ID: 750476
Sample Name: yoyrJ.dll
Cookbook: default.jbs
Time: 04:19:06
Date: 21/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

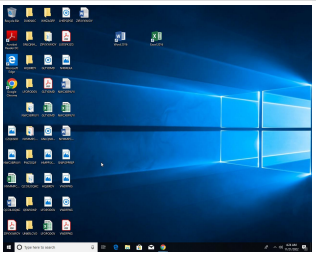
Windows Analysis Report

yoyrJ.dll

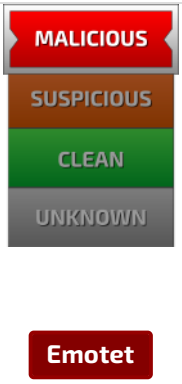
Overview

General Information

Sample Name:	yoyrJ.dll
Analysis ID:	750476
MD5:	dd7105e9748a29.
SHA1:	827b323bda769b.
SHA256:	c987ad0cc79b59..
Infos:	



Detection



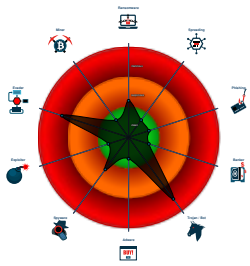
Emotet

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected Emotet
- System process connects to networ…
- Antivirus detection for URL or domain
- Snort IDS alert for network traffic
- Creates an autostart registry key po…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Queries the volume information (nam…
- Yara signature match
- Contains functionality to check if a d…

Classification



Process Tree

- **System is w10x64**
- loaddll64.exe (PID: 3692 cmdline: loaddll64.exe "C:\Users\user\Desktop\yoyrJ.dll" MD5: C676FC0263EDD17D4CE7D644B8F3FCD6)
  - conhost.exe (PID: 3096 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - cmd.exe (PID: 976 cmdline: cmd.exe /C rundll32.exe "C:\Users\user\Desktop\yoyrJ.dll",#1 MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
    - rundll32.exe (PID: 5288 cmdline: rundll32.exe "C:\Users\user\Desktop\yoyrJ.dll",#1 MD5: 73C519F050C20580F8A62C849D49215A)
      - regsvr32.exe (PID: 5412 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\RPhOZPFULSaJ\nMwLrZYwR.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
      - WMIADAP.exe (PID: 5412 cmdline: wmiadap.exe /F /T /R MD5: 9783D0765F31980950445DFD40DB15DA)
  - regsvr32.exe (PID: 5020 cmdline: regsvr32.exe /s C:\Users\user\Desktop\yoyrJ.dll MD5: D78B75FC68247E8A63ACBA846182740E)
    - regsvr32.exe (PID: 5908 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\UgFJoEzLBQVtMeg\qohQcmrlRynEDAUP.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
  - rundll32.exe (PID: 5284 cmdline: rundll32.exe C:\Users\user\Desktop\yoyrJ.dll,DllRegisterServer MD5: 73C519F050C20580F8A62C849D49215A)
    - regsvr32.exe (PID: 4644 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\YbSMYJyTdzumryV\WWgeEzfCEnB.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
  - regsvr32.exe (PID: 5132 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\OGxcy\dYkxHTuA.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
  - regsvr32.exe (PID: 5132 cmdline: C:\Windows\system32\regsvr32.exe" "C:\Windows\system32\UgFJoEzLBQVtMeg\qohQcmrlRynEDAUP.dll MD5: D78B75FC68247E8A63ACBA846182740E)
    - regsvr32.exe (PID: 4192 cmdline: C:\Windows\system32\regsvr32.exe "C:\Users\user\AppData\Local\ArkmTuxCaKyXkTDZ\fBEZnVEOT.dll" MD5: D78B75FC68247E8A63ACBA846182740E)
- **cleanup**

Malware Configuration

Threatname: Emotet

```
{
  "C2 list": [
    "173.255.211.88:443",
    "45.63.99.23:7080",
    "182.162.143.56:443",
    "91.187.140.35:8080",
    "212.24.98.99:8080",
    "119.59.103.152:8080",
    "45.235.8.30:8080",
    "172.104.251.154:8080",
    "72.15.201.15:8080",
    "169.57.156.166:8080",
    "103.75.201.2:443",
    "213.239.212.5:443",
    "164.90.222.65:443",
    "201.94.166.162:443",
    "94.23.45.86:4143",
    "183.111.227.137:8080",
    "186.194.240.217:443",
    "107.170.39.149:8080",
    "147.139.166.154:8080",
    "5.135.159.50:443",
    "206.189.28.199:8080",
    "104.168.155.143:8080",
    "129.232.188.93:443",
    "82.223.21.224:8080",
    "103.43.75.120:443",
    "103.132.242.26:8080",
    "139.59.56.73:8080",
    "164.68.99.3:8080",
    "202.129.205.3:8080",
    "167.172.199.165:8080",
    "110.232.117.186:8080",
    "209.97.163.214:443",
    "167.172.253.162:8080",
    "1.234.2.232:8080",
    "159.65.88.10:8080",
    "95.217.221.146:8080",
    "153.92.5.27:8080",
    "91.207.28.33:8080",
    "188.44.20.25:443",
    "153.126.146.25:7080",
    "163.44.196.120:8080",
    "172.105.226.75:8080",
    "115.68.227.76:8080",
    "159.65.140.115:443",
    "139.59.126.41:443",
    "197.242.150.244:8080",
    "45.176.232.124:443",
    "45.118.115.99:8080",
    "149.56.131.28:8080",
    "79.137.35.198:8080",
    "173.212.193.249:8080",
    "160.16.142.56:8080",
    "159.89.202.34:443",
    "185.4.135.165:8080"
  ],
  "Public Key": [
    "RUNTMSAAAABAX3S2xNjcDD0fBno33Ln5t71eii+mofIPoXkNFOX1MeiwCh48iz97kB0mJjGGZXwardnDXKxI8GCHGNl0PFj5J0rtUQAbAIw=",
    "RUNLMSAAAADzozW1Di4r9DVWzQpMKT588RDdy7BPILP6AiDOTLYMHkSWvrQO5slbmr1OvZ2Pz+AQWzRMggQmAtO6rPH7nyx2AkoOUQAUAJA="
  ]
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.828364693.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000002.828364693.0000000180001000.00000020.00001000.00020000.00000000.sdmp	Windows_Trojan_Emotet_db7d33fa	unknown	unknown	• 0x171c2:$chunk_0: 4C 8D 9C 24 80 00 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0x2a90c:$chunk_0: 4C 8D 9C 24 80 00 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0x24ac0:$chunk_1: 8B C7 41 0F B7 4C 45 00 41 8B 1C 8C 48 03 DD 48 3B DE 72 1B • 0x1b568:$chunk_2: 48 8B C4 48 89 48 08 48 89 50 10 4C 89 40 18 4C 89 48 20 C3 • 0x216e4:$chunk_4: 48 39 3B 4C 8D 9C 24 80 00 00 00 49 8B 5B 10 49 8B 73 18 40 0F 95 C7 8B C7 49 8B 7B 20 49 8B E3 5D C3 • 0x2ae01:$chunk_4: 48 39 3B 4C 8D 9C 24 80 00 00 00 49 8B 5B 10 49 8B 73 20 40 0F 95 C7 8B C7 49 8B 7B 28 49 8B E3 5D C3 • 0x24ad4:$chunk_6: 43 8B 84 FE 8C 00 00 00 48 03 C6 48 3B D8 73 0B
0000000C.00000002.496080462.0000000000D20000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0000000C.00000002.496080462.0000000000D20000.00000040.00001000.00020000.00000000.sdmp	Windows_Trojan_Emotet_db7d33fa	unknown	unknown	• 0x175c2:$chunk_0: 4C 8D 9C 24 80 00 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0x2ad0c:$chunk_0: 4C 8D 9C 24 80 00 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0x24ec0:$chunk_1: 8B C7 41 0F B7 4C 45 00 41 8B 1C 8C 48 03 DD 48 3B DE 72 1B • 0x1b968:$chunk_2: 48 8B C4 48 89 48 08 48 89 50 10 4C 89 40 18 4C 89 48 20 C3 • 0x21ae4:$chunk_4: 48 39 3B 4C 8D 9C 24 80 00 00 00 49 8B 5B 10 49 8B 73 18 40 0F 95 C7 8B C7 49 8B 7B 20 49 8B E3 5D C3 • 0x2b201:$chunk_4: 48 39 3B 4C 8D 9C 24 80 00 00 00 49 8B 5B 10 49 8B 73 20 40 0F 95 C7 8B C7 49 8B 7B 28 49 8B E3 5D C3 • 0x24ed4:$chunk_6: 43 8B 84 FE 8C 00 00 00 48 03 C6 48 3B D8 73 0B
00000000.00000002.322442190.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 20 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.loaddll64.exe.141aeea0000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
0.2.loaddll64.exe.141aeea0000.0.raw.unpack	Windows_Trojan_Emotet_db7d33fa	unknown	unknown	• 0x175c2:$chunk_0: 4C 8D 9C 24 80 00 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0x2ad0c:$chunk_0: 4C 8D 9C 24 80 00 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0x24ec0:$chunk_1: 8B C7 41 0F B7 4C 45 00 41 8B 1C 8C 48 03 DD 48 3B DE 72 1B • 0x1b968:$chunk_2: 48 8B C4 48 89 48 08 48 89 50 10 4C 89 40 18 4C 89 48 20 C3 • 0x21ae4:$chunk_4: 48 39 3B 4C 8D 9C 24 80 00 00 00 49 8B 5B 10 49 8B 73 18 40 0F 95 C7 8B C7 49 8B 7B 20 49 8B E3 5D C3 • 0x2b201:$chunk_4: 48 39 3B 4C 8D 9C 24 80 00 00 00 49 8B 5B 10 49 8B 73 20 40 0F 95 C7 8B C7 49 8B 7B 28 49 8B E3 5D C3 • 0x24ed4:$chunk_6: 43 8B 84 FE 8C 00 00 00 48 03 C6 48 3B D8 73 0B
7.2.regsvr32.exe.ba0000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
7.2.regsvr32.exe.ba0000.0.raw.unpack	Windows_Trojan_Emotet_db7d33fa	unknown	unknown	• 0x175c2:$chunk_0: 4C 8D 9C 24 80 00 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0x2ad0c:$chunk_0: 4C 8D 9C 24 80 00 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0x24ec0:$chunk_1: 8B C7 41 0F B7 4C 45 00 41 8B 1C 8C 48 03 DD 48 3B DE 72 1B • 0x1b968:$chunk_2: 48 8B C4 48 89 48 08 48 89 50 10 4C 89 40 18 4C 89 48 20 C3 • 0x21ae4:$chunk_4: 48 39 3B 4C 8D 9C 24 80 00 00 00 49 8B 5B 10 49 8B 73 18 40 0F 95 C7 8B C7 49 8B 7B 20 49 8B E3 5D C3 • 0x2b201:$chunk_4: 48 39 3B 4C 8D 9C 24 80 00 00 00 49 8B 5B 10 49 8B 73 20 40 0F 95 C7 8B C7 49 8B 7B 28 49 8B E3 5D C3 • 0x24ed4:$chunk_6: 43 8B 84 FE 8C 00 00 00 48 03 C6 48 3B D8 73 0B
4.2.rundll32.exe.1ebd2220000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 19 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET CNC Feodo Tracker Reported CnC Server TCP group 7 - Source IP: 192.168.2.4 - Destination IP: 173.255.211.88

Timestamp:	192.168.2.4173.255.211.88496954432404312 11/21/22-04:20:47.613393
SID:	2404312
Source Port:	49695
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 8 - Source IP: 192.168.2.4 - Destination IP: 182.162.143.56

Timestamp:	192.168.2.4182.162.143.56497004432404314 11/21/22-04:21:09.058938
SID:	2404314
Source Port:	49700
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 16 - Source IP: 192.168.2.4 - Destination IP: 45.63.99.23

Timestamp:	192.168.2.445.63.99.234969970802404330 11/21/22-04:20:53.767379
SID:	2404330
Source Port:	49699
Destination Port:	7080
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Networking

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

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected Emotet

System Summary

Malicious sample detected (through community Yara rule)

Boot Survival

Creates an autostart registry key pointing to binary in C:\Windows

Hooking and other Techniques for Hiding and Protection

Hides that the sample has been downloaded from the Internet (zone.identifier)

HIPS / PFW / Operating System Protection Evasion

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

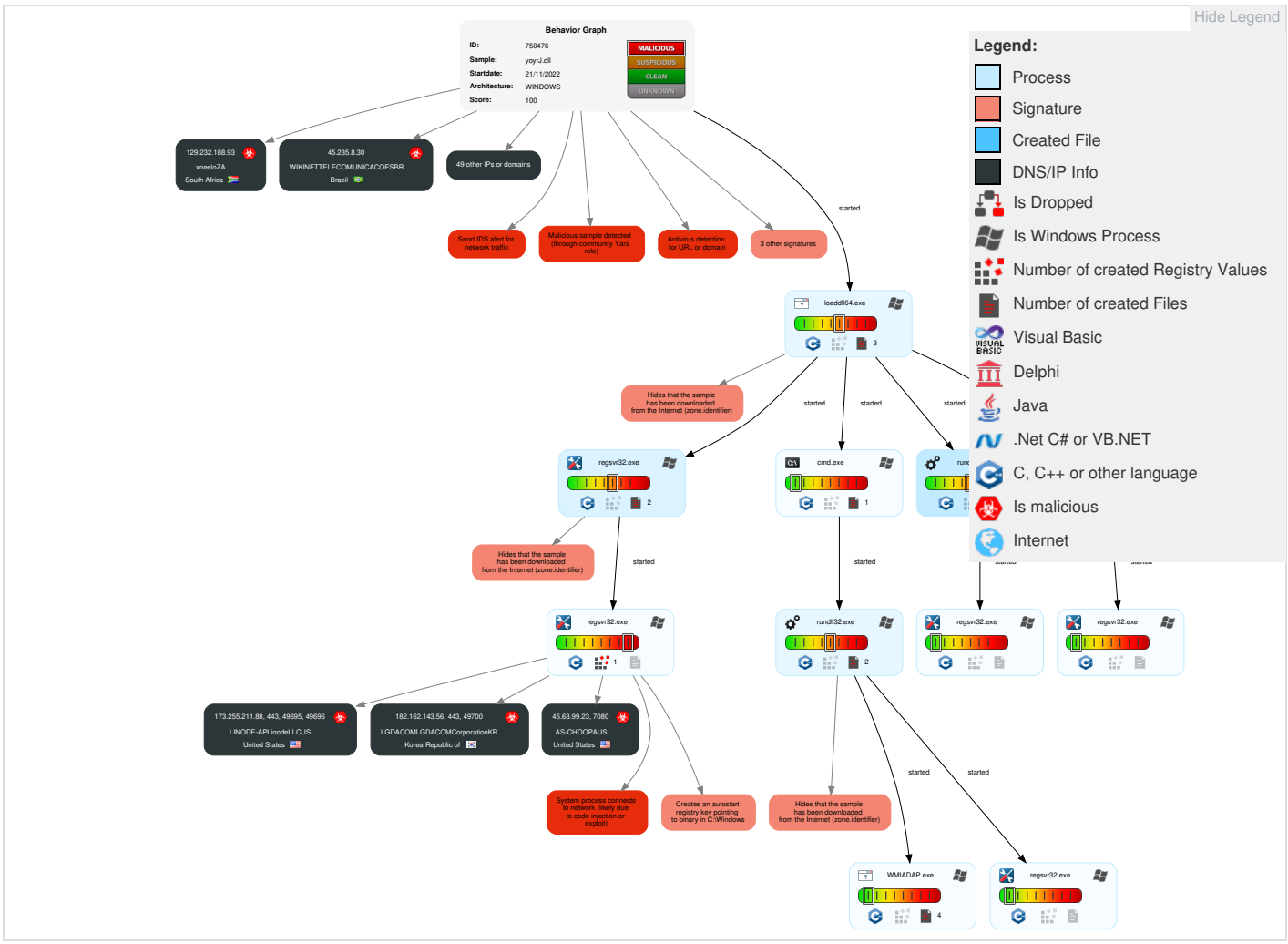
Stealing of Sensitive Information

Yara detected Emotet

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 1 Registry Run Keys / Startup Folder	1 1 1 Process Injection	2 1 Masquerading	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	1 DLL Side-Loading	1 1 Registry Run Keys / Startup Folder	1 Virtualization/Sandbox Evasion	LSASS Memory	1 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 DLL Side-Loading	1 1 1 Process Injection	Security Account Manager	1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 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 Hidden Files and Directories	NTDS	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	LSA Secrets	1 Application Window Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Regsvr32	Cached Domain Credentials	2 File and Directory Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Rundll32	DCSync	2 5 System Information 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	1 DLL Side-Loading	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 File Deletion	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.

Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
yoyrJ.dll	88%	ReversingLabs	Win64.Trojan.Emotet	
yoyrJ.dll	48%	Metadefender		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
12.2.regsvr32.exe.d20000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
5.2.rundll32.exe.1bbc5810000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
7.2.regsvr32.exe.ba0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
0.2.loaddll64.exe.141aeea0000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File

Source	Detection	Scanner	Label	Link	Download
3.2.regsvr32.exe.a90000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File
4.2.rundll32.exe.1ebd2220000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://182.162.143.56/	0%	URL Reputation	safe	
http://https://17.63.99.23:7080/	0%	Avira URL Cloud	safe	
http://https://182.162.143.56/ltqyvaphgamn/iuduszibmmiode/zgmecigm/lvlmwwim/	100%	Avira URL Cloud	malware	
http://https://45.63.99.23:7080/ltqyvaphgamn/iuduszibmmiode/zgmecigm/lvlmwwim/	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

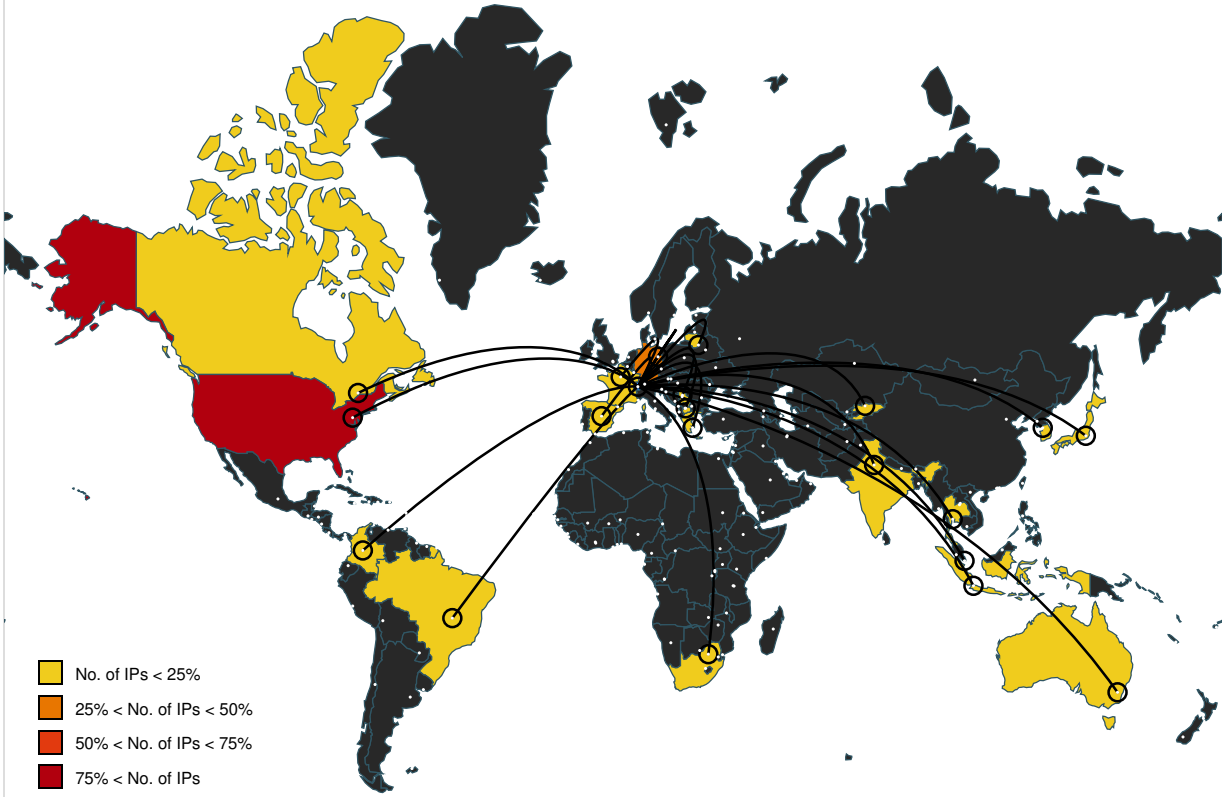
Name	Malicious	Antivirus Detection	Reputation
http://https://182.162.143.56/ltqyvaphgamn/iuduszibmmiode/zgmecigm/lvlmwwim/	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://45.63.99.23:7080/ltqyvaphgamn/iuduszibmmiode/zgmecigm/lvlmwwim/	regsvr32.exe, 00000007.00000003.585426852.0000000000C87000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.584653863.0000000000C86000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.585349266.0000000000C86000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000002.828075611.0000000000C8D000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.456277440.0000000000C86000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.585829274.0000000000C8D000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://182.162.143.56/	regsvr32.exe, 00000007.00000003.585862169.0000000000CBE000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000002.828134623.0000000000CC0000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.584870026.0000000000CB9000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.456389200.0000000000CB800.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.456205938.0000000000CAB000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.584908649.0000000000CBA000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://17.63.99.23:7080/	regsvr32.exe, 00000007.00000003.58537291 5.0000000000C91000.00000004.00000020.000 20000.00000000.sdmp, regsvr32.exe, 00000 007.00000002.828083663.0000000000C91000. 00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.585447 802.0000000000C91000.00000004.00000020.0 0020000.00000000.sdmp, regsvr32.exe, 000 00007.00000003.585835870.0000000000C9100 0.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 00000007.00000003.584690393.0000 000000C91000.00000004.00000020.00020000. 00000000.sdmp, regsvr32.exe, 00000007.00 000003.456292772.0000000000C91000.000000 04.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
110.232.117.186	unknown	Australia		56038	RACKCORP-APRackCorpAU	true
103.132.242.26	unknown	India		45117	INPL-IN-APIshansNetworkIN	true
104.168.155.143	unknown	United States		54290	HOSTWINDSUS	true
79.137.35.198	unknown	France		16276	OVHFR	true
45.118.115.99	unknown	Indonesia		131717	IDNIC-CIFO-AS-IDPTCitraJelajahInformatikaID	true
172.104.251.154	unknown	United States		63949	LINODE-APLinodeLLCUS	true
115.68.227.76	unknown	Korea Republic of		38700	SMILESERV-AS-KRSMILESERVKR	true
163.44.196.120	unknown	Singapore		135161	GMO-Z-COM-THGMO-ZcomNetDesignHoldingsCoLtdSG	true
206.189.28.199	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
45.63.99.23	unknown	United States		20473	AS-CHOOPAUS	true
107.170.39.149	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
197.242.150.244	unknown	South Africa		37611	AfrihostZA	true
185.4.135.165	unknown	Greece		199246	TOPHOSTGR	true
183.111.227.137	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
45.176.232.124	unknown	Colombia		267869	CABLEYTELECOMUNICACIONESDECOLOMBIASASCABLETELCOC	true
139.59.56.73	unknown	Singapore		14061	DIGITALOCEAN-ASNUS	true
169.57.156.166	unknown	United States		36351	SOFTLAYERUS	true
164.68.99.3	unknown	Germany		51167	CONTABODE	true
139.59.126.41	unknown	Singapore		14061	DIGITALOCEAN-ASNUS	true
167.172.253.162	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
147.139.166.154	unknown	United States		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	true
202.129.205.3	unknown	Thailand		45328	NIPA-AS-THNIPATECHNOLOGYCOLTDTH	true
167.172.199.165	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
153.92.5.27	unknown	Germany		47583	AS-HOSTINGERLT	true
159.65.140.115	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
159.65.88.10	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
172.105.226.75	unknown	United States		63949	LINODE-APLinodeLLCUS	true
164.90.222.65	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
213.239.212.5	unknown	Germany		24940	HETZNER-ASDE	true
5.135.159.50	unknown	France		16276	OVHFR	true
173.255.211.88	unknown	United States		63949	LINODE-APLinodeLLCUS	true
212.24.98.99	unknown	Lithuania		62282	RACKRAYUABRakrejusLT	true
186.194.240.217	unknown	Brazil		262733	NetceteraTelecomunicacoesLtdaBR	true
91.187.140.35	unknown	Serbia		13092	UB-ASRS	true
119.59.103.152	unknown	Thailand		56067	METRABYTE-TH453LadplacoutJorakhaebuaTH	true
159.89.202.34	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
201.94.166.162	unknown	Brazil		28573	CLAROSABR	true
160.16.142.56	unknown	Japan		9370	SAKURA-BSAKURAInternetIncJP	true
103.75.201.2	unknown	Thailand		133496	CDNPLUSCOLTD-AS-APCDNPLUSCOLTDTH	true
91.207.28.33	unknown	Kyrgyzstan		39819	PROHOSTKG	true
103.43.75.120	unknown	Japan		20473	AS-CHOOPAUS	true
188.44.20.25	unknown	Macedonia		57374	GIV-ASMK	true
45.235.8.30	unknown	Brazil		267405	WIKINETTELECOMUNICACOESBR	true
153.126.146.25	unknown	Japan		7684	SAKURA-ASAKURAInternetIncJP	true
72.15.201.15	unknown	United States		13649	ASN-VINSUS	true
82.223.21.224	unknown	Spain		8560	ONEANDONE-ASBrauerstrasse48DE	true
173.212.193.249	unknown	Germany		51167	CONTABODE	true
95.217.221.146	unknown	Germany		24940	HETZNER-ASDE	true
149.56.131.28	unknown	Canada		16276	OVHFR	true
209.97.163.214	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
182.162.143.56	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	true
1.234.2.232	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
129.232.188.93	unknown	South Africa		37153	xneeloZA	true
94.23.45.86	unknown	France		16276	OVHFR	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	750476
Start date and time:	2022-11-21 04:19:06 +01:00

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	yoyrJ.dll
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:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winDLL@21/2@0/54
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 67.7% (good quality ratio 58.8%) • Quality average: 65.2% • Quality standard deviation: 35.3%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .dll • Override analysis time to 240s for rundll32

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, conhost.exe, backgroundTaskHost.exe
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- 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 NtQueryValueKey calls found.
- VT rate limit hit for: yoyrJ.dll

Simulations

Behavior and APIs

Time	Type	Description
04:20:48	API Interceptor	3x Sleep call for process: regsvr32.exe modified
04:21:17	Autostart	Run: HKLM64\Software\Microsoft\Windows\CurrentVersion\Run qohQcmrlRynEDAUP.dll C:\Windows\system32\regsvr32.exe "C:\Windows\system32\UgFJoEzLBQVtMeg\qohQcmrlRynEDAUP.dll"

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:\Windows\System32\wbem\Performance\WmiApRpl_new.h

Process:	C:\Windows\System32\wbem\WMIADAP.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	3444
Entropy (8bit):	5.011954215267298
Encrypted:	false
SSDEEP:	48:ADPo+gDMIuK54DeHNg9dqbEzCJGGgGDU3XgLBgaGKFijiVJtVAAF/XRgW:ADw+gDMhK54qHC7aBvGKFijiV7XRgW
MD5:	B133A676D139032A27DE3D9619E70091
SHA1:	1248AA89938A13640252A79113930EDE2F26F1FA
SHA-256:	AE2B6236D3EEB4822835714AE9444E5DCD21BC60F7A909F2962C43BC743C7B15
SHA-512:	C6B99E13D854CE7A6874497473614EE4BD81C490802783DB1349AB851CD80D1DC06DF8C1F6E434ABA873A5BBF6125CC64104709064E19A9DC1C66DCDE3F8985
Malicious:	false
Preview:	//..//..// Copyright (C) 2000 Microsoft Corporation..//..// Module Name:..// WmiApRpl..//..// Abstract:..//..// Include file for object and counters definitions...//..//.....#define.WMI_Objects.0..#define.HiPerf_Classes.2..#define.HiPerf_Validity.4....#define.MSiSCSI_ConnectionStatistics_00000.6....#define.BytesReceived_00000.8..#define.BytesSent_00000.10..#define.PDUCommandsSent_00000.12..#define.PDUResponsesReceived_00000.14....#define.MSiSCSI_InitiatorInstanceStatistics_00001.16....#define.SessionConnectionTimeoutErrorCount_00001.18..#define.SessionDigestErrorCount_00001.20..#define.SessionFailureCount_00001.22..#define.SessionFormatErrorCount_00001.24....#define.MSiSCSI_InitiatorLoginStatistics_00002.26....#define.LoginAcceptRsps_00002.28..#define.LoginAuthenticateFails_00002.30..#define.LoginAuthFai

C:\Windows\system32\wbem\Performance\WmiApRpl.h (copy)

Process:	C:\Windows\System32\wbem\WMIADAP.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	3444
Entropy (8bit):	5.011954215267298
Encrypted:	false
SSDEEP:	48:ADPo+gDMIuK54DeHNg9dqbEzCJGGgGDU3XgLBgaGKFijiVJtVAAF/XRgW:ADw+gDMhK54qHC7aBvGKFijiV7XRgW
MD5:	B133A676D139032A27DE3D9619E70091
SHA1:	1248AA89938A13640252A79113930EDE2F26F1FA
SHA-256:	AE2B6236D3EEB4822835714AE9444E5DCD21BC60F7A909F2962C43BC743C7B15
SHA-512:	C6B99E13D854CE7A6874497473614EE4BD81C490802783DB1349AB851CD80D1DC06DF8C1F6E434ABA873A5BBF6125CC64104709064E19A9DC1C66DCDE3F8985
Malicious:	false
Preview:	//..//..// Copyright (C) 2000 Microsoft Corporation..//..// Module Name:..// WmiApRpl..//..// Abstract:..//..// Include file for object and counters definitions...//..//.....#define.WMI_Objects.0..#define.HiPerf_Classes.2..#define.HiPerf_Validity.4....#define.MSiSCSI_ConnectionStatistics_00000.6....#define.BytesReceived_00000.8..#define.BytesSent_00000.10..#define.PDUCommandsSent_00000.12..#define.PDUResponsesReceived_00000.14....#define.MSiSCSI_InitiatorInstanceStatistics_00001.16....#define.SessionConnectionTimeoutErrorCount_00001.18..#define.SessionDigestErrorCount_00001.20..#define.SessionFailureCount_00001.22..#define.SessionFormatErrorCount_00001.24....#define.MSiSCSI_InitiatorLoginStatistics_00002.26....#define.LoginAcceptRsps_00002.28..#define.LoginAuthenticateFails_00002.30..#define.LoginAuthFai

Static File Info

General

File type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows

Entropy (8bit):	6.773063357716462
TrID:	• Win64 Dynamic Link Library (generic) (102004/3) 86.43% • Win64 Executable (generic) (12005/4) 10.17% • Generic Win/DOS Executable (2004/3) 1.70% • DOS Executable Generic (2002/1) 1.70% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.01%
File name:	yoyrJ.dll
File size:	433152
MD5:	dd7105e9748a29b5bd61ea57214d57e3
SHA1:	827b323bda769ba7fb838a231aa4160209266b14
SHA256:	c987ad0cc79b598bdee9ec7da96b07e82a04cadd73cb3caf85b799731deef9a1
SHA512:	beca102422697e4cd50b81289bdc5097935f11c0c5acc86b7a69893fb819a3cd225e4b2594a2bb40163fbd68d7ac281b0ff260f30b55cf188112445eb26986b7
SSDEEP:	6144:PZUCuTJlyIOziaTGy+IeIt1xJh5eWhv/w62LcuPv8cD4mRKqdONyAzDxkMwp2/uw:Py7EzZ4+HvY62LxHJ4KTGDIT
TLSH:	1C94E141365506F1C9378334CA931E4BE832740A5335A64F02A9D5F67F7B761AB2F32A
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....?...l...l...l...l...l...l../l...l..2l...l.."l...l...l...l...l...l..*l...l..+l...l...,l...lRich...l.....PE..d..

File Icon

Icon Hash:	74f0e4ecccdce0e4

Static PE Info

General

Entrypoint:	0x180005bdc
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x180000000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE, DLL
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x636D291C [Thu Nov 10 16:38:52 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	2
File Version Major:	5
File Version Minor:	2
Subsystem Version Major:	5
Subsystem Version Minor:	2
Import Hash:	b3da9e0a2ac4751e0c486ad7cdc326f7

Entrypoint Preview

Instruction
dec eax
mov dword ptr [esp+08h], ebx
dec eax
mov dword ptr [esp+10h], esi
push edi
dec eax
sub esp, 20h
dec ecx
mov edi, eax
mov ebx, edx
dec eax
mov esi, ecx
cmp edx, 01h
jne 00007FFA20ABA017h
call 00007FFA20ABD060h
dec esp

Instruction
mov eax, edi
mov edx, ebx
dec eax
mov ecx, esi
dec eax
mov ebx, dword ptr [esp+30h]
dec eax
mov esi, dword ptr [esp+38h]
dec eax
add esp, 20h
pop edi
jmp 00007FFA20AB9EBCh
int3
int3
int3
dec eax
mov dword ptr [esp+08h], ecx
dec eax
sub esp, 00000088h
dec eax
lea ecx, dword ptr [00062F31h]
call dword ptr [0001C543h]
dec eax
mov eax, dword ptr [0006301Ch]
dec eax
mov dword ptr [esp+58h], eax
inc ebp
xor eax, eax
dec eax
lea edx, dword ptr [esp+60h]
dec eax
mov ecx, dword ptr [esp+58h]
call 00007FFA20AD2638h
dec eax
mov dword ptr [esp+50h], eax
dec eax
cmp dword ptr [esp+50h], 00000000h
je 00007FFA20ABA053h
dec eax
mov dword ptr [esp+38h], 00000000h
dec eax
lea eax, dword ptr [esp+48h]
dec eax
mov dword ptr [esp+30h], eax
dec eax
lea eax, dword ptr [esp+40h]
dec eax
mov dword ptr [esp+28h], eax
dec eax
lea eax, dword ptr [00062EDCh]
dec eax
mov dword ptr [esp+20h], eax
dec esp
mov ecx, dword ptr [esp+50h]
dec esp
mov eax, dword ptr [esp+58h]
dec eax
mov edx, dword ptr [esp+60h]
xor ecx, ecx

Instruction
call 00007FFA20AD25E6h
jmp 00007FFA20ABA034h
dec eax
mov eax, dword ptr [eax+eax+00000000h]

Rich Headers

Programming Language:	• [C++] VS2010 build 30319 • [C] VS2010 build 30319 • [ASM] VS2010 build 30319 • [C] VS2008 SP1 build 30729 • [IMP] VS2008 SP1 build 30729 • [EXP] VS2010 build 30319 • [RES] VS2010 build 30319 • [LNK] VS2010 build 30319

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x66770	0x57	.rdata
IMAGE_DIRECTORY_ENTRY_IMPORT	0x65cb4	0x64	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x6d000	0x254	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x6a000	0x1ac4	.pdata
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x6e000	0x3ec	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x22000	0x338	.rdata
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	0x20182	0x20200	False	0.5494513010700389	data	6.563588075042218	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rdata	0x22000	0x447c7	0x44800	False	0.6747904311131386	data	6.184568591532381	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x67000	0x2fd0	0x1c00	False	0.291015625	data	3.404968127612506	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ, IMAGE_SCN_MEM_WRITE
.pdata	0x6a000	0x1ac4	0x1c00	False	0.46861049107142855	data	5.279471356455433	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
text	0x6c000	0x91d	0xa00	False	0.389453125	data	5.167000712138923	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_EXECUTE
.rsrc	0x6d000	0x254	0x400	False	0.3134765625	data	4.723033814693597	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x6e000	0x7f6	0x800	False	0.35693359375	data	3.497910650248424	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_STRING	0x6d0a0	0x58	data	English	United States
RT_MANIFEST	0x6d0f8	0x15a	ASCII text, with CRLF line terminators	English	United States

Imports

DLL	Import
USER32.dll	TranslateMessage, DefWindowProcW, UpdateWindow, MessageBoxW, CreateWindowExW, EndPaint, DestroyWindow, TranslateAcceleratorW, GetMessageW, PostQuitMessage, LoadCursorW, BeginPaint, DispatchMessageW, GetTouchInputInfo, RegisterClassExW, RegisterTouchWindow, InvalidateRect, CloseTouchInputHandle, LoadStringW, ShowWindow, UnregisterTouchWindow
GDI32.dll	LineTo, DeleteObject, SelectObject, Polyline, CreatePen, MoveToEx
ole32.dll	CoUninitialize, CoInitialize, CoLoadLibrary, CoCreateInstance
KERNEL32.dll	HeapReAlloc, GetLocaleInfoW, LoadLibraryW, FreeLibrary, SetConsoleCtrlHandler, IsValidCodePage, GetOEMCP, LCMapStringW, GetCPInfo, GetStringTypeW, EnterCriticalSection, FatalAppExitA, LeaveCriticalSection, GetSystemTimeAsFileTime, GetCurrentProcessId, MultiByteToWideChar, GetUserDefaultLCID, GetLocaleInfoA, EnumSystemLocalesA, IsValidLocale, GetACP, GetModuleHandleW, GetTickCount, QueryPerformanceCounter, GetEnvironmentStringsW, WideCharToMultiByte, FreeEnvironmentStringsW, HeapAlloc, EncodePointer, DecodePointer, GetCurrentThreadId, FlsSetValue, GetCommandLineA, TerminateProcess, GetCurrentProcess, UnhandledExceptionFilter, SetUnhandledExceptionFilter, IsDebuggerPresent, RtlVirtualUnwind, RtlLookupFunctionEntry, RtlCaptureContext, GetLastError, HeapFree, GetProcAddress, ExitProcess, WriteFile, GetStdHandle, GetModuleFileNameW, HeapSetInformation, GetVersion, HeapCreate, HeapDestroy, Sleep, HeapSize, RtlUnwindEx, RaiseException, RtlPcToFileHeader, FlsGetValue, FlsFree, SetLastError, GetCurrentThread, FlsAlloc, SetHandleCount, InitializeCriticalSectionAndSpinCount, GetFileType, GetStartupInfoW, DeleteCriticalSection, GetModuleFileNameA

Exports

Name	Ordinal	Address
DllRegisterServer	1	0x180003854

Possible Origin

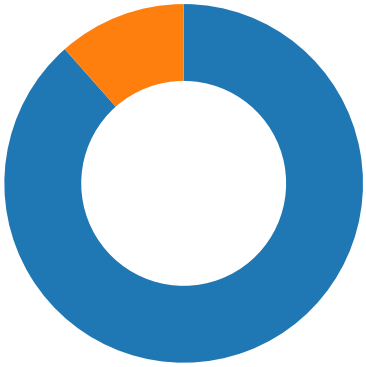
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.4173.255.211.88496954432404312 11/21/22-04:20:47.613393	TCP	2404312	ET CNC Feodo Tracker Reported CnC Server TCP group 7	49695	443	192.168.2.4	173.255.211.88
192.168.2.4182.162.143.56497004432404314 11/21/22-04:21:09.058938	TCP	2404314	ET CNC Feodo Tracker Reported CnC Server TCP group 8	49700	443	192.168.2.4	182.162.143.56
192.168.2.445.63.99.23496997080240433 11/21/22-04:20:53.767379	TCP	2404330	ET CNC Feodo Tracker Reported CnC Server TCP group 16	49699	7080	192.168.2.4	45.63.99.23

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2022 04:20:47.613393068 CET	49695	443	192.168.2.4	173.255.211.88
Nov 21, 2022 04:20:47.613487959 CET	443	49695	173.255.211.88	192.168.2.4
Nov 21, 2022 04:20:47.613646030 CET	49695	443	192.168.2.4	173.255.211.88
Nov 21, 2022 04:20:47.621453047 CET	49695	443	192.168.2.4	173.255.211.88
Nov 21, 2022 04:20:47.621525049 CET	443	49695	173.255.211.88	192.168.2.4
Nov 21, 2022 04:20:47.796107054 CET	443	49695	173.255.211.88	192.168.2.4
Nov 21, 2022 04:20:47.797595978 CET	49696	443	192.168.2.4	173.255.211.88
Nov 21, 2022 04:20:47.797673941 CET	443	49696	173.255.211.88	192.168.2.4
Nov 21, 2022 04:20:47.797794104 CET	49696	443	192.168.2.4	173.255.211.88
Nov 21, 2022 04:20:47.798702002 CET	49696	443	192.168.2.4	173.255.211.88
Nov 21, 2022 04:20:47.798731089 CET	443	49696	173.255.211.88	192.168.2.4
Nov 21, 2022 04:20:47.975795984 CET	443	49696	173.255.211.88	192.168.2.4
Nov 21, 2022 04:20:47.977385998 CET	49697	443	192.168.2.4	173.255.211.88
Nov 21, 2022 04:20:47.977452040 CET	443	49697	173.255.211.88	192.168.2.4
Nov 21, 2022 04:20:47.977592945 CET	49697	443	192.168.2.4	173.255.211.88
Nov 21, 2022 04:20:47.979526997 CET	49697	443	192.168.2.4	173.255.211.88
Nov 21, 2022 04:20:47.979572058 CET	443	49697	173.255.211.88	192.168.2.4
Nov 21, 2022 04:20:48.151135921 CET	443	49697	173.255.211.88	192.168.2.4
Nov 21, 2022 04:20:48.152781963 CET	49698	443	192.168.2.4	173.255.211.88
Nov 21, 2022 04:20:48.152836084 CET	443	49698	173.255.211.88	192.168.2.4
Nov 21, 2022 04:20:48.152923107 CET	49698	443	192.168.2.4	173.255.211.88
Nov 21, 2022 04:20:48.153774023 CET	49698	443	192.168.2.4	173.255.211.88
Nov 21, 2022 04:20:48.153799057 CET	443	49698	173.255.211.88	192.168.2.4
Nov 21, 2022 04:20:48.328830957 CET	443	49698	173.255.211.88	192.168.2.4
Nov 21, 2022 04:20:53.767379045 CET	49699	7080	192.168.2.4	45.63.99.23
Nov 21, 2022 04:20:56.771694899 CET	49699	7080	192.168.2.4	45.63.99.23
Nov 21, 2022 04:21:02.787986040 CET	49699	7080	192.168.2.4	45.63.99.23
Nov 21, 2022 04:21:09.058938026 CET	49700	443	192.168.2.4	182.162.143.56
Nov 21, 2022 04:21:09.059000969 CET	443	49700	182.162.143.56	192.168.2.4
Nov 21, 2022 04:21:09.059458971 CET	49700	443	192.168.2.4	182.162.143.56
Nov 21, 2022 04:21:09.062942028 CET	49700	443	192.168.2.4	182.162.143.56
Nov 21, 2022 04:21:09.063020945 CET	443	49700	182.162.143.56	192.168.2.4
Nov 21, 2022 04:21:09.821538925 CET	443	49700	182.162.143.56	192.168.2.4
Nov 21, 2022 04:21:09.821768045 CET	49700	443	192.168.2.4	182.162.143.56
Nov 21, 2022 04:21:09.830401897 CET	49700	443	192.168.2.4	182.162.143.56
Nov 21, 2022 04:21:09.830475092 CET	443	49700	182.162.143.56	192.168.2.4
Nov 21, 2022 04:21:09.830936909 CET	443	49700	182.162.143.56	192.168.2.4
Nov 21, 2022 04:21:09.882251024 CET	49700	443	192.168.2.4	182.162.143.56
Nov 21, 2022 04:21:10.165709019 CET	49700	443	192.168.2.4	182.162.143.56
Nov 21, 2022 04:21:10.165743113 CET	443	49700	182.162.143.56	192.168.2.4
Nov 21, 2022 04:21:10.165755987 CET	49700	443	192.168.2.4	182.162.143.56

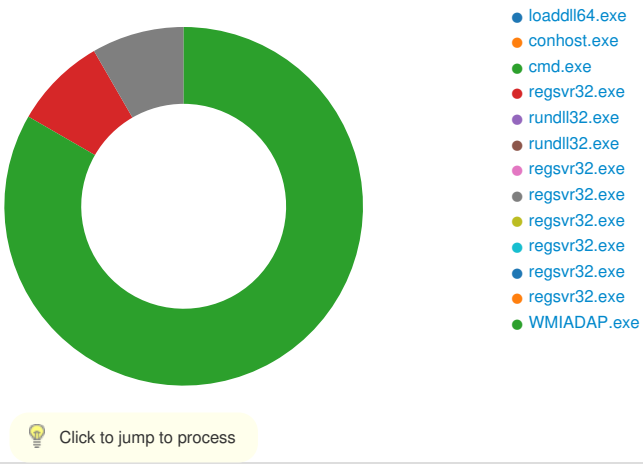
Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 21, 2022 04:21:10.165762901 CET	443	49700	182.162.143.56	192.168.2.4
Nov 21, 2022 04:21:11.838960886 CET	443	49700	182.162.143.56	192.168.2.4
Nov 21, 2022 04:21:11.839132071 CET	443	49700	182.162.143.56	192.168.2.4
Nov 21, 2022 04:21:11.839271069 CET	49700	443	192.168.2.4	182.162.143.56
Nov 21, 2022 04:21:11.840809107 CET	49700	443	192.168.2.4	182.162.143.56
Nov 21, 2022 04:21:11.840810061 CET	49700	443	192.168.2.4	182.162.143.56
Nov 21, 2022 04:21:11.840852022 CET	443	49700	182.162.143.56	192.168.2.4
Nov 21, 2022 04:21:11.840873957 CET	443	49700	182.162.143.56	192.168.2.4

HTTP Request Dependency Graph

- 182.162.143.56

Statistics

Behavior



System Behavior

Analysis Process: loaddll64.exe PID: **3692**, Parent PID: **3528**

General

Target ID:	0
Start time:	04:20:01
Start date:	21/11/2022
Path:	C:\Windows\System32\loaddll64.exe
Wow64 process (32bit):	false
Commandline:	loaddll64.exe "C:\Users\user\Desktop\yoyrJ.dll"
Imagebase:	0x7ff76b0a0000
File size:	139776 bytes
MD5 hash:	C676FC0263EDD17D4CE7D644B8F3FCD6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.322442190.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Emotet_db7d33fa, Description: unknown, Source: 00000000.00000002.322442190.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000000.00000002.322977789.00000141AEEA0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Emotet_db7d33fa, Description: unknown, Source: 00000000.00000002.322977789.00000141AEEA0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **3096**, Parent PID: **3692**

General

Target ID:	1
Start time:	04:20:01
Start date:	21/11/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7c72c0000
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: cmd.exe PID: **976**, Parent PID: **3692**

General

Target ID:	2
Start time:	04:20:02
Start date:	21/11/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd.exe /C rundll32.exe "C:\Users\user\Desktop\yoyrJ.dll",#1
Imagebase:	0x7ff632260000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **5020**, Parent PID: **3692**

General

Target ID:	3
Start time:	04:20:02
Start date:	21/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	regsvr32.exe /s C:\Users\user\Desktop\yoyrJ.dll
Imagebase:	0x7ff7458f0000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.321064194.0000000000A90000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Emotet_db7d33fa, Description: unknown, Source: 00000003.00000002.321064194.0000000000A90000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000003.00000002.322205921.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Emotet_db7d33fa, Description: unknown, Source: 00000003.00000002.322205921.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: unknown
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\System32\UgFJoEzLBQVtMeg\qohQcmrIRynEDAUP.dll:Zone.Identifier	success or wait	1	180027D67	DeleteFileW

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **5288**, Parent PID: **976**

General

Target ID:	4
Start time:	04:20:02
Start date:	21/11/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe "C:\Users\user\Desktop\yoyrJ.dll",#1
Imagebase:	0x7ff6a4af0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.318945591.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Emotet_db7d33fa, Description: unknown, Source: 00000004.00000002.318945591.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000004.00000002.319306896.000001EBD2220000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Emotet_db7d33fa, Description: unknown, Source: 00000004.00000002.319306896.000001EBD2220000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: 5284, Parent PID: 3692

General

Target ID:	5
Start time:	04:20:02
Start date:	21/11/2022
Path:	C:\Windows\System32\rundll32.exe
Wow64 process (32bit):	false
Commandline:	rundll32.exe C:\Users\user\Desktop\yoyrJ.dll,DllRegisterServer
Imagebase:	0x7ff6a4af0000
File size:	69632 bytes
MD5 hash:	73C519F050C20580F8A62C849D49215A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.321445782.000001BBC5810000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Emotet_db7d33fa, Description: unknown, Source: 00000005.00000002.321445782.000001BBC5810000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000005.00000002.320548872.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Emotet_db7d33fa, Description: unknown, Source: 00000005.00000002.320548872.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: unknown
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: 5412, Parent PID: 5288

General

Target ID:	6
Start time:	04:20:07
Start date:	21/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\RPhOZPFULSaJ\nMwLrZYwR.dll"
Imagebase:	0x7ff7458f0000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: 5908, Parent PID: 5020

General	
Target ID:	7
Start time:	04:20:07
Start date:	21/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\UgFJoEzLBQVtMeg\qohQcmrlRynEDAUP.dll"
Imagebase:	0x7ff7458f0000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.828364693.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Emotet_db7d33fa, Description: unknown, Source: 00000007.00000002.828364693.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000007.00000002.827883820.0000000000BA0000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Emotet_db7d33fa, Description: unknown, Source: 00000007.00000002.827883820.0000000000BA0000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Emotet_3, Description: Yara detected Emotet, Source: 00000007.00000002.827986155.0000000000C38000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	qohQcmrlRynEDAUP.dll	unicode	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\UgFJoEzLBQVtMeg\qohQcmrlRynEDAUP.dll"	success or wait	1	180020877	RegSetValueExW

Analysis Process: regsvr32.exe PID: **4644**, Parent PID: **5284**

General	
Target ID:	8
Start time:	04:20:07
Start date:	21/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\YbSMYJyTdzumryV\WWgeEzfCEnB.dll"
Imagebase:	0x7ff7458f0000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **5132**, Parent PID: **3692**

General	
Target ID:	9
Start time:	04:20:08
Start date:	21/11/2022
Path:	C:\Windows\System32\regsvr32.exe

Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\OGxcy\dYkxHTuA.dll"
Imagebase:	0x7ff7458f0000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: 5132, Parent PID: 3528

General

Target ID:	12
Start time:	04:21:26
Start date:	21/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe" "C:\Windows\system32\UgFJoEzLBQVtMeg\qohQcmrlRynEDAUP.dll
Imagebase:	0x7ff7458f0000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.496080462.0000000000D20000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Emotet_db7d33fa, Description: unknown, Source: 0000000C.00000002.496080462.0000000000D20000.00000040.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 0000000C.00000002.496539435.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Emotet_db7d33fa, Description: unknown, Source: 0000000C.00000002.496539435.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: unknown

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: 4192, Parent PID: 5132

General

Target ID:	13
Start time:	04:21:30
Start date:	21/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Users\user\AppData\Local\ArkmTuxCaKyXkTDZ\fBEZnVEOT.dll"
Imagebase:	0x7ff7458f0000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	false
Has administrator privileges:	false

Programmed in:	C, C++ or other language

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: WMIADAP.exe PID: **5412**, Parent PID: **2384**

General

Target ID:	14
Start time:	04:21:50
Start date:	21/11/2022
Path:	C:\Windows\System32\wbem\WMIADAP.exe
Wow64 process (32bit):	false
Commandline:	wmiadap.exe /F /T /R
Imagebase:	0x7ff7ece50000
File size:	177664 bytes
MD5 hash:	9783D0765F31980950445DFD40DB15DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Windows\system32\wbem\Performance\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF7ECE5AA9B	CreateDirectoryW
C:\Windows\system32\wbem\Performance\WmiApRpl_new.h	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF7ECE5AAF3	CreateFileW
C:\Windows\system32\wbem\Performance\	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	7FF7ECE5AA9B	CreateDirectoryW
C:\Windows\system32\wbem\Performance\WmiApRpl_new.ini	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	7FF7ECE5AAF3	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\System32\wbem\Performance\WmiApRpl.h	success or wait	1	7FF7ECE5AE86	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Windows\System32\wbem\Performance\WmiApRpl_new.h	C:\Windows\system32\wbem\Performance\WmiApRpl.h	success or wait	1	7FF7ECE5AE95	MoveFileExW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\System32\wbem\Performance\WmiApRpl_new.h	0	357	2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 2f 0d 0a 2f 2f 0d 0a 2f 2f 20 43 6f 70 79 72 69 67 68 74 20 28 43 29 20 32 30 30 30 20 4d 69 63 72 6f 73 6f 66 74 20 43 6f 72 70 6f 72 61 74 69 6f 6e 0d 0a 2f 2f 0d 0a 2f 2f 20 4d 6f 64 75 6c 65 20 4e 61 6d 65 3a 0d 0a 2f 2f 20 57 6d 69 41 70 52 70 6c 0d 0a 2f 2f 0d 0a 2f 2f 20 41 62 73 74 72 61 63 74 3a 0d 0a 2f 2f 0d 0a 2f 2f 20 49 6e 63 6c 75 64 65 20 66 69 6c 65 20 66 6f 72 20 6f 62 6a 65 63 74 20 61 6e 64 20 63 6f 75 6e 74 65 72 73 20 64 65 66 69 6e 69 74 69 6f 6e 73 2e 0d 0a	////////////////////////////// ////////////////////////////// ////////////////////////////////////// Copyright (C) 2000 Microsoft Corporation//// Module Name:// WmiApRpl//// Abstract://// Include file for object and counters definitions.	success or wait	1	7FF7ECE5A879	WriteFile
C:\Windows\System32\wbem\Performance\WmiApRpl_new.h	357	3087	0d 0a 23 64 65 66 69 6e 65 09 57 4d 49 5f 4f 62 6a 65 63 74 73 09 30 0d 0a 23 64 65 66 69 6e 65 09 48 69 50 65 72 66 5f 43 6c 61 73 73 65 73 09 32 0d 0a 23 64 65 66 69 6e 65 09 48 69 50 65 72 66 5f 56 61 6c 69 64 69 74 79 09 34 0d 0a 0d 0a 23 64 65 66 69 6e 65 09 4d 53 69 53 43 53 49 5f 43 6f 6e 6e 65 63 74 69 6f 6e 53 74 61 74 69 73 74 69 63 73 5f 30 30 30 30 30 09 36 0d 0a 0d 0a 23 64 65 66 69 6e 65 09 42 79 74 65 73 52 65 63 65 69 76 65 64 5f 30 30 30 30 30 09 38 0d 0a 23 64 65 66 69 6e 65 09 42 79 74 65 73 53 65 6e 74 5f 30 30 30 30 30 09 31 30 0d 0a 23 64 65 66 69 6e 65 09 50 44 55 43 6f 6d 6d 61 6e 64 73 53 65 6e 74 5f 30 30 30 30 30 09 31 32 0d 0a 23 64 65 66 69 6e 65 09 50 44 55 52 65 73 70 6f 6e 73 65 73 52 65 63 65 69 76 65 64 5f 30 30 30 30 30	#defineWMI_Objects0#defineHiPerf_Classes2#defineHiPerf_Validity4#defineMSiSCSI_ConnectionStatistics_000006#defineBytesReceived_000008#defineBytesSent_0000010#definePDUCommandsSent_0000012#definePDUResponsesReceived_00000	success or wait	1	7FF7ECE5A879	WriteFile
unknown	0	2	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF7ECE5CB1C	WriteFile
unknown	2	922	75 6e 6b 6e 6f 77 6e	unknown	success or wait	1	7FF7ECE5A92F	WriteFile

Disassembly

No disassembly