ID: 492876
Sample Name: RpcNs4.exe
Cookbook: default.jbs
Time: 04:13:11
Date: 29/09/2021
Version: 33.0.0 White Diamond

Table of Contents

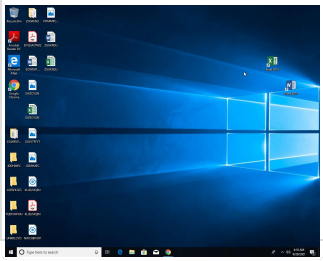
Windows Analysis Report RpcNs4.exe

Overview

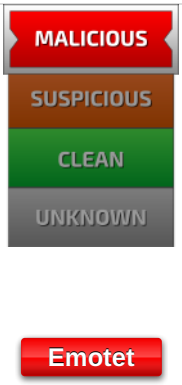
General Information

Sample Name:	RpcNs4.exe
Analysis ID:	492876
MD5:	1ed37c4a225bbd..
SHA1:	51caf718c3d8584..
SHA256:	8b504e796986fba.
Infos:	

Most interesting Screenshot:



Detection



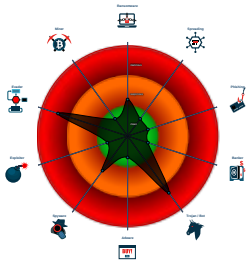
Emotet

Score:	96
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Antivirus / Scanner detection for sub…
- Yara detected Emotet
- Changes security center settings (no…
- Machine Learning detection for samp…
- Found evasive API chain (may stop…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Drops executables to the windows d…
- Uses 32bit PE files
- Queries the volume information (nam…

Classification



Process Tree

- **System is w10x64**
- RpcNs4.exe (PID: 5968 cmdline: 'C:\Users\user\Desktop\RpcNs4.exe' MD5: 1ED37C4A225BBD35716CF241E14541A8)
  - networkitemfactory.exe (PID: 900 cmdline: C:\Windows\SysWOW64\rasphone\networkitemfactory.exe MD5: 1ED37C4A225BBD35716CF241E14541A8)
- svchost.exe (PID: 4840 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 3228 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 4228 cmdline: C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5992 cmdline: c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 2852 cmdline: c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 5984 cmdline: C:\Windows\System32\svchost.exe -k NetworkService -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- SgrmBroker.exe (PID: 1752 cmdline: C:\Windows\system32\SgrmBroker.exe MD5: D3170A3F3A9626597EEE1888686E3EA6)
- svchost.exe (PID: 5780 cmdline: c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc MD5: 32569E403279B3FD2EDB7EBD036273FA)
  - MpCmdRun.exe (PID: 2252 cmdline: 'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable MD5: A267555174BFA53844371226F482B86B)
    - conhost.exe (PID: 4636 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- svchost.exe (PID: 328 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- svchost.exe (PID: 1560 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)
- **cleanup**

Malware Configuration

Threatname: Emotet


```
{
  "RSA Public Key":
"MHwwDQYJKoZIhvcNAQEBBQADawAwaAJhAM/TXLLvX91I6dVMYe+T1PPO6mpcg7OJ\ncMl9o/g4nUhZOp8fAAmQl8XMXeGvDhZXTyX1AXf401iPFui0RB6glhl/7/djvi7j\nl32lAhyBANpKGty8xf3J5kGwwClnG/CXHQIDAQAB",
  "C2 list": [
    "190.191.171.72:80",
    "5.189.168.53:8080",
    "162.241.41.111:7080",
    "190.85.46.52:7080",
    "37.205.9.252:7080",
    "172.96.190.154:8080",
    "120.51.34.254:80",
    "181.95.133.104:80",
    "139.59.61.215:443",
    "157.7.164.178:8081",
    "41.185.29.128:8080",
    "86.57.216.23:80",
    "185.80.172.199:80",
    "54.38.143.245:8080",
    "41.212.89.128:80"
```

```
    "223.17.215.76:80",
    "37.187.100.220:7080",
    "167.71.227.113:8080",
    "8.4.9.137:8080",
    "113.160.248.110:80",
    "220.147.247.145:80",
    "60.125.114.64:443",
    "182.227.240.189:443",
    "45.177.120.37:8080",
    "103.229.73.17:8080",
    "117.247.235.44:80",
    "115.78.11.155:80",
    "79.133.6.236:8080",
    "139.59.12.63:8080",
    "91.83.93.103:443",
    "186.20.52.237:80",
    "185.208.226.142:8080",
    "115.79.195.246:80",
    "116.202.10.123:8080",
    "162.144.42.60:8080",
    "185.142.236.163:443",
    "172.105.78.244:8080",
    "37.46.129.215:8080",
    "157.245.138.101:7080",
    "182.253.83.234:7080",
    "143.95.101.72:8080",
    "187.189.66.200:8080",
    "103.48.68.173:80",
    "200.116.93.61:80",
    "223.135.30.189:80",
    "36.91.44.183:80",
    "198.57.203.63:8080",
    "203.153.216.178:7080",
    "46.32.229.152:8080",
    "51.38.201.19:7080",
    "103.93.220.182:80",
    "103.133.66.57:443",
    "202.166.170.43:80",
    "95.216.205.155:8080",
    "77.74.78.80:443",
    "78.114.175.216:80",
    "189.150.209.206:80",
    "113.156.82.32:80",
    "58.27.215.3:8080",
    "192.241.220.183:8080",
    "185.86.148.68:443",
    "74.208.173.91:8080",
    "126.126.139.26:443",
    "88.247.58.26:80",
    "49.243.9.118:80",
    "2.144.244.204:80",
    "138.201.45.2:8080",
    "91.75.75.46:80",
    "119.92.77.17:80",
    "202.153.220.157:80",
    "46.105.131.68:8080",
    "178.33.167.120:8080",
    "190.192.39.136:80",
    "115.176.16.221:80",
    "179.5.118.12:80",
    "190.190.15.20:80",
    "113.161.148.81:80",
    "14.241.182.160:80",
    "192.163.221.191:8080",
    "128.106.187.110:80",
    "190.194.12.132:80",
    "75.127.14.170:8080",
    "195.201.56.70:8080",
    "118.243.83.70:80",
    "50.116.78.109:8080",
    "192.210.217.94:8080",
    "103.80.51.61:8080"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000004.00000002.517659433.0000000000510000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	

Source	Rule	Description	Author	Strings
00000002.00000002.256801219.00000000005F4000.00000004.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000004.00000002.519092750.00000000020B1000.00000020.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000002.00000002.256746048.00000000005E0000.00000040.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
00000004.00000002.519022380.0000000002094000.00000004.00000001.sdmp	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 1 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.RpcNs4.exe.5e279e.1.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
2.2.RpcNs4.exe.20b0000.3.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
4.2.networkitemfactory.exe.51279e.1.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
2.2.RpcNs4.exe.5e052e.2.raw.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
4.2.networkitemfactory.exe.20b0000.3.unpack	JoeSecurity_Emotet	Yara detected Emotet	Joe Security	
Click to see the 5 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Antivirus / Scanner detection for submitted sample

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Emotet

Persistence and Installation Behavior:

Drops executables to the windows directory (C:\Windows) and starts them

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Found evasive API chain (may stop execution after reading information in the PEB, e.g. number of processors)

Lowering of HIPS / PFW / Operating System Security Settings:

Changes security center settings (notifications, updates, antivirus, firewall)

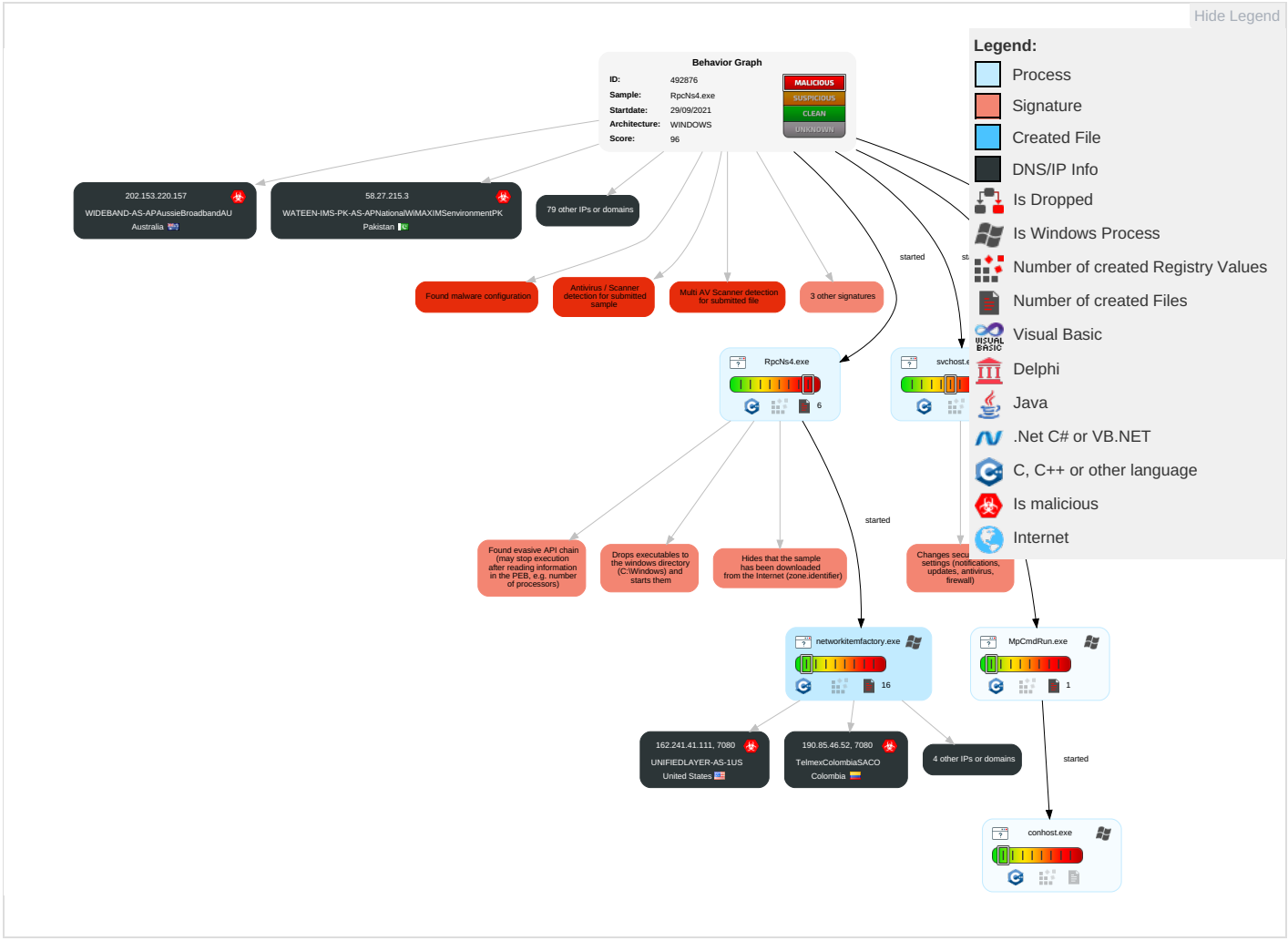
Stealing of Sensitive Information:

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	Networ Effects
Valid Accounts	Windows Management Instrumentation 1	Windows Service 1	Windows Service 1	Masquerading 1 2 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesd Insecur Networ Commu
Default Accounts	Native API 1 1	DLL Side-Loading 1	Process Injection 2	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 6 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Standard Port 1	Exploit Redirec Calls/SI
Domain Accounts	At (Linux)	Application Shimming 1	DLL Side-Loading 1	Virtualization/Sandbox Evasion 2	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 1	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Application Shimming 1	Process Injection 2	NTDS	Process Discovery 3	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipu Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Hidden Files and Directories 1	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammin Denial Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 2	DCSync	System Information Discovery 4 5	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	DLL Side-Loading 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgr Insecur Protoco
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 Base St

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
RpcNs4.exe	78%	Virustotal		Browse
RpcNs4.exe	74%	Metadefender		Browse
RpcNs4.exe	89%	ReversingLabs	Win32.Trojan.Emotet	
RpcNs4.exe	100%	Avira	TR/AD.Emotet.dbl	
RpcNs4.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.RpcNs4.exe.20b0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
4.2.networkitemfactory.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1138861		Download File
2.2.RpcNs4.exe.5e279e.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.2.RpcNs4.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1138861		Download File
4.2.networkitemfactory.exe.51052e.2.unpack	100%	Avira	HEUR/AGEN.1142428		Download File
2.2.RpcNs4.exe.5e052e.2.unpack	100%	Avira	HEUR/AGEN.1142428		Download File
4.0.networkitemfactory.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1138861		Download File
4.2.networkitemfactory.exe.51279e.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
4.2.networkitemfactory.exe.20b0000.3.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
2.0.RpcNs4.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1138861		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://5.189.168.53:8080/o3fBhuuz/	0%	Avira URL Cloud	safe	
http://162.241.41.111:7080/LYQRy6c93vecgvHJfH5/EZsl1rJ8QXw/bisGJm2RzFKv/0FbacJYj1q62Xn/2	0%	Avira URL Cloud	safe	
http://172.96.190.154:8080/yTJ2v9/Gv4Y0SVYAXfP/7otgMR8dm3c0Q43/p	0%	Avira URL Cloud	safe	
http://190.191.171.72/e7oyvJu0ryVUBL/0INT0lnzMU2/MpBFVePNcAJo4Omc/IfhZZOLYmyGUpB2z7/y67uuC8o/	0%	Avira URL Cloud	safe	
http://172.96.190.154:8080/yTJ2v9/Gv4Y0SVYAXfP/7otgMR8dm3c0Q43/c/IfhZZOLYmyGUpB2z7/y67uuC8o/	0%	Avira URL Cloud	safe	
http://5.189.168.53:8080/o3fBhuuz/m	0%	Avira URL Cloud	safe	
http://5.189.168.53:8080/o3fBhuuz/i	0%	Avira URL Cloud	safe	
http://190.85.46.52:7080/1CMBtWf1oEz5/	0%	Avira URL Cloud	safe	
http://172.96.190.154:8080/yTJ2v9/Gv4Y0SVYAXfP/7otgMR8dm3c0Q43/	0%	Avira URL Cloud	safe	
http://190.85.46.52:7080/1CMBtWf1oEz5/f	0%	Avira URL Cloud	safe	
http://crl.ver)	0%	Avira URL Cloud	safe	
http://172.96.190.154:8080/yTJ2v9/Gv4Y0SVYAXfP/7otgMR8dm3c0Q43/5	0%	Avira URL Cloud	safe	
http://https://%s.xboxlive.com	0%	URL Reputation	safe	
http://5.189.168.53:8080/o3fBhuuz/3	0%	Avira URL Cloud	safe	
http://https://dynamic.t	0%	URL Reputation	safe	
http://162.241.41.111:7080/LYQRy6c93vecgvHJfH5/EZsl1rJ8QXw/bisGJm2RzFKv/0FbacJYj1q62Xn/	0%	Avira URL Cloud	safe	
http://190.85.46.52:7080/1CMBtWf1oEz5/m32	0%	Avira URL Cloud	safe	
http://5.189.168.53:8080/o3fBhuuz/#	0%	Avira URL Cloud	safe	
http://37.205.9.252:7080/RFYvVKd2K/sy7dp7xsNv9/Rrh3Sh9wg/SwbGDOylYnDUpHudO/ri7bprIvQeGD/Bd2yo6ti2p6c	0%	Avira URL Cloud	safe	
http://https://%s.dnet.xboxlive.com	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
126.126.139.26	unknown	Japan		17676	GIGAINFRASoftbankBBCorpJP	true
192.210.217.94	unknown	United States		36352	AS-COLOCROSSINGUS	true
223.17.215.76	unknown	Hong Kong		18116	HGC-AS-APHGCGlobalCommunicationsLimitedHK	true
185.208.226.142	unknown	Hungary		43359	TARHELYHU	true
14.241.182.160	unknown	Viet Nam		45899	VNPT-AS-VNVNPTCorpVN	true
75.127.14.170	unknown	United States		36352	AS-COLOCROSSINGUS	true
172.96.190.154	unknown	Canada		59253	LEASEWEB-APAC-SIN-11LeasewebAsiaPacificpteltdSG	true
78.114.175.216	unknown	France		8228	CEGETEL-ASFR	true
51.38.201.19	unknown	France		16276	OVHFR	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
200.116.93.61	unknown	Colombia		13489	EPMTelecomunicacionesSAESPCO	true
115.78.11.155	unknown	Viet Nam		7552	VIETEL-AS-APViettelGroupVN	true
203.153.216.178	unknown	Indonesia		45291	SURF-IDPTSurfindoNetworkID	true
190.191.171.72	unknown	Argentina		10481	TelecomArgentinaSAAR	true
220.147.247.145	unknown	Japan		2510	INFOWEBFUJITSULIMITEDJP	true
143.95.101.72	unknown	United States		62729	ASMALLORANGE1US	true
5.189.168.53	unknown	Germany		51167	CONTABODE	true
113.156.82.32	unknown	Japan		2516	KDDIKDDICORPORATIONJP	true
103.229.73.17	unknown	Indonesia		55660	MWN-AS-IDPTMasterWebNetworkID	true
182.227.240.189	unknown	Korea Republic of		17858	POWERVIS-AS-KRLGPOWERCOMMKR	true
178.33.167.120	unknown	France		16276	OVHFR	true
162.144.42.60	unknown	United States		46606	UNIFIEDLAYER-AS-1US	true
190.190.15.20	unknown	Argentina		10481	TelecomArgentinaSAAR	true
95.216.205.155	unknown	Germany		24940	HETZNER-ASDE	true
37.187.100.220	unknown	France		16276	OVHFR	true
41.212.89.128	unknown	Kenya		15399	WANANCHI-KE	true
190.85.46.52	unknown	Colombia		14080	TelmexColombiaSACO	true
120.51.34.254	unknown	Japan		2519	VECTANTARTERIANetworksCorporationJP	true
187.189.66.200	unknown	Mexico		22884	TOTALPLAYTELECOMUNICACIONESSADECVMX	true
88.247.58.26	unknown	Turkey		9121	TTNETTR	true
103.93.220.182	unknown	Philippines		17639	CONVERGE-ASConvergeICTSolutionsIncPH	true
181.95.133.104	unknown	Argentina		7303	TelecomArgentinaSAAR	true
117.247.235.44	unknown	India		9829	BSNL-NIBNationalInternetBackboneIN	true
138.201.45.2	unknown	Germany		24940	HETZNER-ASDE	true
37.205.9.252	unknown	Czech Republic		24971	MASTER-ASCzechRepublicwwwmasterczCZ	true
190.194.12.132	unknown	Argentina		10481	TelecomArgentinaSAAR	true
186.20.52.237	unknown	Chile		6535	TelmexServiciosEmpresarialesSACL	true
118.243.83.70	unknown	Japan		4685	ASAHI-NETAsahiNetJP	true
103.80.51.61	unknown	Thailand		136023	PTE-AS-APPTEGroupCoLtdTH	true
103.48.68.173	unknown	India		17754	EXCELL-ASExcellmediaIN	true
185.86.148.68	unknown	Latvia		52173	MAKONIXLV	true
103.133.66.57	unknown	India		138520	LNSPL-AS-APLaluNetworkSolutionsPrivateLimitedIN	true
157.245.138.101	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
119.92.77.17	unknown	Philippines		9299	IPG-AS-APPhilippineLongDistanceTelephoneCompanyPH	true
46.105.131.68	unknown	France		16276	OVHFR	true
172.105.78.244	unknown	United States		63949	LINODE-APLinodeLLCUS	true
37.46.129.215	unknown	Russian Federation		29182	THEFIRST-ASRU	true
192.163.221.191	unknown	United States		46606	UNIFIEDLAYER-AS-1US	true
162.241.41.111	unknown	United States		46606	UNIFIEDLAYER-AS-1US	true
190.192.39.136	unknown	Argentina		10481	TelecomArgentinaSAAR	true
45.177.120.37	unknown	Brazil		268987	NETLIMITTELECOMBR	true
202.166.170.43	unknown	Pakistan		55501	CONNECTEL-PK141-143MaulanaShaukatAliRoadPK	true
86.57.216.23	unknown	Belarus		6697	BELPAK-ASBELPAKBY	true
113.161.148.81	unknown	Viet Nam		45899	VNPT-AS-VNVNPTCorpVN	true
157.7.164.178	unknown	Japan		7506	INTERQGMOInternetIncJP	true
116.202.10.123	unknown	Germany		24940	HETZNER-ASDE	true
192.241.220.183	unknown	United States		14061	DIGITALOCEAN-ASNUS	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
115.176.16.221	unknown	Japan		2510	INFOWEBFUJITSULIMITED JP	true
198.57.203.63	unknown	United States		46606	UNIFIEDLAYER-AS-1US	true
46.32.229.152	unknown	United Kingdom		20738	GD-EMEA-DC-LD5GB	true
167.71.227.113	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
54.38.143.245	unknown	France		16276	OVHFR	true
77.74.78.80	unknown	Russian Federation		31261	GARS-ASMoscowRussiaRU	true
49.243.9.118	unknown	Japan		10013	FBDCFreeBitCoLtdJP	true
8.4.9.137	unknown	United States		3356	LEVEL3US	true
60.125.114.64	unknown	Japan		17676	GIGAINFRASoftbankBBCorp JP	true
113.160.248.110	unknown	Viet Nam		45899	VNPT-AS-VNVNPTCorpVN	true
79.133.6.236	unknown	Finland		3238	ALCOMFI	true
189.150.209.206	unknown	Mexico		8151	UninetSAdeCVMX	true
58.27.215.3	unknown	Pakistan		38264	WATEEN-IMS-PK-AS-APNationalWiMAXIMSenvironmentPK	true
185.80.172.199	unknown	Azerbaijan		39232	UNINETAZ	true
74.208.173.91	unknown	United States		8560	ONEANDONE-ASBrauerstrasse48DE	true
41.185.29.128	unknown	South Africa		36943	GridhostZA	true
223.135.30.189	unknown	Japan		2527	SO-NETSo-netEntertainmentCorporation JP	true
139.59.61.215	unknown	Singapore		14061	DIGITALOCEAN-ASNUS	true
91.75.75.46	unknown	United Arab Emirates		15802	DU-AS1AE	true
50.116.78.109	unknown	United States		46606	UNIFIEDLAYER-AS-1US	true
128.106.187.110	unknown	Singapore		9506	SINGTEL-FIBRESingtelFibreBroadbandSG	true
202.153.220.157	unknown	Australia		4764	WIDEBAND-AS-APAussieBroadbandAU	true
139.59.12.63	unknown	Singapore		14061	DIGITALOCEAN-ASNUS	true
115.79.195.246	unknown	Viet Nam		7552	VIETEL-AS-APViettelGroupVN	true
185.142.236.163	unknown	Netherlands		174	COGENT-174US	true
2.144.244.204	unknown	Iran (ISLAMIC Republic Of)		44244	IRANCELL-ASIR	true
182.253.83.234	unknown	Indonesia		17451	BIZNET-AS-APBIZNETNETWORKSID	true
179.5.118.12	unknown	El Salvador		14754	TelguaGT	true
91.83.93.103	unknown	Hungary		12301	INVITECHHU	true
195.201.56.70	unknown	Germany		24940	HETZNER-ASDE	true
36.91.44.183	unknown	Indonesia		17974	TELKOMNET-AS2-APPTTelekomunikasiIndonesiaID	true

Private

IP
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	492876
Start date:	29.09.2021
Start time:	04:13:11
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RpcNs4.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:	25
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:	mal96.troj.evad.winEXE@16/5@0/88
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 72.1% (good quality ratio 69%) • Quality average: 82.8% • Quality standard deviation: 26.7%
HCA Information:	• Successful, ratio: 86% • 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
04:14:16	API Interceptor	2x Sleep call for process: svchost.exe modified
04:15:32	API Interceptor	1x Sleep call for process: MpCmdRun.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
126.126.139.26	sample1.doc	Get hash	malicious	Browse	
	MV9tCJw8Xr.exe	Get hash	malicious	Browse	
192.210.217.94	sample1.doc	Get hash	malicious	Browse	
	MV9tCJw8Xr.exe	Get hash	malicious	Browse	
223.17.215.76	sample1.doc	Get hash	malicious	Browse	
	MV9tCJw8Xr.exe	Get hash	malicious	Browse	
185.208.226.142	sample1.doc	Get hash	malicious	Browse	
	MV9tCJw8Xr.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
GIGAINFRASoftbankBBCorpJP	arm	Get hash	malicious	Browse	• 133.121.255.44
	Le85313EpP	Get hash	malicious	Browse	• 126.240.223.57
	46gV91KJhQ	Get hash	malicious	Browse	• 220.38.228.196
	x86	Get hash	malicious	Browse	• 218.133.10 8.199

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	arm	Get hash	malicious	Browse	• 126.32.30.5
	RaVPWTArgG	Get hash	malicious	Browse	• 218.178.205.12
	b2wx6oZNsC	Get hash	malicious	Browse	• 219.212.202.78
	mirkatclpb.x86	Get hash	malicious	Browse	• 126.174.10 3.192
	mirkatclpb.arm	Get hash	malicious	Browse	• 221.87.174.160
	ho4yrUrdk1	Get hash	malicious	Browse	• 221.77.141.3
	qJvDfzBXbs	Get hash	malicious	Browse	• 126.11.242.65
	uTfW1dzdIk	Get hash	malicious	Browse	• 60.107.73.68
	G3kV1FpdsS	Get hash	malicious	Browse	• 220.61.174.7
	Sht1aYGDIX	Get hash	malicious	Browse	• 126.184.36.243
	8u6nZbyMxl	Get hash	malicious	Browse	• 126.210.43.40
	TfaQUm3e4Y	Get hash	malicious	Browse	• 220.47.221.201
	sora.arm7	Get hash	malicious	Browse	• 126.27.223.210
	L3Gl0GugHo	Get hash	malicious	Browse	• 219.213.5.22
	Q7rLYKgTht	Get hash	malicious	Browse	• 126.175.55.215
	F0ZMmHZif5	Get hash	malicious	Browse	• 220.34.5.157
AS-COLOCROSSINGUS	Suppression .xlsx	Get hash	malicious	Browse	• 107.172.73.191
	Notification.xlsx	Get hash	malicious	Browse	• 107.172.93.32
	swift confrimation copy.xlsx	Get hash	malicious	Browse	• 192.3.141.149
	ORDERCONFIRMATION_00001679918.xlsx	Get hash	malicious	Browse	• 23.94.159.204
	suppression des suspensions.xlsx	Get hash	malicious	Browse	• 107.172.73.191
	rrVvnZMcFs	Get hash	malicious	Browse	• 23.94.26.138
	pAu4km62R9	Get hash	malicious	Browse	• 23.94.26.138
	kUFNxyzq7h	Get hash	malicious	Browse	• 23.94.26.138
	RPM.xlsx	Get hash	malicious	Browse	• 23.95.13.176
	OOLU2032650751.doc	Get hash	malicious	Browse	• 107.175.64.227
	Invoice PO.doc	Get hash	malicious	Browse	• 107.175.64.227
	MOQ-Request_0927210-006452.xlsx	Get hash	malicious	Browse	• 107.173.21 9.122
	RFQ_final version.xlsx	Get hash	malicious	Browse	• 107.173.21 9.122
	New Price List.xlsx	Get hash	malicious	Browse	• 192.227.22 5.173
	RFQ.xlsx	Get hash	malicious	Browse	• 23.94.159.207
	RFQ.xlsx	Get hash	malicious	Browse	• 23.94.159.207
	X86_64	Get hash	malicious	Browse	• 172.245.16 8.189
	RQcnbthZwW	Get hash	malicious	Browse	• 172.245.16 8.189
	haK4nXUWd3	Get hash	malicious	Browse	• 172.245.16 8.189
	YIjCULj55a	Get hash	malicious	Browse	• 172.245.16 8.189

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Network\Downloader\edb.log

Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	4096
Entropy (8bit):	0.5961753579683815
Encrypted:	false
SSDEEP:	6:bJtk1GaD0JOCEfMuaaD0JOCEfMKQmD7/tAl/gz2cE0fMbhEZolrRSQ2hyYIIT:boGaD0JcaaD0JwQQ7/tAg/0bjSQJ
MD5:	FEDBD07F059E293B1CD3A36CE0BF727A

C:\ProgramData\Microsoft\Network\Downloader\edb.log	
SHA1:	C75214CD386425539B6F6CFD4F48F90753ECC8E7
SHA-256:	5F2FC139A11B5A3E93489883C7A89D0E8B1A4041C87A7ECCEC784845724B031F
SHA-512:	2C6E4AAEA9EFB60D669ED1E420000D09300C46718D9C113DD7A3043703C0BAADFEB9768C78FC80CB5419A1CA845E5985045D452B90EF0FFFFBC0F252CCF7036
Malicious:	false
Preview:	....E..h..(.....y..... ..1C:\ProgramData\Microsoft\Network\Downloader\..... .....C:\ProgramData\Microsoft\Network\Downloader\..... .....0u.....@...@.....y.....&.....e.f.3...w.....3...w.....h..C.:.\.P.r.o.g.r.a.m .D.a.t.a.\.M.i.c.r.o.s.o.f.t.\.N.e.t.w.o.r.k.\.D.o.w.n.l.o.a.d.e.r.\.q.m.g.r...d.b...G..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.db	
Process:	C:\Windows\System32\svchost.exe
File Type:	Extensible storage engine DataBase, version 0x620, checksum 0xa82e71d7, page size 16384, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	32768
Entropy (8bit):	0.09679207472564298
Encrypted:	false
SSDEEP:	6:BOzzwl/+0XRIE11Y8TRXQlFHKrOzzwl/+0XRIE11Y8TRXQlFHK:K0+0XO4blQlFHKA0+0XO4blQlFHK
MD5:	CDEE6462BDFBADCE486062CB208FC2D9
SHA1:	8DB277B7CA8CCF9AFDA1AAB7A52FDA9FBAE4FC53
SHA-256:	7CFEB754B63AD2FB2518B163B7626B390B012D8A21773FE973F30E3923A7CC7A
SHA-512:	73DA8F7A98AAB76E4955CB961CBC688C69FB07EF9FD59DCDFAC6A1F379515E7BA1FA601572CAD8400DF8D84E45B7320BC65A767C67A132C5DF53E6147856530
Malicious:	false
Preview:	..q.... .....e.f.3...w.....&.....w.....y..h.(.....3...w.....B.....@..... ....3...w..... .....'J!.....y.....n.....y..... .....

C:\ProgramData\Microsoft\Network\Downloader\qmgr.jfm	
Process:	C:\Windows\System32\svchost.exe
File Type:	data
Category:	dropped
Size (bytes):	8192
Entropy (8bit):	0.1120151278868993
Encrypted:	false
SSDEEP:	3:+G1Ev1oj8l/bJdAtiE1Tll:pQKj8t4np
MD5:	CEFA19C920301379F5EF73328CDDC635
SHA1:	C2E331B44A1FD9E196F915D0E12208220B4D7A40
SHA-256:	3874419093305358718AEF8A3E11991C90376C705A62C9599D5F0FBCA8F9D678
SHA-512:	79A5FB2F15E7C11D28D6CFBB127C4F775AC64F5CFA409FD8E486995DAC171E7BFB870CC19D6BE84567619159BAEBC07E7B197C4C83611F384AE73C8911B14E9
Malicious:	false
Preview:	H..a.....3...w.....y.....w.....w.....w....:O.....w.....n.....y..... ....

C:\Windows\ServiceProfiles\LocalService\AppData\Local\FontCache\Fonts\Download-1.tmp	
Process:	C:\Windows\System32\svchost.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	55
Entropy (8bit):	4.306461250274409
Encrypted:	false
SSDEEP:	3:YDQRWu83XfAw2fHbY:YMRl83Xt2f7Y
MD5:	DCA83F08D448911A14C22EBCACC5AD57
SHA1:	91270525521B7FE0D986DB19747F47D34B6318AD
SHA-256:	2B4B2D4A06044AD0BD2AE3287CFCBECD90B959FEB2F503AC258D7C0A235D6FE9
SHA-512:	96F3A02DC4AE302A30A376FC7082002065C7A35ECB74573DE66254EFD701E8FD9E9D867A2C8ABEB4C482738291B715D4965A0D2412663FDF1EE6CBC0BA9FBA
Malicious:	false
Preview:	{"fontSetUri":"fontset-2017-04.json","baseUri":"fonts"}

C:\Windows\ServiceProfiles\LocalService\AppData\Local\Temp\MpCmdRun.log	
Process:	C:\Program Files\Windows Defender\MpCmdRun.exe
File Type:	data
Category:	modified
Size (bytes):	906
Entropy (8bit):	3.148114293486276
Encrypted:	false
SSDEEP:	12:58KRBubdpkoF1AG3rlsQlwAuXURk9+MlWlLehB4yAq7ejCEsQlwAuXUw:OaqdmuF3rlp+z+kWReH4yJ7MNp+Z
MD5:	19E4C16502BE85E35AE649BCC464A2FC
SHA1:	5F2C7E7EDDE9D2FB82173C8D2D475261962B6EC8
SHA-256:	DF3C8E555F788FD5070E09BE94C3C9E6D1BEEF3F1B56AC5BE54F99EEB2DAA57D
SHA-512:	04F1E4A94FA9351E3CE88A8DC62453D19FDCD211C61EC1518D40F97DEC3ACD6BE65A2BFABD8E1BA8B4E449F276C694DF8804AA5D75EFF04DD2585D351A2AA CEB
Malicious:	false
Preview:	........-.....M.p.C.m.d.R.u.n.:. .C.o.m.m.a.n.d. .L.i.n.e.:. .".C.:.\.P.r.o.g.r.a.m. .F.i.l.e.s.\.W.i.n.d.o.w.s. .D.e.f.e.n.d.e.r.\.m.p.c.m.d.r.u.n...e.x.e.". .-.w.d.e.n.a.b.l.e..... .S.t.a.r.t. .T.i.m.e.:. .. W.e.d. .. S.e.p. .. 2.9. .. 2.0.2.1. .0.4.:.1.5.:.3. 2.........M.p.E.n.s.u.r.e.P.r.o.c.e.s.s.M.i.t.i.g.a.t.i.o.n.P.o.l.i.c.y.:. .h.r. .=. .0.x.1.....W.D.E.n.a.b.l.e.....E.R.R.O.R.:. .M.p.W.D.E.n.a.b.l.e.(.T.R.U.E.). .f.a.i.l.e.d. .(.8.0.0.7.0. 4.E.C.).....M.p.C.m.d.R.u.n.:. .E.n.d. .T.i.m.e.:. .. W.e.d. .. S.e.p. .. 2.9. .. 2.0.2.1. .0.4.:.1.5.:.3.2.....-.....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.227386311899768
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	RpcNs4.exe
File size:	310784
MD5:	1ed37c4a225bbd35716cf241e14541a8
SHA1:	51caf718c3d85847e9f9246b291149a0a7afb698
SHA256:	8b504e796986fbae7d1bea49c95dfad222758cca5cada56 472f40a0bde41e485
SHA512:	fa54f2057b8e85c1a84307ee2325cda4393960ca81efe87 e929dd5e19516e62604b9081d0964c23b2e8d97fc7a02d 5b66a952dc0771a5249cf10074fa765a5e3
SSDEEP:	3072:sNzPwNwAtJKqgYLdcF7pGG7MjzQP3xswlVQN2 Lxu2ntX8NUX7uFLuloc:sJPwNwAt/T2F7JcN8U2tM6iV8
File Content Preview:	MZ......................@...!..L.!Th is program cannot be run in DOS mode....$............u.U.u .U.u.U.'.U.u.U.'8U.u.U.'.U.u.Uy.,U.u.U.u.U.u.U...U.u.U..; U.u.U.'<U.u.U.upU.u.U..9U.u.URich.u.U................PE..L. .

File Icon

Icon Hash:	317971b1b1b1b1b0

Static PE Info

General

Entrypoint:	0x402aec
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, NX_COMPAT
Time Stamp:	0x5F68E28E [Mon Sep 21 17:27:42 2020 UTC]
TLS Callbacks:	

General

CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	81f57b81eb6db8b252da01e9143dfb75

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x2a1d1	0x2a200	False	0.40440699184	data	5.8183204417	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x2c000	0x8c7c	0x8e00	False	0.263011663732	data	3.37323787881	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x35000	0x3c20	0x1a00	False	0.244891826923	data	2.84139335758	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0x39000	0xfb9	0x1000	False	0.3642578125	data	4.6782022268	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x3a000	0x13d10	0x13e00	False	0.767614976415	data	6.94887089309	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x4e000	0x207f	0x2200	False	0.650620404412	data	5.98371531894	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Exports

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
09/29/21-04:15:05.886157	ICMP	399	ICMP Destination Unreachable Host Unreachable			108.167.150.86	192.168.2.5
09/29/21-04:15:08.898226	ICMP	399	ICMP Destination Unreachable Host Unreachable			108.167.150.86	192.168.2.5
09/29/21-04:15:14.914137	ICMP	399	ICMP Destination Unreachable Host Unreachable			108.167.150.86	192.168.2.5

Network Port Distribution

TCP Packets

UDP Packets

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: RpcNs4.exe PID: 5968 Parent PID: 2092

General

Start time:	04:14:12
Start date:	29/09/2021
Path:	C:\Users\user\Desktop\RpcNs4.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\RpcNs4.exe'
Imagebase:	0x400000
File size:	310784 bytes
MD5 hash:	1ED37C4A225BBD35716CF241E14541A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000002.00000002.256801219.00000000005F4000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000002.00000002.256746048.00000000005E0000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000002.00000002.257541494.00000000020B1000.00000020.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Deleted

Analysis Process: networkitemfactory.exe PID: 900 Parent PID: 5968

General

Start time:	04:14:14
Start date:	29/09/2021
Path:	C:\Windows\SysWOW64\rasphone\networkitemfactory.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rasphone\networkitemfactory.exe

Imagebase:	0x400000
File size:	310784 bytes
MD5 hash:	1ED37C4A225BBD35716CF241E14541A8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000004.00000002.517659433.0000000000510000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000004.00000002.519092750.00000000020B1000.00000020.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Emotet, Description: Yara detected Emotet, Source: 00000004.00000002.519022380.0000000002094000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

Analysis Process: svchost.exe PID: 4840 Parent PID: 556

General

Start time:	04:14:16
Start date:	29/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p -s BITS
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Analysis Process: svchost.exe PID: 3228 Parent PID: 556

General

Start time:	04:14:20
Start date:	29/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 4228 Parent PID: 556

General

Start time:	04:14:26
Start date:	29/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted -p -s NcbService
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 5992 Parent PID: 556

General

Start time:	04:14:27
Start date:	29/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservice -p -s CDPSvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 2852 Parent PID: 556

General

Start time:	04:14:28
Start date:	29/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k networkservice -p -s DoSvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 5984 Parent PID: 556

General

Start time:	04:14:29
Start date:	29/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k NetworkService -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: SgrmBroker.exe PID: 1752 Parent PID: 556

General

Start time:	04:14:30
Start date:	29/09/2021
Path:	C:\Windows\System32\SgrmBroker.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\SgrmBroker.exe
Imagebase:	0x7ff6ee970000
File size:	163336 bytes
MD5 hash:	D3170A3F3A9626597EEE1888686E3EA6
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 5780 Parent PID: 556

General

Start time:	04:14:30
Start date:	29/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	c:\windows\system32\svchost.exe -k localservicenetworkrestricted -p -s wscsvc
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

Registry Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 328 Parent PID: 556

General

Start time:	04:14:36
Start date:	29/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000

File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: svchost.exe PID: 1560 Parent PID: 556

General

Start time:	04:14:46
Start date:	29/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff797770000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: MpCmdRun.exe PID: 2252 Parent PID: 5780

General

Start time:	04:15:31
Start date:	29/09/2021
Path:	C:\Program Files\Windows Defender\MpCmdRun.exe
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Windows Defender\mpcmdrun.exe' -wdenable
Imagebase:	0x7ff71de40000
File size:	455656 bytes
MD5 hash:	A267555174BFA53844371226F482B86B
Has elevated privileges:	true
Has administrator privileges:	false
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

File Written

Analysis Process: conhost.exe PID: 4636 Parent PID: 2252

General

Start time:	04:15:32
Start date:	29/09/2021
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:	false
Programmed in:	C, C++ or other language

Disassembly

Code Analysis