ID: 682147
Sample Name:
SecuriteInfo.com.W32.AIDetectNet.01.16858.8637
Cookbook: default.jbs
Time: 06:30:12
Date: 11/08/2022
Version: 35.0.0 Citrine

Table of Contents

Copyright Joe Security LLC 2022

Copyright Joe Security LLC 2022

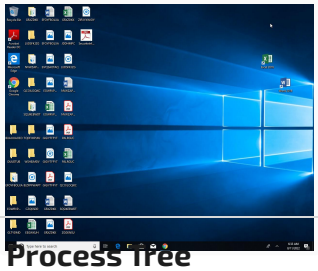
Windows Analysis Report

SecuriteInfo.com.W32.AIDetectNet.01.16858.8637

Overview

General Information

Sample Name:	SecuriteInfo.com.W32.AIDetectNet.01.16858.8637 (renamed file extension from 8637 to exe)
Analysis ID:	682147
MD5:	dfe8f6d0b1fb5fb…
SHA1:	0e94379e76c28d..
SHA256:	342c1de5e06e65..
Tags:	exe
Infos:	



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

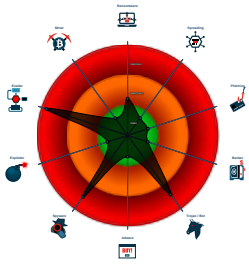
AgentTesla

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

Signatures

- Multi AV Scanner detection for subm…
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Multi AV Scanner detection for drop…
- Installs a global keyboard hook
- Tries to steal Mail credentials (via fi…
- Tries to harvest and steal Putty / W…
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.W32.AIDetectNet.01.16858.exe (PID: 5884 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetectNet.01.16858.exe" MD5: DFE8F6D0B1FB5FB795F5596564ED5A60)
  - SecuriteInfo.com.W32.AIDetectNet.01.16858.exe (PID: 5800 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetectNet.01.16858.exe MD5: DFE8F6D0B1FB5FB795F5596564ED5A60)
- bgnFA.exe (PID: 2508 cmdline: "C:\Users\user\AppData\Roaming\bgnFA\bgnFA.exe" MD5: DFE8F6D0B1FB5FB795F5596564ED5A60)
  - bgnFA.exe (PID: 5936 cmdline: C:\Users\user\AppData\Roaming\bgnFA\bgnFA.exe MD5: DFE8F6D0B1FB5FB795F5596564ED5A60)
- bgnFA.exe (PID: 5312 cmdline: "C:\Users\user\AppData\Roaming\bgnFA\bgnFA.exe" MD5: DFE8F6D0B1FB5FB795F5596564ED5A60)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "mostafa@gpd-qatar.com",
  "Password": "Toy?C@R2v$4bKt",
  "Host": "mail.gpd-qatar.com"
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.449409906.0000000002CDC000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000000.00000002.451298378.0000000003D65000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Copyright Joe Security LLC 2022

Source	Rule	Description	Author	Strings
00000000.00000002.451298378.0000000003D65000.00000004.00000800.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.451298378.0000000003D65000.00000004.00000800.00020000.00000000.sdmp	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x678c1:$a13: get_DnsResolver • 0x9b6e1:$a13: get_DnsResolver • 0xcf301:$a13: get_DnsResolver • 0x6611e:$a20: get_LastAccessed • 0x99f3e:$a20: get_LastAccessed • 0xcdb5e:$a20: get_LastAccessed • 0x68251:$a27: set_InternalServerPort • 0x9c071:$a27: set_InternalServerPort • 0xcfc91:$a27: set_InternalServerPort • 0x6856e:$a30: set_GuidMasterKey • 0x9c38e:$a30: set_GuidMasterKey • 0xcffae:$a30: set_GuidMasterKey • 0x66225:$a33: get_Clipboard • 0x9a045:$a33: get_Clipboard • 0xcdc65:$a33: get_Clipboard • 0x66233:$a34: get_Keyboard • 0x9a053:$a34: get_Keyboard • 0xcdc73:$a34: get_Keyboard • 0x674de:$a35: get_ShiftKeyDown • 0x9b2fe:$a35: get_ShiftKeyDown • 0xcef1e:$a35: get_ShiftKeyDown
00000006.00000000.445181594.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 18 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.SecuriteInfo.com.W32.AIDetectNet.01.16858.exe.3d9ce08.8.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.SecuriteInfo.com.W32.AIDetectNet.01.16858.exe.3d9ce08.8.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.SecuriteInfo.com.W32.AIDetectNet.01.16858.exe.3d9ce08.8.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x3059a:$s10: logins • 0x2fff6:$s11: credential • 0x2c61d:$g1: get_Clipboard • 0x2c62b:$g2: get_Keyboard • 0x2c638:$g3: get_Password • 0x2d8c6:$g4: get_CtrlKeyDown • 0x2d8d6:$g5: get_ShiftKeyDown • 0x2d8e7:$g6: get_AltKeyDown
0.2.SecuriteInfo.com.W32.AIDetectNet.01.16858.exe.3d9ce08.8.unpack	Windows_Trojan_AgentTesla_d3ac2b2f	unknown	unknown	• 0x2dcb9:$a13: get_DnsResolver • 0x2c516:$a20: get_LastAccessed • 0x2e649:$a27: set_InternalServerPort • 0x2e966:$a30: set_GuidMasterKey • 0x2c61d:$a33: get_Clipboard • 0x2c62b:$a34: get_Keyboard • 0x2d8d6:$a35: get_ShiftKeyDown • 0x2d8e7:$a36: get_AltKeyDown • 0x2c638:$a37: get_Password • 0x2d0ac:$a38: get_PasswordHash • 0x2e0c1:$a39: get_DefaultCredentials
6.0.SecuriteInfo.com.W32.AIDetectNet.01.16858.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 22 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Copyright Joe Security LLC 2022

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Key, Mouse, Clipboard, Microphone and Screen Capturing

Installs a global keyboard hook

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Data Obfuscation

.NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection

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

Malware Analysis System Evasion

Yara detected AntiVM3

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

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion

Injects a PE file into a foreign processes

Stealing of Sensitive Information

Yara detected AgentTesla

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

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

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

Remote Access Functionality

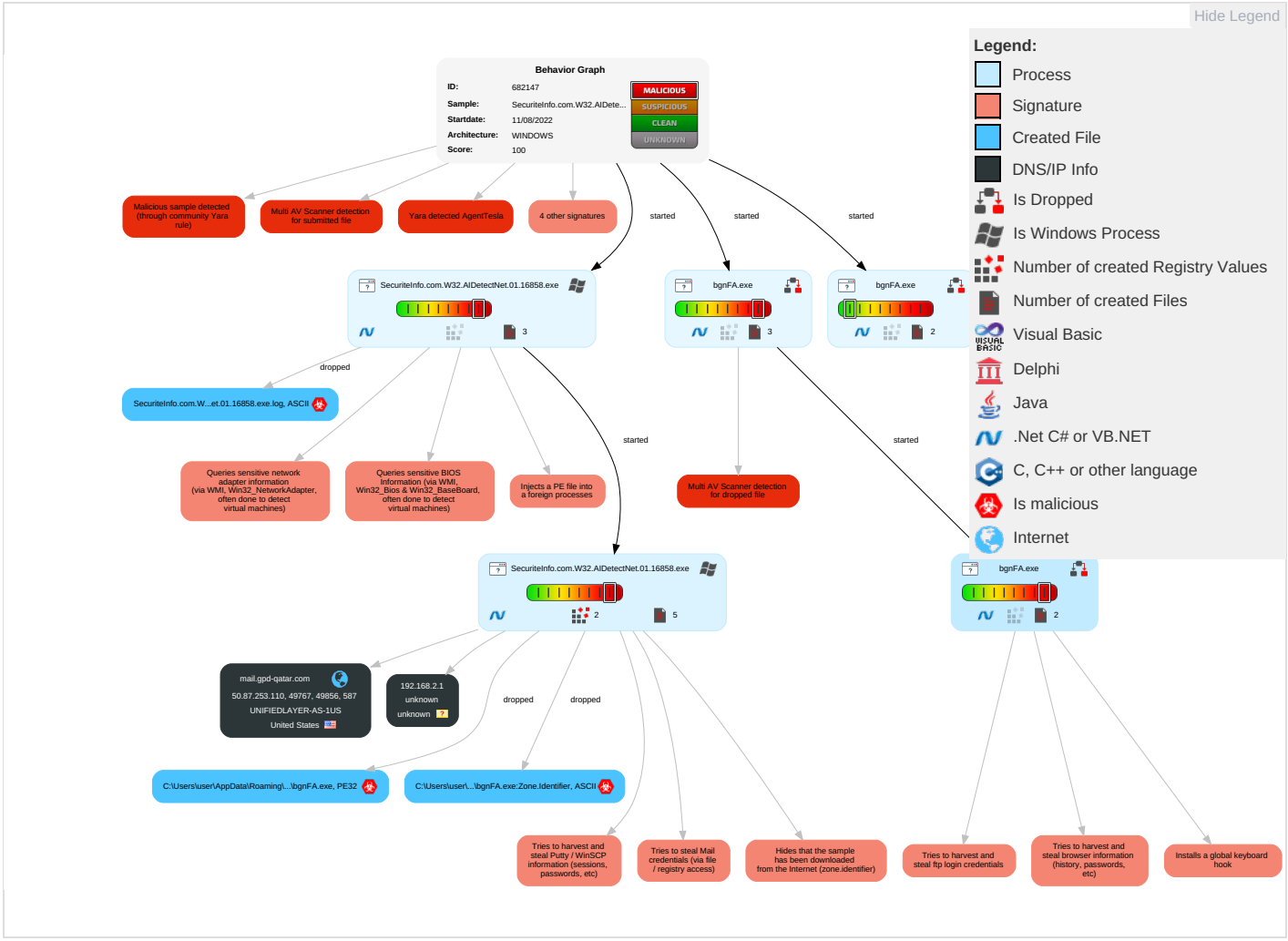
Yara detected AgentTesla

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

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	2 1 1 Windows Management Instrumentation	1 Registry Run Keys / Startup Folder	1 1 1 Process Injection	1 Disable or Modify Tools	2 OS Credential Dumping	1 1 4 System Information Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Registry Run Keys / Startup Folder	1 Deobfuscate/Decode Files or Information	1 1 1 Input Capture	1 Query Registry	Remote Desktop Protocol	2 Data from Local System	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)	Logon Script (Windows)	2 Obfuscated Files or Information	1 Credentials in Registry	3 1 1 Security Software Discovery	SMB/Windows Admin Shares	1 Email Collection	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 2 Software Packing	NTDS	1 Process Discovery	Distributed Component Object Model	1 1 1 Input Capture	Scheduled Transfer	1 1 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Masquerading	LSA Secrets	1 3 1 Virtualization/Sandbox Evasion	SSH	1 Clipboard Data	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 3 1 Virtualization/Sandbox Evasion	Cached Domain Credentials	1 Application Window 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 1 1 Process Injection	DCSync	1 Remote System Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 Hidden Files and Directories	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

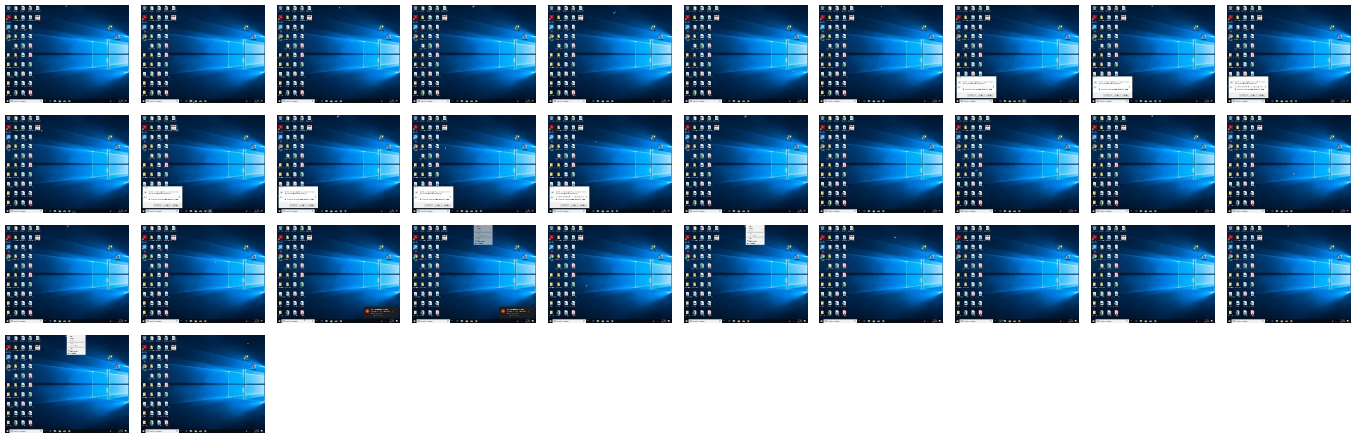
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
SecuriteInfo.com.W32.AIDetectNet.01.16858.exe	17%	Virustotal		Browse

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\bgnFA\bgnFA.exe	17%	Virustotal		Browse

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.0.SecuriteInfo.com.W32.AIDetectNet.01.16858.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://api.ipify.org%GETOK	0%	URL Reputation	safe	

Copyright Joe Security LLC 2022

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3.crl0	0%	URL Reputation	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://ocsp.suscerte.gob.ve0	0%	URL Reputation	safe	
http://www.postsignum.cz/crl/psrootqca2.crl02	0%	URL Reputation	safe	
http://crl.dhimyotis.com/certignarootca.crl0	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.pkioverheid.nl/policies/root-policy0	0%	URL Reputation	safe	
http://www.suscerte.gob.ve/lcr0#	0%	URL Reputation	safe	
http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-c/cacrl.crl0	0%	URL Reputation	safe	
http://postsignum.ttc.cz/crl/psrootqca2.crl0	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://crl1.comsign.co.il/crl/comsignglobalrootca.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3P.crl0	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.suscerte.gob.ve/dpc0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.defence.gov.au/pki0	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.fontbureau.comgrito	0%	URL Reputation	safe	
http://www.sk.ee/cps/0	0%	URL Reputation	safe	
http://www.globaltrust.info0=	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://cps.root-x1.letsencrypt.org0	0%	URL Reputation	safe	
http://policy.camerfirma.com0	0%	URL Reputation	safe	
http://www.ssc.lt/cps03	0%	URL Reputation	safe	
http://ocsp.pki.gva.es0	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0?	0%	URL Reputation	safe	
http://ca.mtin.es/mtin/ocsp0	0%	URL Reputation	safe	
http://cps.letsencrypt.org0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-b/cacrl.crl0	0%	URL Reputation	safe	
http://web.ncdc.gov.sa/crl/nrcacomb1.crl0	0%	URL Reputation	safe	
http://www.uce.gub.uy/informacion-tecnica/politicas/cp_acrn.pdf0G	0%	URL Reputation	safe	
http://https://wwww.certigna.fr/autorites/0m	0%	URL Reputation	safe	
http://philiphanson.org/medius/temp-transform	0%	Avira URL Cloud	safe	
http://www.dnie.es/dpc0	0%	URL Reputation	safe	
http://www.ica.co.il/repository/cps/PersonalID_Practice_Statement.pdf0	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	0%	URL Reputation	safe	
http://ca.mtin.es/mtin/DPCyPoliticas0	0%	URL Reputation	safe	
http://www.carterandcone.como	0%	URL Reputation	safe	
http://www.globaltrust.info0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3TS.crl0	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://ac.economia.gob.mx/last.crl0G	0%	URL Reputation	safe	
http://LyFPshcnr7V.net	0%	Avira URL Cloud	safe	
http://https://www.catcert.net/verarrel	0%	URL Reputation	safe	
http://www.disig.sk/ca0f	0%	URL Reputation	safe	
http://www.founder.com.cn/cn-	0%	URL Reputation	safe	
http://www.sk.ee/juur/crl/0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersignroot.crl0	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://crl.xrampsecurity.com/XGCA.crl0	0%	URL Reputation	safe	
http://certs.oati.net/repository/OATICA2.crl0	0%	URL Reputation	safe	
http://crl.oces.trust2408.com/oces.crl0	0%	URL Reputation	safe	
http://www.quovadis.bm0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-a/cacrl.crl0	0%	URL Reputation	safe	
http://certs.oaticerts.com/repository/OATICA2.crl	0%	URL Reputation	safe	
http://www.trustdst.com/certificates/policy/ACES-index.html0	0%	URL Reputation	safe	
http://certs.oati.net/repository/OATICA2.crt0	0%	URL Reputation	safe	
http://www.accv.es00	0%	URL Reputation	safe	
http://www.pkioverheid.nl/policies/root-policy-G20	0%	URL Reputation	safe	
http://https://www.netlock.net/docs	0%	URL Reputation	safe	
http://www.e-trust.be/CPS/QNcerts	0%	URL Reputation	safe	
http://ocsp.ncdc.gov.sa0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignCA.crl0	0%	URL Reputation	safe	
http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_ROOT_CA.crl0	0%	URL Reputation	safe	
http://web.ncdc.gov.sa/crl/nrcaparta1.crl	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.gpd-qatar.com	50.87.253.110	true	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.ipify.org%GETOK	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000002.688305990.00000000029C1000.00000004.00000800.00020000.00000000.sdmp, bgnFA.exe, 0000000E.00000002.687783160.0000000002DA1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://127.0.0.1:HTTP/1.1	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000002.688305990.00000000029C1000.00000004.00000800.00020000.00000000.sdmp, bgnFA.exe, 0000000E.00000002.687783160.0000000002DA1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.627807287.0000000005F7500.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.497721282.0000000005EFA000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.499223145.0000000005F75000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.certplus.com/CRL/class3.crl0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.497226278.0000000005F7B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.e-me.lv/repository0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.495605505.00000000067C5000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.acabogacia.org/doc0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.497226278.0000000005F7B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496752658.0000000005F9E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.chambersign.org/chambersroot.crl0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496596703.0000000005FB400.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ocsp.suscerte.gob.ve0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.497226278.0000000005F7B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.postsignum.cz/crl/psrootqca2.crl02	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496912081.0000000005F8E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.dhimyotis.com/certignarootca.crl0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.495605505.00000000067C5000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://sertifikati.ca.posta.rs/crl/PostaCARoot.crl0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.497226278.0000000005F7B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.chambersign.org1	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.495605505.00000000067C5000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496596703.0000000005FB4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.pkioverheid.nl/policies/root-policy0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496752658.0000000005F9E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://repository.swisssign.com/0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.497437781.0000000005F9600.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000002.706213888.0000000005F96000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.497226278.0000000005F7B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.497043630.0000000005F97000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496912081.0000000005F8E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.499099053.0000000005F96000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496596703.0000000005FB4000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com/designers	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000000.00000002.454376754.0000000006DE200.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.suscerte.gob.ve/lcr0#	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.497226278.0000000005F7B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ca2.mtin.es/mtin/crl/MTINAutoridadRaiz0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496596703.0000000005FB4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.ssc.lt/root-c/cacrl.crl0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000002.708046683.00000000067CF000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.495605505.00000000067C5000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.627443158.00000000067CF000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://postsignum.ttc.cz/crl/psrootqca2.crl0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496912081.0000000005F8E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496752658.0000000005F9E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ca.disig.sk/ca/crl/ca_disig.crl0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.495605505.00000000067C5000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl1.comsign.co.il/crl/comsignglobalrootca.crl0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.497226278.0000000005F7B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.certplus.com/CRL/class3P.crl0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.495605505.00000000067C5000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000000.00000003.411626950.0000000005BEB000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000000.00000002.454376754.0000000006DE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000000.00000002.454376754.0000000006DE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.suscerte.gob.ve/dpc0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.497226278.0000000005F7B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.certeurope.fr/reference/root2.crl0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.497721282.0000000005EFA000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.499223145.0000000005F75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.certplus.com/CRL/class2.crl0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496596703.0000000005FB400.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.disig.sk/ca/crl/ca_disig.crl0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.495605505.00000000067C500.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://eca.hinet.net/repository/Certs/IssuedToThisCA.p7b05	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496752658.0000000005F9E000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.defence.gov.au/pki0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496752658.0000000005F9E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000000.00000002.454376754.0000000006DE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comgrito	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000000.00000002.448367203.00000000012D7000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sk.ee/cps/0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496102748.0000000005FC800.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.globaltrust.info0=	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.495605505.00000000067C500.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.anf.es	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496596703.0000000005FB400.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.pki.admin.ch/cps/CPS_2_16_756_1_17_3_1_0.pdf09	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496912081.0000000005F8E000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.urwpp.deDPlease	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000000.00000002.454376754.0000000006DE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000000.00000002.454376754.0000000006DE2000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://pki.registradores.org/normativa/index.htm0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.495605505.00000000067C500.00000004.00000800.00020000.00000000.sdmp	false		high
http://cps.root-x1.letsencrypt.org0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000002.698029049.0000000002D2200.00000004.00000800.00020000.00000000.sdmp, bgnFA.exe, 0000000E.00000002.697854473.00000000030FF000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://policy.camerfirma.com0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496752658.0000000005F9E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496596703.0000000005FB4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

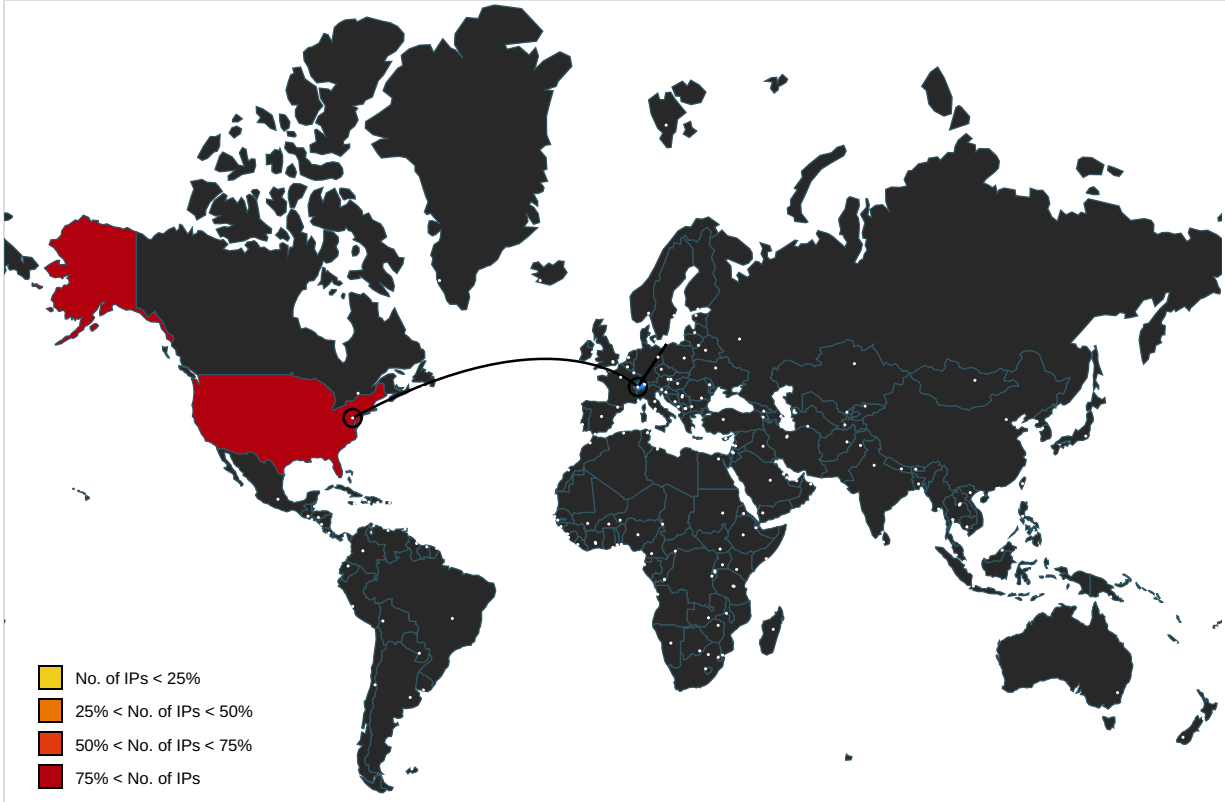
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.ssc.lt/cps03	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000002.708046683.00000000067CF000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.495605505.00000000067C5000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496596703.0000000005FB4000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496102748.0000000005FC8000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.627443158.00000000067CF000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ocsp.pki.gva.es0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496912081.0000000005F8E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.anf.es/es/address-direccion.html	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496596703.0000000005FB400.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.anf.es/address/)1(0&	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.497065018.0000000000AE300.00000004.00000020.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.497616371.0000000000AEE000.00000004.00000020.00020000.00000000.sdmp	false		high
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0?	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496912081.0000000005F8E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496596703.0000000005FB4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ca.mtin.es/mtin/ocsp0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496596703.0000000005FB400.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://cps.letsencrypt.org0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000002.698029049.0000000002D2200.00000004.00000800.00020000.00000000.sdmp, bgnFA.exe, 0000000E.00000002.697854473.00000000030FF000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.ssc.lt/root-b/cacrl.crl0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496102748.0000000005FC800.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://web.ncdc.gov.sa/crl/nrcacomb1.crl0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496752658.0000000005F9E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.certicamara.com/dpc/0Z	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.497065018.0000000000AE300.00000004.00000020.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.497616371.0000000000AEE000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.uce.gub.uy/informacion-tecnica/politicas/cp_acrn.pdf0G	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496752658.0000000005F9E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.pki.wellsfargo.com/wsprca.crl0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.497226278.0000000005F7B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://wwww.certigna.fr/autorites/0m	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.495605505.00000000067C500.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://philiphanson.org/medius/temp-transform	bgnFA.exe.6.dr	false	• Avira URL Cloud: safe	unknown
http://www.dnie.es/dpc0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.497065018.0000000000AE300.00000004.00000020.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.497616371.0000000000AEE000.00000004.00000020.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.627511724.000000000AF6000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.ica.co.il/repository/cps/PersonalID_Practice_Statement.pdf0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496102748.0000000005FC800.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.ziphttps://www	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000002.688305990.00000000029C1000.00000004.00000800.00020000.00000000.sdmp, bgnFA.exe, 0000000E.00000002.687783160.00000002DA1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ca.mtin.es/mtin/DPCyPoliticas0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496596703.0000000005FB4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.anf.es/AC/ANFServerCA.crl0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.497065018.0000000000AE3000.00000004.00000020.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.497616371.0000000000AEE000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.carterandcone.como	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000000.00000003.415362435.0000000005BDE000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.globaltrust.info0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.495605505.00000000067C5000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://certificates.starfieldtech.com/repository/1604	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496596703.0000000005FB4000.00000004.00000800.00020000.00000000.sdmp	false		high
http://acedicom.edicomgroup.com/doc0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.497226278.0000000005F7B000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.certplus.com/CRL/class3TS.crl0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.497721282.0000000005EFA000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.499067814.0000000005F79000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://crl.anf.es/AC/ANFServerCA.crl0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.497065018.0000000000AE3000.00000004.00000020.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.497616371.0000000000AEE000.00000004.00000020.00020000.00000000.sdmp	false		high
http://www.carterandcone.coml	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000000.00000002.454376754.0000000006DE200.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.certeurope.fr/reference/pc-root2.pdf0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.497721282.0000000005EFA000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.499223145.0000000005F75000.00000004.00000800.00020000.00000000.sdmp	false		high
http://ac.economia.gob.mx/last.crl0G	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.495605505.00000000067C5000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://LyFPshcnr7V.net	bgnFA.exe, 0000000E.00000002.687783160.000000002DA1000.00000004.00000800.00020000.00000000.sdmp, bgnFA.exe, 0000000E.00000002.698098173.0000000003121000.00000004.00000800.00020000.00000000.sdmp, bgnFA.exe, 0000000E.00000002.698171434.000000000312A000.00000004.00000800.00020000.00000000.sdmp, bgnFA.exe, 0000000E.00000002.697762371.00000000030F7000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000000.00000002.454376754.0000000006DE200.00000004.00000800.00020000.00000000.sdmp	false		high
http://https://www.catcert.net/verarrel	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.495605505.00000000067C5000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.disig.sk/ca0f	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.495605505.00000000067C5000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn-	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000000.00000003.413853855.0000000005BD8000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.accv.es/fileadmin/Archivos/certificados/raizaccv1.crt0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496912081.0000000005F8E000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.e-szigno.hu/RootCA.crl	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.495605505.00000000067C5000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sk.ee/juur/crl/0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496102748.0000000005FC8000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.chambersign.org/chambersignroot.crl0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.495605505.00000000067C5000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.xrampsecurity.com/XGCA.crl0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.497065018.0000000000AE3000.00000004.00000020.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.497616371.0000000000AEE000.00000004.00000020.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://certs.oati.net/repository/OATICA2.crl0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496596703.0000000005FB4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://crl.oces.trust2408.com/oces.crl0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496596703.0000000005FB4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.quovadis.bm0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.497226278.0000000005F7B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://eca.hinet.net/repository0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496752658.0000000005F9E000.00000004.00000800.00020000.00000000.sdmp	false		high
http://crl.ssc.lt/root-a/cacrl.crl0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496596703.0000000005FB4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://certs.oaticerts.com/repository/OATICA2.crl	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496596703.0000000005FB4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.trustdst.com/certificates/policy/ACES-index.html0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496102748.0000000005FC8000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://certs.oati.net/repository/OATICA2.crt0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496596703.0000000005FB4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.accv.es00	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496912081.0000000005F8E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.pkioverheid.nl/policies/root-policy-G20	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496596703.0000000005FB4000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://www.netlock.net/docs	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.497226278.0000000005F7B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_21_1.pdf0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496596703.0000000005FB4000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.e-trust.be/CPS/QNcerts	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.497585491.0000000005FB3000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496752658.0000000005F9E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496912081.0000000005F8E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.495605505.00000000067C5000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000002.706267699.0000000005FAC000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://ocsp.ncdc.gov.sa0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496752658.0000000005F9E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designersG	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000000.00000002.454376754.0000000006DE200.00000004.00000800.00020000.00000000.sdmp	false		high
http://fedir.comsign.co.il/crl/ComSignCA.crl0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.497226278.0000000005F7B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers/?	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000000.00000002.454376754.0000000006DE2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_ROOT_CA.crl0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.497437781.0000000005F96000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000002.706213888.0000000005F96000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496912081.0000000005F8E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.499099053.0000000005F96000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://web.ncdc.gov.sa/crl/nrcaparta1.crl	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496752658.0000000005F9E000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.datev.de/zertifikat-policy-int0	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.497454262.0000000005F9B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496912081.0000000005F8E000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.W32.AIDetectNet.01.16858.exe, 00000006.00000003.496596703.0000000005FB4000.00000004.00000800.00020000.00000000.sdmp	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
50.87.253.110	mail.gpd-qatar.com	United States		46606	UNIFIEDLAYER-AS-1US	false

Private

IP
192.168.2.1

Copyright Joe Security LLC 2022

General Information

Joe Sandbox Version:	35.0.0 Citrine
Analysis ID:	682147
Start date and time:	2022-08-11 06:30:12 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 37s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.W32.AIDetectNet.01.16858.8637 (renamed file extension from 8637 to 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:	mal100.troj.spyw.evad.winEXE@7/4@2/2
EGA Information:	• Successful, ratio: 100%
HDC Information:	Failed
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 23.211.6.115, 209.197.3.8
- Excluded domains from analysis (whitelisted): www.bing.com, client.wns.windows.com, fs.microsoft.com, store-images.s-microsoft.com-c.edgekey.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, arc.msn.com, wu-bg-shim.trafficmanager.net, ris.api.iris.microsoft.com, e12564.dspb.akamaiedge.net, licensing.mp.microsoft.com, login.live.com, store-images.s-microsoft.com, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing disassembly code information.
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
06:31:25	API Interceptor	623x Sleep call for process: SecuriteInfo.com.W32.AIDetectNet.01.16858.exe modified
06:31:39	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run bgnFA C:\Users\user\AppData\Roaming\bgnFA\bgnFA.exe
06:31:47	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run bgnFA C:\Users\user\AppData\Roaming\bgnFA\bgnFA.exe
06:32:03	API Interceptor	341x Sleep call for process: bgnFA.exe modified

Copyright Joe Security LLC 2022

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.W32.AIDetectNet.01.16858.exe.log

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetectNet.01.16858.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427
SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\bgnFA.exe.log

Process:	C:\Users\user\AppData\Roaming\bgnFA\bgnFA.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427

SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Roaming\bgnFA\bgnFA.exe

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetectNet.01.16858.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1131008
Entropy (8bit):	7.058493037232615
Encrypted:	false
SSDEEP:	24576:AAi4vwHmQl/HrwmpStXqDrbWtOJqyp9hgi:ANHrw7aCOJJ
MD5:	DFE8F6D0B1FB5FB795F5596564ED5A60
SHA1:	0E94379E76C28D605FD35C65369626A823924000
SHA-256:	342C1DE5E06E65EF00A4D5C0C39E4157D5B54268F3324D6DB17F76498B02A7C1
SHA-512:	4C188F028F2FE1D73E009B754C670CE6267FAB4CDBA288E75E544D8FA153F6A1AB1BC363BE69F5D7E713D672CC737CD2D69B67793E89C248352B4EBB7BB9CE8D
Malicious:	**true**
Antivirus:	• Antivirus: Virustotal, Detection: 17%, Browse
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....b.b.....0.....:.....V$.. ...@....@.. ....@.....$..O....@...7..... ....H.....text...\.... ....`.rsrc....7...@...8..... ..@..@.reloc.....@.....@..B.....8$.....H.....L.....j....l.. .....0.....{....o.....+..*f..{.....,.+.~ ...o!....*&...}....*....0..j.....s"..... {....o#...o$....+(.o%...t.....o&.....,...o'...u....o(.....o)...-....u.....,...o*.....+...*.....4M.....s"...}.....}.....(+.....(.....*..0..s.....{.....s,...o-.....{....o.....+0..(/.....o....s0.....o1..... {....o#....o2...&...(3...-.....o*.....*.....&.=c.....0..+.....,..{.....

C:\Users\user\AppData\Roaming\bgnFA\bgnFA.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetectNet.01.16858.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64E
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.058493037232615
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	SecuriteInfo.com.W32.AIDetectNet.01.16858.exe

File size:	1131008
MD5:	dfe8f6d0b1fb5fb795f5596564ed5a60
SHA1:	0e94379e76c28d605fd35c65369626a823924000
SHA256:	342c1de5e06e65ef00a4d5c0c39e4157d5b54268f3324d6db17f76498b02a7c1
SHA512:	4c188f028f2fe1d73e009b754c670ce6267fab4cdba288e75e544d8fa153f6a1ab1bc363be69f5d7e713d672cc737cd2d69b67793e89c248352b4ebb7bb9ce8d
SSDEEP:	24576:AAi4vwHmQl/HrwmpStXqDrbWtOJqyp9hgi:ANHrw7aCOJJ
TLSH:	D2359DDEEA48C85ADD154B30E83948F05767BDA5F435D85F285BBC21BA7338E212AD03
File Content Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L....b.b..............0......:.......V$... ...@....@.. ....@.................................

File Icon

Icon Hash:	0f3135466416514c

Static PE Info

General

Entrypoint:	0x4e2456
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, 32BIT_MACHINE
DLL Characteristics:	DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x62F46281 [Thu Aug 11 01:59:29 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Instruction
jmp dword ptr [00402000h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

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

Copyright Joe Security LLC 2022

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xe2404	0x4f	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xe4000	0x337a4	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x118000	0xc	.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	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0xe045c	0xe0600	False	0.6771903290389972	data	7.433620851852969	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.rsrc	0xe4000	0x337a4	0x33800	False	0.1639961316747573	data	4.093478798314193	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x118000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xe4160	0x33090	data		
RT_GROUP_ICON	0x1171f0	0x14	data		
RT_GROUP_ICON	0x117204	0x14	data		
RT_VERSION	0x117218	0x3a0	data		
RT_MANIFEST	0x1175b8	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

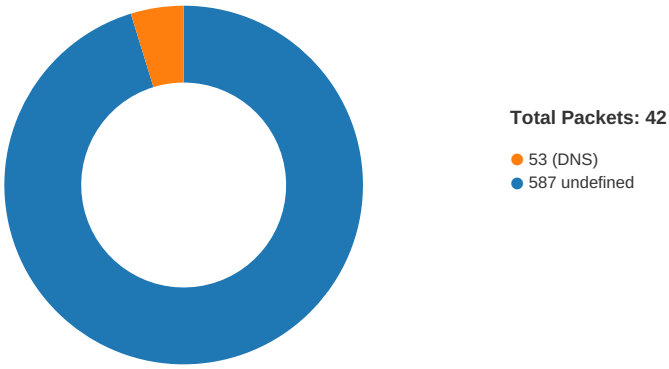
Copyright Joe Security LLC 2022

Imports

DLL	Import
mscoree.dll	_CorExeMain

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 06:31:52.393898010 CEST	49767	587	192.168.2.5	50.87.253.110
Aug 11, 2022 06:31:52.564441919 CEST	587	49767	50.87.253.110	192.168.2.5
Aug 11, 2022 06:31:52.565962076 CEST	49767	587	192.168.2.5	50.87.253.110
Aug 11, 2022 06:31:52.872816086 CEST	587	49767	50.87.253.110	192.168.2.5
Aug 11, 2022 06:31:52.873655081 CEST	49767	587	192.168.2.5	50.87.253.110
Aug 11, 2022 06:31:53.044276953 CEST	587	49767	50.87.253.110	192.168.2.5
Aug 11, 2022 06:31:53.044578075 CEST	49767	587	192.168.2.5	50.87.253.110
Aug 11, 2022 06:31:53.216497898 CEST	587	49767	50.87.253.110	192.168.2.5
Aug 11, 2022 06:31:53.341092110 CEST	49767	587	192.168.2.5	50.87.253.110
Aug 11, 2022 06:31:53.518033028 CEST	587	49767	50.87.253.110	192.168.2.5
Aug 11, 2022 06:31:53.518070936 CEST	587	49767	50.87.253.110	192.168.2.5
Aug 11, 2022 06:31:53.518093109 CEST	587	49767	50.87.253.110	192.168.2.5
Aug 11, 2022 06:31:53.518110037 CEST	587	49767	50.87.253.110	192.168.2.5
Aug 11, 2022 06:31:53.518186092 CEST	49767	587	192.168.2.5	50.87.253.110
Aug 11, 2022 06:31:53.518229961 CEST	49767	587	192.168.2.5	50.87.253.110
Aug 11, 2022 06:31:53.520034075 CEST	587	49767	50.87.253.110	192.168.2.5
Aug 11, 2022 06:31:53.581407070 CEST	49767	587	192.168.2.5	50.87.253.110
Aug 11, 2022 06:31:53.752665043 CEST	587	49767	50.87.253.110	192.168.2.5
Aug 11, 2022 06:31:53.959604025 CEST	49767	587	192.168.2.5	50.87.253.110
Aug 11, 2022 06:31:57.128820896 CEST	49767	587	192.168.2.5	50.87.253.110
Aug 11, 2022 06:31:57.299420118 CEST	587	49767	50.87.253.110	192.168.2.5
Aug 11, 2022 06:31:57.304728031 CEST	49767	587	192.168.2.5	50.87.253.110
Aug 11, 2022 06:31:57.475887060 CEST	587	49767	50.87.253.110	192.168.2.5
Aug 11, 2022 06:31:57.476553917 CEST	49767	587	192.168.2.5	50.87.253.110
Aug 11, 2022 06:31:57.687643051 CEST	587	49767	50.87.253.110	192.168.2.5
Aug 11, 2022 06:31:57.783134937 CEST	587	49767	50.87.253.110	192.168.2.5
Aug 11, 2022 06:31:57.785454988 CEST	49767	587	192.168.2.5	50.87.253.110
Aug 11, 2022 06:31:57.955754042 CEST	587	49767	50.87.253.110	192.168.2.5
Aug 11, 2022 06:31:57.959969044 CEST	587	49767	50.87.253.110	192.168.2.5
Aug 11, 2022 06:31:57.960346937 CEST	49767	587	192.168.2.5	50.87.253.110
Aug 11, 2022 06:31:58.132647038 CEST	587	49767	50.87.253.110	192.168.2.5

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 06:31:58.135360003 CEST	49767	587	192.168.2.5	50.87.253.110
Aug 11, 2022 06:31:58.305826902 CEST	587	49767	50.87.253.110	192.168.2.5
Aug 11, 2022 06:31:58.306900978 CEST	49767	587	192.168.2.5	50.87.253.110
Aug 11, 2022 06:31:58.307035923 CEST	49767	587	192.168.2.5	50.87.253.110
Aug 11, 2022 06:31:58.307812929 CEST	49767	587	192.168.2.5	50.87.253.110
Aug 11, 2022 06:31:58.307898998 CEST	49767	587	192.168.2.5	50.87.253.110
Aug 11, 2022 06:31:58.477329016 CEST	587	49767	50.87.253.110	192.168.2.5
Aug 11, 2022 06:31:58.477361917 CEST	587	49767	50.87.253.110	192.168.2.5
Aug 11, 2022 06:31:58.478331089 CEST	587	49767	50.87.253.110	192.168.2.5
Aug 11, 2022 06:31:58.478370905 CEST	587	49767	50.87.253.110	192.168.2.5
Aug 11, 2022 06:31:58.479069948 CEST	587	49767	50.87.253.110	192.168.2.5
Aug 11, 2022 06:31:58.647525072 CEST	49767	587	192.168.2.5	50.87.253.110
Aug 11, 2022 06:32:38.429254055 CEST	49856	587	192.168.2.5	50.87.253.110
Aug 11, 2022 06:32:38.599436998 CEST	587	49856	50.87.253.110	192.168.2.5
Aug 11, 2022 06:32:38.599688053 CEST	49856	587	192.168.2.5	50.87.253.110
Aug 11, 2022 06:32:38.903387070 CEST	587	49856	50.87.253.110	192.168.2.5
Aug 11, 2022 06:32:38.903830051 CEST	49856	587	192.168.2.5	50.87.253.110
Aug 11, 2022 06:32:39.074331999 CEST	587	49856	50.87.253.110	192.168.2.5
Aug 11, 2022 06:32:39.074683905 CEST	49856	587	192.168.2.5	50.87.253.110
Aug 11, 2022 06:32:39.246436119 CEST	587	49856	50.87.253.110	192.168.2.5
Aug 11, 2022 06:32:39.266998053 CEST	49856	587	192.168.2.5	50.87.253.110
Aug 11, 2022 06:32:39.446536064 CEST	587	49856	50.87.253.110	192.168.2.5
Aug 11, 2022 06:32:39.446569920 CEST	587	49856	50.87.253.110	192.168.2.5
Aug 11, 2022 06:32:39.446587086 CEST	587	49856	50.87.253.110	192.168.2.5
Aug 11, 2022 06:32:39.446599960 CEST	587	49856	50.87.253.110	192.168.2.5
Aug 11, 2022 06:32:39.446610928 CEST	587	49856	50.87.253.110	192.168.2.5
Aug 11, 2022 06:32:39.446913004 CEST	49856	587	192.168.2.5	50.87.253.110
Aug 11, 2022 06:32:39.455908060 CEST	49856	587	192.168.2.5	50.87.253.110
Aug 11, 2022 06:32:39.626528025 CEST	587	49856	50.87.253.110	192.168.2.5
Aug 11, 2022 06:32:39.689002991 CEST	49856	587	192.168.2.5	50.87.253.110
Aug 11, 2022 06:32:39.859565973 CEST	587	49856	50.87.253.110	192.168.2.5
Aug 11, 2022 06:32:39.860413074 CEST	49856	587	192.168.2.5	50.87.253.110
Aug 11, 2022 06:32:40.031085968 CEST	587	49856	50.87.253.110	192.168.2.5
Aug 11, 2022 06:32:40.031702995 CEST	49856	587	192.168.2.5	50.87.253.110
Aug 11, 2022 06:32:40.242882013 CEST	587	49856	50.87.253.110	192.168.2.5
Aug 11, 2022 06:32:40.338757038 CEST	587	49856	50.87.253.110	192.168.2.5
Aug 11, 2022 06:32:40.339184999 CEST	49856	587	192.168.2.5	50.87.253.110
Aug 11, 2022 06:32:40.509526968 CEST	587	49856	50.87.253.110	192.168.2.5
Aug 11, 2022 06:32:40.509551048 CEST	587	49856	50.87.253.110	192.168.2.5
Aug 11, 2022 06:32:40.509987116 CEST	49856	587	192.168.2.5	50.87.253.110
Aug 11, 2022 06:32:40.682395935 CEST	587	49856	50.87.253.110	192.168.2.5
Aug 11, 2022 06:32:40.682790995 CEST	49856	587	192.168.2.5	50.87.253.110
Aug 11, 2022 06:32:40.853790998 CEST	587	49856	50.87.253.110	192.168.2.5
Aug 11, 2022 06:32:40.854865074 CEST	49856	587	192.168.2.5	50.87.253.110
Aug 11, 2022 06:32:40.854993105 CEST	49856	587	192.168.2.5	50.87.253.110
Aug 11, 2022 06:32:40.855067015 CEST	49856	587	192.168.2.5	50.87.253.110
Aug 11, 2022 06:32:40.855168104 CEST	49856	587	192.168.2.5	50.87.253.110
Aug 11, 2022 06:32:41.026067019 CEST	587	49856	50.87.253.110	192.168.2.5
Aug 11, 2022 06:32:41.026170969 CEST	587	49856	50.87.253.110	192.168.2.5
Aug 11, 2022 06:32:41.027707100 CEST	587	49856	50.87.253.110	192.168.2.5
Aug 11, 2022 06:32:41.161303997 CEST	49856	587	192.168.2.5	50.87.253.110
Aug 11, 2022 06:33:32.128531933 CEST	49767	587	192.168.2.5	50.87.253.110
Aug 11, 2022 06:33:32.339531898 CEST	587	49767	50.87.253.110	192.168.2.5
Aug 11, 2022 06:33:32.771600962 CEST	587	49767	50.87.253.110	192.168.2.5
Aug 11, 2022 06:33:32.772248030 CEST	49767	587	192.168.2.5	50.87.253.110

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Aug 11, 2022 06:31:52.169194937 CEST	59661	53	192.168.2.5	8.8.8.8
Aug 11, 2022 06:31:52.350989103 CEST	53	59661	8.8.8.8	192.168.2.5
Aug 11, 2022 06:32:38.382360935 CEST	62525	53	192.168.2.5	8.8.8.8
Aug 11, 2022 06:32:38.401916981 CEST	53	62525	8.8.8.8	192.168.2.5

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 11, 2022 06:31:52.169194937 CEST	192.168.2.5	8.8.8.8	0x100e	Standard query (0)	mail.gpd-qatar.com	A (IP address)	IN (0x0001)
Aug 11, 2022 06:32:38.382360935 CEST	192.168.2.5	8.8.8.8	0xf46	Standard query (0)	mail.gpd-qatar.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 11, 2022 06:31:52.350989103 CEST	8.8.8.8	192.168.2.5	0x100e	No error (0)	mail.gpd-qatar.com		50.87.253.110	A (IP address)	IN (0x0001)
Aug 11, 2022 06:32:38.401916981 CEST	8.8.8.8	192.168.2.5	0xf46	No error (0)	mail.gpd-qatar.com		50.87.253.110	A (IP address)	IN (0x0001)

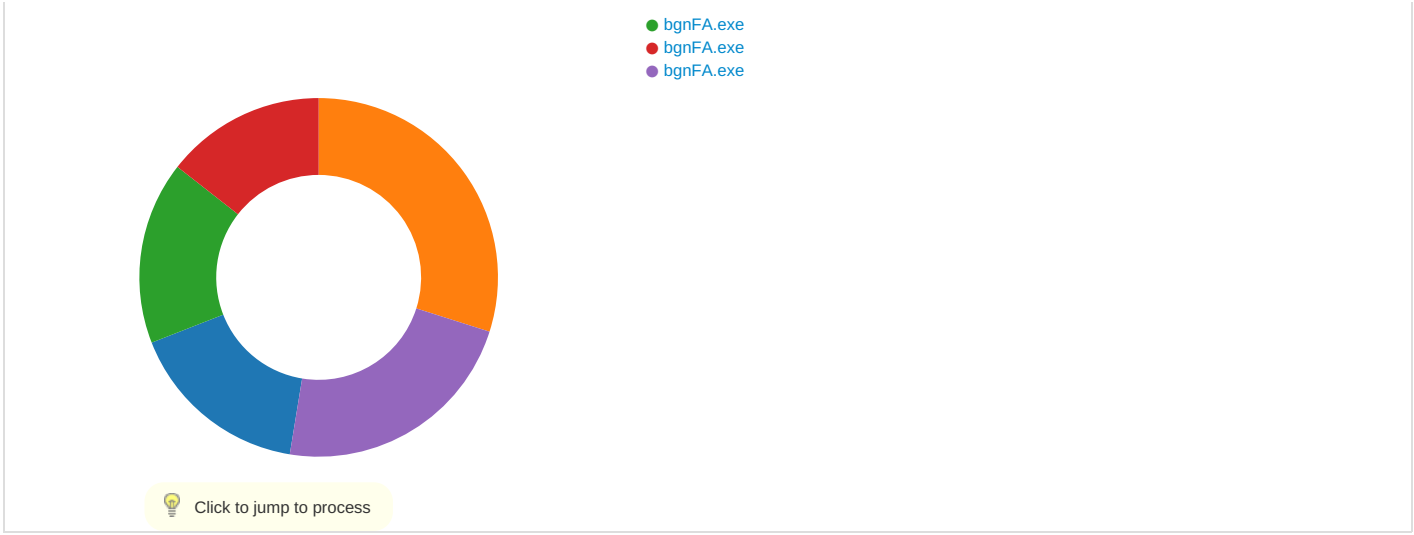
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Aug 11, 2022 06:31:52.872816086 CEST	587	49767	50.87.253.110	192.168.2.5	220-box2181.bluehost.com ESMTP Exim 4.95 #2 Wed, 10 Aug 2022 22:31:52 -0600 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Aug 11, 2022 06:31:52.873655081 CEST	49767	587	192.168.2.5	50.87.253.110	EHLO 320946
Aug 11, 2022 06:31:53.044276953 CEST	587	49767	50.87.253.110	192.168.2.5	250-box2181.bluehost.com Hello 320946 [102.129.143.3] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Aug 11, 2022 06:31:53.044578075 CEST	49767	587	192.168.2.5	50.87.253.110	STARTTLS
Aug 11, 2022 06:31:53.216497898 CEST	587	49767	50.87.253.110	192.168.2.5	220 TLS go ahead
Aug 11, 2022 06:32:38.903387070 CEST	587	49856	50.87.253.110	192.168.2.5	220-box2181.bluehost.com ESMTP Exim 4.95 #2 Wed, 10 Aug 2022 22:32:38 -0600 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Aug 11, 2022 06:32:38.903830051 CEST	49856	587	192.168.2.5	50.87.253.110	EHLO 320946
Aug 11, 2022 06:32:39.074331999 CEST	587	49856	50.87.253.110	192.168.2.5	250-box2181.bluehost.com Hello 320946 [102.129.143.3] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Aug 11, 2022 06:32:39.074683905 CEST	49856	587	192.168.2.5	50.87.253.110	STARTTLS
Aug 11, 2022 06:32:39.246436119 CEST	587	49856	50.87.253.110	192.168.2.5	220 TLS go ahead

Statistics

Behavior

Copyright Joe Security LLC 2022



System Behavior

Analysis Process: SecuriteInfo.com.W32.AIDetectNet.01.16858.exe PID: 5884, Parent PID: 5796

General

Target ID:	0
Start time:	06:31:13
Start date:	11/08/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetectNet.01.16858.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetectNet.01.16858.exe"
Imagebase:	0x810000
File size:	1131008 bytes
MD5 hash:	DFE8F6D0B1FB5FB795F5596564ED5A60
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.449409906.0000000002CDC000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.451298378.0000000003D65000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.451298378.0000000003D65000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000000.00000002.451298378.0000000003D65000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.450695772.0000000002F57000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D88CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D88CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.W32.AIDetectNet.01.16858.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DB9C78D	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.W32.AIDetectNet.01.16858.exe.log	0	1308	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6DB9C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D865705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D865705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D86CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D865705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D865705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C6D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C6D1B4F	ReadFile

Analysis Process: SecuriteInfo.com.W32.AIDetectNet.01.16858.exe PID: **5800**, Parent PID: **5884**

General

Target ID:	6
Start time:	06:31:27
Start date:	11/08/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetectNet.01.16858.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.W32.AIDetectNet.01.16858.exe
Imagebase:	0x4f0000
File size:	1131008 bytes
MD5 hash:	DFE8F6D0B1FB5FB795F5596564ED5A60
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000000.445181594.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000000.445181594.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_AgentTesla_d3ac2b2f, Description: unknown, Source: 00000006.00000000.445181594.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.688305990.00000000029C1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000006.00000002.688305990.00000000029C1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D88CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D88CF06	unknown
C:\Users\user\AppData\Roaming\bgnFA	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6C6DBEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\bgnFA\bgnFA.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6C6DDD66	CopyFileW
C:\Users\user\AppData\Roaming\bgnFA\bgnFA.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6C6DDD66	CopyFileW

File Path	Completion	Count	Source Address	Symbol

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:\Users\user\AppData\Roaming\bgnFA\bgnFA.exe	0	262144	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fd 62 fd 62 00 00 00 00 00 00 00 00 fd 00 02 01 0b 01 30 00 00 06 0e 00 00 3a 03 00 00 00 00 00 56 24 0e 00 00 20 00 00 00 40 0e 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 11 00 00 02 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELbb0:V$ @@ @	success or wait	5	6C6DDD66	CopyFileW
C:\Users\user\AppData\Roaming\bgnFA\bgnFA.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]ZoneId=0	success or wait	1	6C6DDD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D865705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D865705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D86CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D865705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D865705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C6D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C6D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C6D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C6D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C6D1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C6D1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\c3d0bcad-59c3-41fa-89dd-89b9005799af	unknown	4096	success or wait	1	6C6D1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C6D1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C6D1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C6D1B4F	ReadFile

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run	bgnFA	unicode	C:\Users\user\AppData\Roaming\bgnFA\bgnFA.exe	success or wait	1	6C6D646A	RegSetValueExW
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\StartupApproved\Run	bgnFA	binary	02 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	6C6DDE2E	RegSetValueExW

Analysis Process: bgnFA.exe PID: **2508**, Parent PID: **684**

General

Target ID:	10
Start time:	06:31:47
Start date:	11/08/2022
Path:	C:\Users\user\AppData\Roaming\bgnFA\bgnFA.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\bgnFA\bgnFA.exe"
Imagebase:	0xd60000
File size:	1131008 bytes
MD5 hash:	DFE8F6D0B1FB5FB795F5596564ED5A60
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000A.00000002.539353757.000000000327C000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000A.00000002.545607388.00000000034F7000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 17%, Virustotal, Browse
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D88CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D88CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\bgnFA.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6DB9C78D	CreateFileW

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:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\bgnFA.exe.log	0	1308	31 2c 22 66 75 73 69 6f 6e 22 2c 22 47 41 43 22 2c 30 0d 0a 31 2c 22 57 69 6e 52 54 22 2c 22 4e 6f 74 41 70 70 22 2c 31 0d 0a 32 2c 22 53 79 73 74 65 6d 2e 57 69 6e 64 6f 77 73 2e 46 6f 72 6d 73 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 30 0d 0a 33 2c 22 53 79 73 74 65 6d 2c 20 56 65 72 73 69 6f 6e 3d 34 2e 30 2e 30 2e 30 2c 20 43 75 6c 74 75 72 65 3d 6e 65 75 74 72 61 6c 2c 20 50 75 62 6c 69 63 4b 65 79 54 6f 6b 65 6e 3d 62 37 37 61 35 63 35 36 31 39 33 34 65 30 38 39 22 2c 22 43 3a 5c 57 69 6e 64 6f 77 73 5c 61 73 73 65 6d 62 6c 79 5c 4e 61 74 69 76 65 49 6d 61 67 65 73 5f 76 34 2e 30 2e 33	1,"fusion","GAC",01,"WinRT","NotApp",12,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",03,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.3	success or wait	1	6DB9C907	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D865705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D865705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D86CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D865705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D865705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C6D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C6D1B4F	ReadFile

Analysis Process: bgnFA.exe PID: **5312**, Parent PID: **684**

General

Target ID:	13
Start time:	06:31:58
Start date:	11/08/2022
Path:	C:\Users\user\AppData\Roaming\bgnFA\bgnFA.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\bgnFA\bgnFA.exe"
Imagebase:	0x9b0000
File size:	1131008 bytes
MD5 hash:	DFE8F6D0B1FB5FB795F5596564ED5A60
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Copyright Joe Security LLC 2022

Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D88CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D88CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D865705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D865705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D86CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D865705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D865705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C6D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C6D1B4F	ReadFile

Analysis Process: bgnFA.exe PID: **5936**, Parent PID: **2508**

General

Target ID:	14
Start time:	06:32:10
Start date:	11/08/2022
Path:	C:\Users\user\AppData\Roaming\bgnFA\bgnFA.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\bgnFA\bgnFA.exe
Imagebase:	0x9f0000
File size:	1131008 bytes
MD5 hash:	DFE8F6D0B1FB5FB795F5596564ED5A60
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000002.687783160.0000000002DA1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000E.00000002.687783160.0000000002DA1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D88CF06	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	6D88CF06	unknown

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D865705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6D865705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6D7C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D86CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6D7C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6D7C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6D7C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6D7C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6D865705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6D865705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C6D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C6D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6C6D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6C6D1B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6C6D1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C6D1B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\4c37bcc4-63a7-4f57-8166-3b0871421bd6	unknown	4096	success or wait	1	6C6D1B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11088	success or wait	1	6C6D1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6C6D1B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6C6D1B4F	ReadFile

Disassembly

No disassembly