 2022 12:49:34.517870903 CET	80	49722	5.183.8.25	192.168.2.6
Nov 29, 2022 12:49:34.518026114 CET	49722	80	192.168.2.6	5.183.8.25
Nov 29, 2022 12:49:34.518452883 CET	80	49722	5.183.8.25	192.168.2.6
Nov 29, 2022 12:49:34.518476963 CET	80	49722	5.183.8.25	192.168.2.6
Nov 29, 2022 12:49:34.518580914 CET	49722	80	192.168.2.6	5.183.8.25
Nov 29, 2022 12:49:34.640245914 CET	80	49722	5.183.8.25	192.168.2.6
Nov 29, 2022 12:49:34.640320063 CET	80	49722	5.183.8.25	192.168.2.6
Nov 29, 2022 12:49:34.640342951 CET	80	49722	5.183.8.25	192.168.2.6
Nov 29, 2022 12:49:34.640482903 CET	49722	80	192.168.2.6	5.183.8.25
Nov 29, 2022 12:49:34.640957117 CET	80	49722	5.183.8.25	192.168.2.6
Nov 29, 2022 12:49:34.640971899 CET	80	49722	5.183.8.25	192.168.2.6
Nov 29, 2022 12:49:34.642323971 CET	80	49722	5.183.8.25	192.168.2.6
Nov 29, 2022 12:49:34.642950058 CET	80	49722	5.183.8.25	192.168.2.6
Nov 29, 2022 12:49:34.643400908 CET	80	49722	5.183.8.25	192.168.2.6
Nov 29, 2022 12:49:34.644447088 CET	80	49722	5.183.8.25	192.168.2.6
Nov 29, 2022 12:49:34.644464016 CET	80	49722	5.183.8.25	192.168.2.6

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 12:49:34.763107061 CET	80	49722	5.183.8.25	192.168.2.6
Nov 29, 2022 12:49:34.803478003 CET	80	49722	5.183.8.25	192.168.2.6
Nov 29, 2022 12:49:34.903083086 CET	80	49722	5.183.8.25	192.168.2.6
Nov 29, 2022 12:49:34.903107882 CET	80	49722	5.183.8.25	192.168.2.6
Nov 29, 2022 12:49:34.903337955 CET	49722	80	192.168.2.6	5.183.8.25
Nov 29, 2022 12:49:34.903377056 CET	49722	80	192.168.2.6	5.183.8.25
Nov 29, 2022 12:49:52.364892006 CET	49724	80	192.168.2.6	212.32.237.90
Nov 29, 2022 12:49:52.390316963 CET	80	49724	212.32.237.90	192.168.2.6
Nov 29, 2022 12:49:52.390595913 CET	49724	80	192.168.2.6	212.32.237.90
Nov 29, 2022 12:49:52.390693903 CET	49724	80	192.168.2.6	212.32.237.90
Nov 29, 2022 12:49:52.416079998 CET	80	49724	212.32.237.90	192.168.2.6
Nov 29, 2022 12:49:52.436357975 CET	80	49724	212.32.237.90	192.168.2.6
Nov 29, 2022 12:49:52.436377048 CET	80	49724	212.32.237.90	192.168.2.6
Nov 29, 2022 12:49:52.436654091 CET	49724	80	192.168.2.6	212.32.237.90
Nov 29, 2022 12:49:52.436655045 CET	49724	80	192.168.2.6	212.32.237.90
Nov 29, 2022 12:49:52.462446928 CET	80	49724	212.32.237.90	192.168.2.6
Nov 29, 2022 12:49:54.440421104 CET	49725	80	192.168.2.6	212.32.237.90
Nov 29, 2022 12:49:54.465629101 CET	80	49725	212.32.237.90	192.168.2.6
Nov 29, 2022 12:49:54.465823889 CET	49725	80	192.168.2.6	212.32.237.90
Nov 29, 2022 12:49:54.468302011 CET	49725	80	192.168.2.6	212.32.237.90
Nov 29, 2022 12:49:54.493021965 CET	80	49725	212.32.237.90	192.168.2.6
Nov 29, 2022 12:49:54.493052959 CET	80	49725	212.32.237.90	192.168.2.6
Nov 29, 2022 12:49:54.493073940 CET	80	49725	212.32.237.90	192.168.2.6
Nov 29, 2022 12:49:54.493140936 CET	49725	80	192.168.2.6	212.32.237.90
Nov 29, 2022 12:49:54.493207932 CET	80	49725	212.32.237.90	192.168.2.6
Nov 29, 2022 12:49:54.493293047 CET	49725	80	192.168.2.6	212.32.237.90
Nov 29, 2022 12:49:54.493347883 CET	49725	80	192.168.2.6	212.32.237.90
Nov 29, 2022 12:49:54.503956079 CET	80	49725	212.32.237.90	192.168.2.6
Nov 29, 2022 12:49:54.504040003 CET	49725	80	192.168.2.6	212.32.237.90
Nov 29, 2022 12:49:54.504345894 CET	80	49725	212.32.237.90	192.168.2.6
Nov 29, 2022 12:49:54.504422903 CET	49725	80	192.168.2.6	212.32.237.90
Nov 29, 2022 12:49:54.518055916 CET	80	49725	212.32.237.90	192.168.2.6
Nov 29, 2022 12:49:54.518148899 CET	49725	80	192.168.2.6	212.32.237.90
Nov 29, 2022 12:49:54.518177986 CET	80	49725	212.32.237.90	192.168.2.6
Nov 29, 2022 12:49:54.518209934 CET	80	49725	212.32.237.90	192.168.2.6
Nov 29, 2022 12:49:54.518248081 CET	49725	80	192.168.2.6	212.32.237.90
Nov 29, 2022 12:49:54.518273115 CET	80	49725	212.32.237.90	192.168.2.6
Nov 29, 2022 12:49:54.518336058 CET	49725	80	192.168.2.6	212.32.237.90
Nov 29, 2022 12:49:54.518404007 CET	80	49725	212.32.237.90	192.168.2.6
Nov 29, 2022 12:49:54.518462896 CET	49725	80	192.168.2.6	212.32.237.90
Nov 29, 2022 12:49:54.518464088 CET	49725	80	192.168.2.6	212.32.237.90
Nov 29, 2022 12:49:54.518980980 CET	80	49725	212.32.237.90	192.168.2.6
Nov 29, 2022 12:49:54.519053936 CET	49725	80	192.168.2.6	212.32.237.90

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 12:48:04.529771090 CET	56331	53	192.168.2.6	8.8.8.8
Nov 29, 2022 12:48:05.730691910 CET	50506	53	192.168.2.6	8.8.8.8
Nov 29, 2022 12:49:31.579010963 CET	54903	53	192.168.2.6	8.8.8.8
Nov 29, 2022 12:49:31.611258984 CET	53	54903	8.8.8.8	192.168.2.6
Nov 29, 2022 12:49:52.314426899 CET	56122	53	192.168.2.6	8.8.8.8
Nov 29, 2022 12:49:52.363502979 CET	53	56122	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 12:48:04.529771090 CET	192.168.2.6	8.8.8.8	0xe7f6	Standard query (0)	onedrive.live.com	A (IP address)	IN (0x0001)	false

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 12:48:05.730691910 CET	192.168.2.6	8.8.8.8	0xf118	Standard query (0)	ppq0oq.ph.files.1drv.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 12:49:31.579010963 CET	192.168.2.6	8.8.8.8	0x77	Standard query (0)	www.jam-nins.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 12:49:52.314426899 CET	192.168.2.6	8.8.8.8	0x6c7a	Standard query (0)	www.stillwatersagawork.com	A (IP address)	IN (0x0001)	false

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 12:48:04.579268932 CET	8.8.8.8	192.168.2.6	0xe7f6	No error (0)	onedrive.live.com	odc-web-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 12:48:05.779105902 CET	8.8.8.8	192.168.2.6	0xf118	No error (0)	ppq0oq.ph.files.1drv.com	ph-files.fe.1drv.com		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 12:48:05.779105902 CET	8.8.8.8	192.168.2.6	0xf118	No error (0)	ph-files.fe.1drv.com	odc-ph-files-geo.onedrive.akadns.net		CNAME (Canonical name)	IN (0x0001)	false
Nov 29, 2022 12:49:31.611258984 CET	8.8.8.8	192.168.2.6	0x77	No error (0)	www.jam-nins.com		5.183.8.25	A (IP address)	IN (0x0001)	false
Nov 29, 2022 12:49:52.363502979 CET	8.8.8.8	192.168.2.6	0x6c7a	No error (0)	www.stillwatersagawork.com		212.32.237.90	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- www.jam-nins.com
- www.stillwatersagawork.com

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

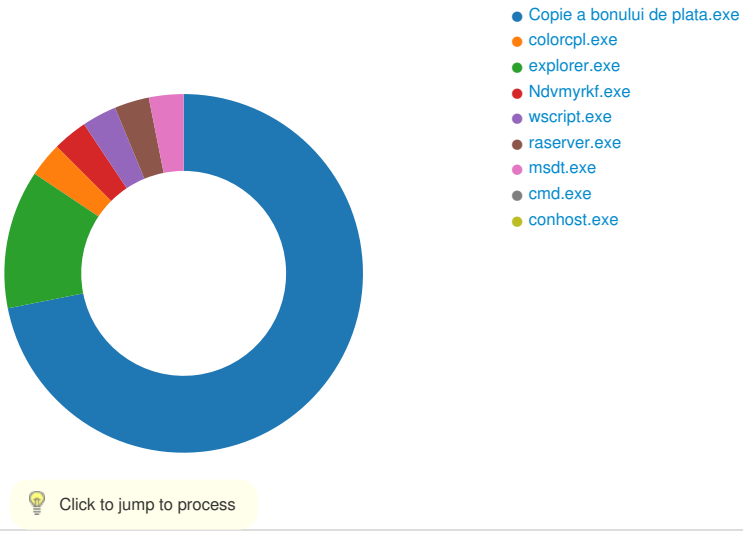
Process: explorer.exe, Module: user32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x82 0x2E 0xEF
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x8A 0xAE 0xEF
GetMessageW	INLINE	0x48 0x8B 0xB8 0x8A 0xAE 0xEF
GetMessageA	INLINE	0x48 0x8B 0xB8 0x82 0x2E 0xEF

Statistics

Behavior

Copyright Joe Security LLC 2022



System Behavior

Analysis Process: Copie a bonului de plata.exe PID: 5152, Parent PID: 3452

General

Target ID:	0
Start time:	12:48:00
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\Copie a bonului de plata.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Copie a bonului de plata.exe
Imagebase:	0x400000
File size:	750592 bytes
MD5 hash:	EB8C68C29D6131D6B903DD268D6FF0EF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000002.262570610.0000000002320000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.265578930.0000000004B07000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000000.00000002.265578930.0000000004B07000.00000004.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.265578930.0000000004B07000.00000004.00001000.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.265578930.0000000004B07000.00000004.00001000.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.265182733.0000000004A77000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000000.00000002.265182733.0000000004A77000.00000004.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.265182733.0000000004A77000.00000004.00001000.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.265182733.0000000004A77000.00000004.00001000.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_DBatLoader, Description: Yara detected DBatLoader, Source: 00000000.00000002.263522793.0000000002A4E000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	22C8D40	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	22C8D40	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	22C8D40	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	22C8D40	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	22C8D40	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	22C8D40	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	22C8D40	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	22C8D40	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	22C8D40	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	22C8D40	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	22C8D40	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\History	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	22C8D40	InternetOpenUrlA
C:\Users\Public\Libraries\Ndvmyrkf	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	22C89E0	_lcreat

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\Public\Libraries\Ndvmyrkf.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	22CB37E	CopyFileA
C:\Users\Public\Libraries\Ndvmyrkf.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	22CB37E	CopyFileA
C:\Users\Public\Libraries\fkrymvdN.url	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file	success or wait	1	22C2AB9	CreateFileA

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\Ndvmyrkfoxm[1]	0	1025	1e 1c fd fd 34 fd 65 fd 34 fd fd 6b 6b fd 34 fd 18 fd fd 1a 1e 1c fd 6b 6b fd 34 18 fd fd fd 18 fd fd 34 02 6d 6f 04 06 73 00 fd 00 fd 6f 0a 06 77 0a 6d fd 73 7d 77 0c 0c 04 fd 77 75 7f fd 00 fd 02 fd fd 0c fd 79 0e 7b 04 fd 04 fd 00 02 02 00 fd 06 77 fd 0e 1e 1c fd fd 34 fd 65 fd 34 fd fd 6b 6b fd 34 fd 18 fd fd 1a 1e 1c fd 6b 6b fd 34 18 fd fd fd 18 fd fd 34 42 fd 0c 79 fd 08 77 fd 7b 0e 79 1e 1c fd fd 34 fd 65 fd 34 fd fd 6b 6b fd 34 fd 18 fd fd 1a 1e 1c fd 6b 6b fd 34 18 fd fd fd 18 fd fd 34 27 fd fd 29 2b fd 25 21 25 fd fd 2f 2b fd 2f fd fd fd fd fd 31 31 29 21 fd fd fd 1d 25 fd 27 fd 1d 31 23 fd 33 fd 29 fd 29 fd 25 27 27 25 fd 2b fd fd 33 27 fd fd 29 2b fd 25 21 25 fd fd 2f 2b fd 2f fd fd fd fd fd 31 31 29 21 fd fd fd 1d 25 fd 27 fd 1d 31	4e4kk4kk44mosowms}wwuy{w4e4kk4kk44Byw{y4e4kk4kk44')+%!%/+/11)!%'1#3))%'"%+3')+%!%/+/11)!%'1	success or wait	184	22C8D76	InternetReadFile
C:\Users\Public\Libraries\Ndvmyrkf	0	189867	1e 1c fd fd 34 fd 65 fd 34 fd fd 6b 6b fd 34 fd 18 fd fd 1a 1e 1c fd 6b 6b fd 34 18 fd fd fd 18 fd fd 34 02 6d 6f 04 06 73 00 fd 00 fd 6f 0a 06 77 0a 6d fd 73 7d 77 0c 0c 04 fd 77 75 7f fd 00 fd 02 fd fd 0c fd 79 0e 7b 04 fd 04 fd 00 02 02 00 fd 06 77 fd 0e 1e 1c fd fd 34 fd 65 fd 34 fd fd 6b 6b fd 34 fd 18 fd fd 1a 1e 1c fd 6b 6b fd 34 18 fd fd fd 18 fd fd 34 42 fd 0c 79 fd 08 77 fd 7b 0e 79 1e 1c fd fd 34 fd 65 fd 34 fd fd 6b 6b fd 34 fd 18 fd fd 1a 1e 1c fd 6b 6b fd 34 18 fd fd fd 18 fd fd 34 27 fd fd 29 2b fd 25 21 25 fd fd 2f 2b fd 2f fd fd fd fd fd 31 31 29 21 fd fd fd 1d 25 fd 27 fd 1d 31 23 fd 33 fd 29 fd 29 fd 25 27 27 25 fd 2b fd fd 33 27 fd fd 29 2b fd 25 21 25 fd fd 2f 2b fd 2f fd fd fd fd fd 31 31 29 21 fd fd fd 1d 25 fd 27 fd 1d 31	4e4kk4kk44mosowms}wwuy{w4e4kk4kk44Byw{y4e4kk4kk44')+%!%/+/11)!%'1#3))%'"%+3')+%!%/+/11)!%'1	success or wait	1	22C8A00	_lwrite

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\Public\Libraries\Ndvmyrkf.exe	0	262144	4d 5a 50 00 02 00 00 00 04 00 0f 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 fd 10 00 0e 1f fd 09 fd 21 fd 01 4c fd 21 fd fd 54 68 69 73 20 70 72 6f 67 72 61 6d 20 6d 75 73 74 20 62 65 20 72 75 6e 20 75 6e 64 65 72 20 57 69 6e 33 32 0d 0a 24 37 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	MZP@!L!This program must be run under Win32$7	success or wait	3	22CB37E	CopyFileA
C:\Users\Public\Libraries\Ndvmyrkf.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	22CB37E	CopyFileA
C:\Users\Public\Libraries\fkrymvdN.url	0	100	5b 49 6e 74 65 72 6e 65 74 53 68 6f 72 74 63 75 74 5d 0d 0a 55 52 4c 3d 66 69 6c 65 3a 22 43 3a 5c 5c 55 73 65 72 73 5c 5c 50 75 62 6c 69 63 5c 5c 4c 69 62 72 61 72 69 65 73 5c 5c 4e 64 76 6d 79 72 6b 66 2e 65 78 65 22 0d 0a 49 63 6f 6e 49 6e 64 65 78 3d 35 37 0d 0a 48 6f 74 4b 65 79 3d 33 37 0d 0a	[InternetShortcut]URL=file:"C:\\Users\\Public\\Libraries\\Ndvmyrkf.exe"IconIndex=57 HotKey=37	success or wait	1	22B8095	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\Desktop\Copie a bonului de plata.exe	unknown	750592	success or wait	1	22B33F1	ReadFile

Registry Activities

Analysis Process: colorcpl.exe PID: **3556**, Parent PID: **5152**

General

Target ID:	1
Start time:	12:48:06
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\colorcpl.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\colorcpl.exe
Imagebase:	0xec0000
File size:	86528 bytes
MD5 hash:	746F3B5E7652EA0766BA10414D317981
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: 00000001.00000002.368934423.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000001.00000002.368934423.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.368934423.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.368934423.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.363700003.0000000004E70000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000001.00000002.363700003.0000000004E70000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.363700003.0000000004E70000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.363700003.0000000004E70000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000000.260531980.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000001.00000000.260531980.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000000.260531980.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000000.260531980.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000000.259676945.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000001.00000000.259676945.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000000.259676945.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000000.259676945.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.363506192.0000000004E40000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000001.00000002.363506192.0000000004E40000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.363506192.0000000004E40000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.363506192.0000000004E40000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000000.259327533.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000001.00000000.259327533.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000000.259327533.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000000.259327533.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000000.260096262.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000001.00000000.260096262.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000000.260096262.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000000.260096262.0000000010410000.00000040.00000400.00020000.00000000.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	1622408	success or wait	1	1042A417	NtReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: explorer.exe PID: **3452**, Parent PID: **3556**

General	
Target ID:	2
Start time:	12:48:10
Start date:	29/11/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff647860000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000000.333241932.00000000100D9000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000000.333241932.00000000100D9000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.333241932.00000000100D9000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.333241932.00000000100D9000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\9N30RODQ\9N3logri.ini	0	40	success or wait	2	5A46604	NtReadFile
C:\Users\user\AppData\Roaming\9N30RODQ\9N3logrg.ini	0	38	success or wait	2	5A46604	NtReadFile
C:\Users\user\AppData\Roaming\9N30RODQ\9N3logrv.ini	0	40	success or wait	2	5A46604	NtReadFile
C:\Users\user\AppData\Roaming\9N30RODQ\9N3logim.jpeg	0	92472	success or wait	2	5A46604	NtReadFile

Analysis Process: Ndvmyrkf.exe PID: **5252**, Parent PID: **3452**

General	
Target ID:	3
Start time:	12:48:18
Start date:	29/11/2022
Path:	C:\Users\Public\Libraries\Ndvmyrkf.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\Libraries\Ndvmyrkf.exe"
Imagebase:	0x400000
File size:	750592 bytes
MD5 hash:	EB8C68C29D6131D6B903DD268D6FF0EF
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	Borland Delphi
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.305721420.00000000046D3000.00000004.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000003.00000002.305721420.00000000046D3000.00000004.00001000.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.305721420.00000000046D3000.00000004.00001000.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.305721420.00000000046D3000.00000004.00001000.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 20%, ReversingLabs
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\Public\Libraries\Ndvmyrkf	unknown	189867	success or wait	1	27733F1	ReadFile

Analysis Process: wscript.exe PID: **4648**, Parent PID: **5252**

General	
Target ID:	6
Start time:	12:48:25
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\wscript.exe
Imagebase:	0xa20000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.300982694.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000006.00000000.300982694.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.300982694.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.300982694.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.301779661.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000006.00000000.301779661.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.301779661.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.301779661.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.362672301.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000006.00000002.362672301.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.362672301.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.362672301.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.301417348.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000006.00000000.301417348.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.301417348.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.301417348.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.300560859.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000006.00000000.300560859.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.300560859.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.300560859.0000000010410000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.349866867.00000000052F0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000006.00000002.349866867.00000000052F0000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.349866867.00000000052F0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.349866867.00000000052F0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.350083246.00000000060B0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000006.00000002.350083246.00000000060B0000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.350083246.00000000060B0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.350083246.00000000060B0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	1042A417	NtReadFile

Analysis Process: raserver.exe PID: **3868**, Parent PID: **3452**

General

Target ID:	12
Start time:	12:48:46
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\raserver.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\raserver.exe

Imagebase:	0xfc0000
File size:	108544 bytes
MD5 hash:	2AADF65E395BFBD0D9B71D7279C8B5EC
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.514213076.00000000035F0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000C.00000002.514213076.00000000035F0000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.514213076.00000000035F0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.514213076.00000000035F0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.511910785.0000000003200000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000C.00000002.511910785.0000000003200000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.511910785.0000000003200000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.511910785.0000000003200000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000C.00000002.514481833.0000000003620000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000C.00000002.514481833.0000000003620000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000C.00000002.514481833.0000000003620000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000C.00000002.514481833.0000000003620000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	321A417	NtReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Analysis Process: msdt.exe PID: **632**, Parent PID: **3452**

General

Target ID:	13
Start time:	12:48:46
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\msdt.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\msdt.exe
Imagebase:	0x1030000
File size:	1508352 bytes
MD5 hash:	7F0C51DBA69B9DE5DDF6AA04CE3A69F4
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.367412831.0000000000AF0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000D.00000002.367412831.0000000000AF0000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.367412831.0000000000AF0000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.367412831.0000000000AF0000.00000040.80000000.00040000.00000000.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	1622408	success or wait	1	B0A417	NtReadFile

Analysis Process: cmd.exe PID: **3672**, Parent PID: **3868**

General

Target ID:	14
Start time:	12:48:58
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c copy "C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data" "C:\Users\user\AppData\Local\Temp\DB1" /V
Imagebase:	0x1b0000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: **1808**, Parent PID: **3672**

General

Target ID:	15
Start time:	12:48:59
Start date:	29/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6da640000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

No disassembly