ID: 635306
Sample Name:
SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.12211
Cookbook: default.jbs
Time: 18:49:55
Date: 27/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.12211 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Agenttesla 4
Yara Signatures 4
Memory Dumps 4
Unpacked PEs 5
Sigma Signatures 5
Snort Signatures 5
Joe Sandbox Signatures 6
AV Detection 6
Networking 6
Spam, unwanted Advertisements and Ransom Demands 6
System Summary 6
Data Obfuscation 6
Malware Analysis System Evasion 6
HIPS / PFW / Operating System Protection Evasion 6
Lowering of HIPS / PFW / Operating System Security Settings 6
Stealing of Sensitive Information 6
Remote Access Functionality 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 9
Initial Sample 9
Dropped Files 9
Unpacked PE Files 9
Domains 9
URLs 10
Domains and IPs 11
Contacted Domains 11
URLs from Memory and Binaries 11
World Map of Contacted IPs 17
General Information 17
Warnings 18
Simulations 18
Behavior and APIs 18
Joe Sandbox View / Context 18
IPs 18
Domains 18
ASNs 18
JA3 Fingerprints 18
Dropped Files 18
Created / dropped Files 18
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe.log 18
C:\Windows\System32\drivers\etc\hosts 19
Static File Info 19
General 19
File Icon 19
Static PE Info 19
General 19
Entrypoint Preview 20
Data Directories 21
Sections 22
Resources 22
Imports 22
Version Infos 22
Network Behavior 23
Snort IDS Alerts 23
UDP Packets 23
DNS Queries 23
DNS Answers 23
Statistics 23
Behavior 23
System Behavior 24
Analysis Process: SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exePID: 7136, Parent PID: 4912 24

General 24
File Activities 24
File Created 24
File Written 24
File Read 25
Analysis Process: SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exePID: 6444, Parent PID: 7136 25
General 25
File Activities 26
File Created 26
File Written 26
File Read 26
Disassembly 27

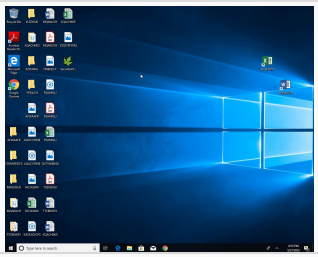
Windows Analysis Report

SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.12211

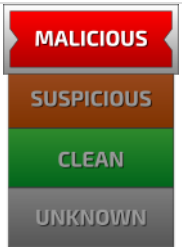
Overview

General Information

Sample Name:	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.12211 (renamed file extension from 12211 to exe)
Analysis ID:	635306
MD5:	d773da82f041dd..
SHA1:	1eb7d229a442c4..
SHA256:	f59af126d04f289..
Tags:	exe
Infos:	



Detection



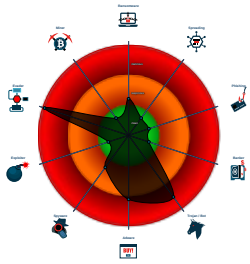
AgentTesla

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

Signatures

- Found malware configuration
- Malicious sample detected (through…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Snort IDS alert for network traffic
- .NET source code references suspic…
- Modifies the hosts file
- Tries to detect sandboxes and other…
- Machine Learning detection for sam…
- Injects a PE file into a foreign proce…
- Yara detected Generic Downloader
- .NET source code contains method …

Classification



Process Tree

- **System is w10x64**
- SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe (PID: 7136 cmdline: "C:\Users\user\Desktop\SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe" MD5: D773DA82F041DD37630E773240A97878)
  - SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe (PID: 6444 cmdline: C:\Users\user\Desktop\SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe MD5: D773DA82F041DD37630E773240A97878)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "adim@waterchem.com.tr",
  "Password": "2022payment$",
  "Host": "mail.waterchem.com.tr"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000000.484536622.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000003.00000000.484536622.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000003.00000000.482330735.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000000.482330735.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000003.00000002.692625873.0000000000402000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 19 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe.3f00930.10.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe.3f00930.10.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe.3f00930.10.raw.unpack	JoeSecurity_GenericDownloader_1	Yara detected Generic Downloader	Joe Security	
0.2.SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe.3f00930.10.raw.unpack	MALWARE_Win_AgentTeslaV3	AgentTeslaV3 infostealer payload	ditekSHen	• 0x31110:$s1: get_kbok • 0x69530:$s1: get_kbok • 0x31a44:$s2: get_CHoo • 0x69e64:$s2: get_CHoo • 0x326b7:$s3: set_passwordIsSet • 0x6aad7:$s3: set_passwordIsSet • 0x30f08:$s4: get_enableLog • 0x69328:$s4: get_enableLog • 0x35606:$s8: torbrowser • 0x6da26:$s8: torbrowser • 0x33fe2:$s10: logins • 0x6c402:$s10: logins • 0x33961:$s11: credential • 0x6bd81:$s11: credential • 0x302f1:$g1: get_Clipboard • 0x68711:$g1: get_Clipboard • 0x302ff:$g2: get_Keyboard • 0x6871f:$g2: get_Keyboard • 0x3030c:$g3: get_Password • 0x6872c:$g3: get_Password • 0x318f2:$g4: get_CtrlKeyDown
0.2.SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe.3f00930.10.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 37 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2 - Source IP: 192.168.2.5 - Destination IP: 109.232.216.96

Timestamp:	192.168.2.5109.232.216.96498515872840032 05/27/22-18:53:13.512096
SID:	2840032
Source Port:	49851
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET TROJAN AgentTesla Exfil Via SMTP - Source IP: 192.168.2.5 - Destination IP: 109.232.216.96

Timestamp:	192.168.2.5109.232.216.96498515872030171 05/27/22-18:53:13.512043
SID:	2030171
Source Port:	49851
Destination Port:	587
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Found malware configuration

Machine Learning detection for sample

Networking

Snort IDS alert for network traffic

Yara detected Generic Downloader

Spam, unwanted Advertisements and Ransom Demands

Modifies the hosts file

System Summary

Malicious sample detected (through community Yara rule)

.NET source code contains very large array initializations

Data Obfuscation

.NET source code contains method to dynamically call methods (often used by packers)

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

.NET source code references suspicious native API functions

Modifies the hosts file

Injects a PE file into a foreign processes

Lowering of HIPS / PFW / Operating System Security Settings

Modifies the hosts file

Stealing of Sensitive Information

Yara detected AgentTesla

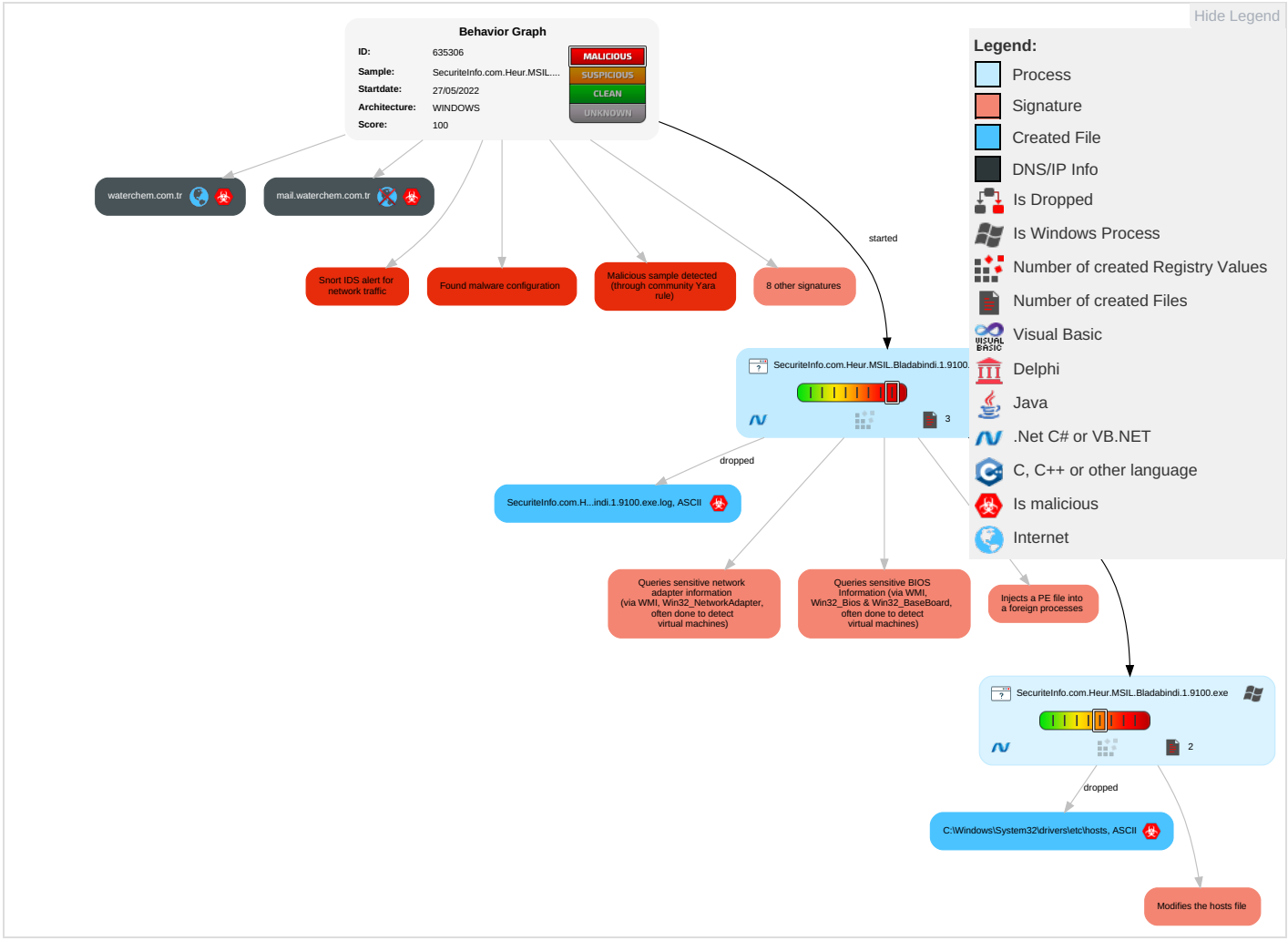
Remote Access Functionality

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
Valid Accounts	2 1 1 Windows Management Instrumentation	Path Interception	1 1 1 Process Injection	1 Masquerading	OS Credential Dumping	2 1 1 Security Software 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	1 Native API	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 File and Directory Permissions Modification	LSASS Memory	1 Process Discovery	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	1 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	1 Disable or Modify Tools	Security Account Manager	1 3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 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 3 1 Virtualization/Sandbox Evasion	NTDS	1 Application Window Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 1 Process Injection	LSA Secrets	1 Account Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Deobfuscate/Decode Files or Information	Cached Domain Credentials	1 System Owner/User 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 Obfuscated Files or Information	DCSync	1 1 3 System Information Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	1 3 Software Packing	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.Heur.MSIL.Bladabindi.1.9100.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.0.SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.2.SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
3.0.SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.jiyu-kobo.co.jp/8?	0%	Avira URL Cloud	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.comiv	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/g?V	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/p?O	0%	Avira URL Cloud	safe	
http://www.fontbureau.comepko	0%	URL Reputation	safe	
http://www.fontbureau.comgrito8?	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.comd/?	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnG	0%	URL Reputation	safe	
http://www.founder.com.cn/cnD	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/5	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/T?c	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp//?	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.founder.com.cn/cnpor	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.com.TTF	0%	URL Reputation	safe	
http://https://api.ipify.org%	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comK?j	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/g?V	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/y?D	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.fontbureau.comnc.X	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fontbureau.comsivF	0%	Avira URL Cloud	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/K?j	0%	Avira URL Cloud	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	
http://www.fontbureau.comnc.d	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/B?	0%	Avira URL Cloud	safe	
http://bzoyKu.com	0%	Avira URL Cloud	safe	
http://www.fontbureau.comcomFK?j	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
waterchem.com.tr	109.232.216.96	true	true		unknown
mail.waterchem.com.tr	unknown	unknown	true		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/8?	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.439778926.000000000594B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://127.0.0.1:HTTP/1.1	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000003.00000002.695684477.0000000002C61000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.fontbureau.com/designersG	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000002.497743975.0000000006C22000.00000004.00000800.00020000.00000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.comiv	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.437258223.000000000595B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.438215115.000000000595B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.438689789.000000000595B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.438487341.000000000595B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.434676161.000000000595B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.436055262.000000000595B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.436146385.000000000595B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.436025085.000000000595B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.436869999.000000000595B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.436385775.000000000595B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.436262765.000000000595B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.435428648.000000000595B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.435161846.000000000595B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.437166591.000000000595B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.435960511.000000000595B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.438719541.000000000595B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.435335715.000000000595B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.435615131.000000000595B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.434977200.000000000595B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.436242853.000000000595B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.436341040.000000000595B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/?	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000002.497743975.0000000006C22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.founder.com.cn/cn/bThe	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000002.497743975.0000000006C22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers?	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000002.497743975.0000000006C22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.jiyu-kobo.co.jp/jp/g?V	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.439778926.000000000594B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000002.497743975.0000000006C22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/p?O	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.439623500.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.439778926.000000000594B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000002.497743975.0000000006C22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comepko	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.455510334.000000000594A000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comgrito8?	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.455510334.000000000594A000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.goodfont.co.kr	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000002.497743975.0000000006C22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comd/?	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.446537861.0000000005948000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.446350631.0000000005947000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnG	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.437047763.0000000005947000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnD	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.437001631.0000000005948000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.437047763.0000000005947000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sajatypeworks.com	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.437258223.000000000595B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.438215115.000000000595B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.438689789.00000000595B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.438487341.000000000595B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.434676161.000000000595B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.436055262.000000000595B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.436146385.000000000595B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.436025085.000000000595B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.436869999.000000000595B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.436385775.000000000595B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.434435634.000000000595B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.436262765.000000000595B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.435428648.00000000595B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.435161846.000000000595B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.437166591.000000000595B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000002.497743975.0000000006C22000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.435960511.000000000595B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.438719541.000000000595B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.435335715.000000000595B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.435615131.000000000595B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.434977200.000000000595B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.typography.netD	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000002.497743975.0000000006C22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cn/cThe	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000002.497743975.0000000006C22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000002.497743975.0000000006C22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://fontfabrik.com	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000002.497743975.0000000006C22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/5	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.439623500.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.439778926.000000000594B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/T?c	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.439623500.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.439778926.000000000594B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp//?	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.439778926.000000000594B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp//	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.439623500.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.439778926.000000000594B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.galapagosdesign.com/DPlease	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000002.497743975.0000000006C22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.org%GETMozilla/5.0	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000003.00000002.695684477.0000000002C61000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://www.fonts.com	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000002.497743975.0000000006C22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.sandoll.co.kr	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000002.497743975.0000000006C22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.founder.com.cn/cnpor	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.437001631.000000000594800.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000002.497743975.0000000006C22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.zhongyicts.com.cn	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000002.497743975.0000000006C22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.sakkal.com	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000002.497743975.0000000006C22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com.TTF	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.446537861.000000000594800.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.446350631.0000000005947000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.ipify.org%	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000003.00000002.695684477.0000000002C61000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	low
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000002.494486784.0000000003B31000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000002.495384487.0000000003F00000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000003.00000000.484536622.0000000000402000.00000040.00000400.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000003.00000000.481183749.0000000000402000.00000040.00000400.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.apache.org/licenses/LICENSE-2.0	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000002.497743975.0000000006C22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.com	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.446350631.0000000005947000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.galapagosdesign.com/	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.448197601.000000000597000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://DynDns.comDynDNS	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000003.00000002.695684477.0000000002C61000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comF	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.446537861.000000000594800.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.446350631.0000000005947000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.comK?j	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.455510334.000000000594A000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.486701026.0000000005940000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000002.497067298.0000000005940000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000003.00000002.695684477.0000000002C61000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/g?V	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.439623500.000000000594B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/y?D	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.439623500.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.439778926.000000000594B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.439623500.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.439778926.000000000594B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://en.w	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.434968462.000000000594600.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.carterandcone.coml	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000002.497743975.0000000006C22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000002.497743975.0000000006C22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comnc.X	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.446350631.000000000594700.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.436914055.000000000594700.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.437001631.000000000594800.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.437047763.0000000005947000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000002.497743975.0000000006C22000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-jones.html	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000002.497743975.0000000006C22000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comsivF	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.446537861.000000000594800.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.446350631.000000000594700.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comm	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.455510334.000000000594A000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.486701026.0000000005940000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000002.497067298.0000000005940000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.439778926.000000000594B000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/K?j	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.439623500.000000000594B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.439778926.000000000594B000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fontbureau.com/designers8	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000002.497743975.0000000006C2 2000.00000004.00000800.00020000.00000000.sdmp	false		high
http://www.fontbureau.comals	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.446537861.000000000594 8000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.446350631.000000000594700 0.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.fontbureau.comnc.d	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.446537861.000000000594 8000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/B?	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.439623500.000000000594 B000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.439778926.000000000594B00 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://bzoyKu.com	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000003.00000002.695684477.0000000002C6 1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comcomFK?j	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.446537861.000000000594 8000.00000004.00000800.00020000.00000000.sdmp, SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe, 00000000.00000003.446350631.000000000594700 0.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	635306
Start date and time: 27/05/202218:49:55	2022-05-27 18:49:55 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 51s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.12211 (renamed file extension from 12211 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:	16
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.adwa.evad.winEXE@3/2@2/0
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 1% (good quality ratio 0.7%) • Quality average: 53.6% • Quality standard deviation: 38.4%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 52.168.117.173
- Excluded domains from analysis (whitelisted): onedsblobprdeus16.eastus.cloudapp.azure.com, client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com, arc.msn.com, ris.api.iris.microsoft.com, store-images.s-microsoft.com, login.live.com, blobcollector.events.data.trafficmanager.net, sls.update.microsoft.com, displaycatalog.mp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, watson.telemetry.microsoft.com
- Report size getting too big, too many NtAllocateVirtualMemory calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- VT rate limit hit for: SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe

Simulations

Behavior and APIs

Time	Type	Description
18:51:26	API Interceptor	532x Sleep call for process: SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe.log

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.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:\Windows\System32\drivers\etc\hosts

Process:	C:\Users\user\Desktop\SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	835
Entropy (8bit):	4.694294591169137
Encrypted:	false
SSDEEP:	24:QWDZh+ragzMZfuMMs1L/JU5fFCkK8T1rTt8:vDZhyoZWM9rU5fFcP
MD5:	6EB47C1CF858E25486E42440074917F2
SHA1:	6A63F93A95E1AE831C393A97158C526A4FA0FAAE
SHA-256:	9B13A3EA948A1071A81787AAC1930B89E30DF22CE13F8FF751F31B5D83E79FFB
SHA-512:	08437AB32E7E905EB11335E670CDD5D999803390710ED39CBC31A2D3F05868D5D0E5D051CCD7B06A85BB466932F99A220463D27FAC29116D241E8ADAC495FA F
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	# Copyright (c) 1993-2009 Microsoft Corp...#..# This is a sample HOSTS file used by Microsoft TCP/IP for Windows...#..# This file contains the mappings of IP addresses to host names. Each..# entry should be kept on an individual line. The IP address should..# be placed in the first column followed by the corresponding host name...# The IP address and the host name should be separated by at least one..# space...#..# Additionally, comments (such as these) may be inserted on individual..# lines or following the machine name denoted by a '#' symbol...#..# For example:..#..# 102.54.94.97 rhino.acme.com # source server..# 38.25.63.10 x.acme.com # x client host....# localhost name resolution is handled within DNS itself...#.127.0.0.1 localhost..#.::1 localhost....127.0.0.1

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.762601740842663
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe
File size:	835072
MD5:	d773da82f041dd37630e773240a97878
SHA1:	1eb7d229a442c4c49a9e3d7994e72d2062f8be59
SHA256:	f59af126d04f289707903724c3bfb87e50404154b89665b8f669649e3c24a503
SHA512:	842233ba5feada84cdca6bb5b491134f6e149c8a315e9923ec6ba05ab89cb81a1807d1997cd1a05856e4aa30f2b177e0c09dc18c79925ab2cc7068c3636be1cc
SSDEEP:	12288:IGPCzjEkC/cVfzktmrfGwVlT9CNPXLGL56D+sG7YFk9t08RNdHi5ug2PG:I2e6YGcdhcLGVDieG
TLSH:	0905E02876662F03C1A942F6C1DBA42803F15443A573D7C76FC631CA2B16BE95DC9B8B
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...J..b.....0..b...Z.....N.... .....@.. ....@.....

File Icon

Icon Hash:	4462f276dcec30e6

Static PE Info

General

Entrypoint:	0x4c804e
Entrypoint Section:	.text

Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6290DB4A [Fri May 27 14:08:10 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

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
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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xc8000	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xca000	0x57a0	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xd0000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0xc7fb3	0x1c	.text
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	0xc6054	0xc6200	False	0.887911573344	data	7.76150292506	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xca000	0x57a0	0x5800	False	0.964311079545	data	7.88907759888	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd0000	0xc	0x200	False	0.044921875	data	0.0980041756627	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0xca130	0x51a3	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_GROUP_ICON	0xcf2d4	0x14	data		
RT_VERSION	0xcf2e8	0x2cc	data		
RT_MANIFEST	0xcf5b4	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

Description	Data
Translation	0x0000 0x04b0
LegalCopyright	
Assembly Version	1.0.0.0
InternalName	IBind.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	
ProductVersion	1.0.0.0
FileDescription	
OriginalFilename	IBind.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.5109.232.216.96498515872840032 05/27/22-18:53:13.512096	TCP	2840032	ETPRO TROJAN Win32/AgentTesla/OriginLogger Data Exfil via SMTP M2	49851	587	192.168.2.5	109.232.216.96
192.168.2.5109.232.216.96498515872030171 05/27/22-18:53:13.512043	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49851	587	192.168.2.5	109.232.216.96

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 27, 2022 18:53:12.806375027 CEST	59933	53	192.168.2.5	8.8.8.8
May 27, 2022 18:53:12.865677118 CEST	53	59933	8.8.8.8	192.168.2.5
May 27, 2022 18:53:12.869817019 CEST	50829	53	192.168.2.5	8.8.8.8
May 27, 2022 18:53:12.926898003 CEST	53	50829	8.8.8.8	192.168.2.5

DNS Queries

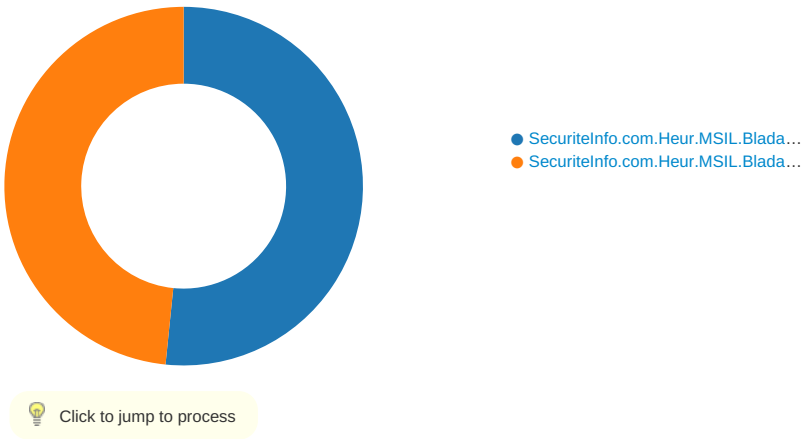
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 27, 2022 18:53:12.806375027 CEST	192.168.2.5	8.8.8.8	0xbe05	Standard query (0)	mail.waterchem.com.tr	A (IP address)	IN (0x0001)
May 27, 2022 18:53:12.869817019 CEST	192.168.2.5	8.8.8.8	0x83ab	Standard query (0)	mail.waterchem.com.tr	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 27, 2022 18:53:12.865677118 CEST	8.8.8.8	192.168.2.5	0xbe05	No error (0)	mail.waterchem.com.tr	waterchem.com.tr		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 18:53:12.865677118 CEST	8.8.8.8	192.168.2.5	0xbe05	No error (0)	waterchem.com.tr		109.232.216.96	A (IP address)	IN (0x0001)
May 27, 2022 18:53:12.926898003 CEST	8.8.8.8	192.168.2.5	0x83ab	No error (0)	mail.waterchem.com.tr	waterchem.com.tr		CNAME (Canonical name)	IN (0x0001)
May 27, 2022 18:53:12.926898003 CEST	8.8.8.8	192.168.2.5	0x83ab	No error (0)	waterchem.com.tr		109.232.216.96	A (IP address)	IN (0x0001)

Statistics

Behavior



System Behavior

Analysis Process: SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe PID: **7136**, Parent PID: **4912**

General

Target ID:	0
Start time:	18:51:04
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe"
Imagebase:	0x3c0000
File size:	835072 bytes
MD5 hash:	D773DA82F041DD37630E773240A97878
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: 00000000.00000002.495384487.0000000003F00000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.495384487.0000000003F00000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.494486784.0000000003B31000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.494486784.0000000003B31000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.491557261.0000000002AD0000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_zgRAT, Description: Detects zgRAT, Source: 00000000.00000002.498195237.0000000007440000.00000004.08000000.00040000.00000000.sdmp, Author: ditekSHen
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	6E68CF06	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	6E68CF06	unknown
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E99C78D	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\SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.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	6E99C907	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	6E665705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E665705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E5C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E66CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E5C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E5C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E5C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E5C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E665705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E665705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D4D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D4D1B4F	ReadFile

Analysis Process: SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe PID: **6444**, Parent PID: **7136**

General

Target ID:	3
Start time:	18:51:29
Start date:	27/05/2022
Path:	C:\Users\user\Desktop\SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\SecuriteInfo.com.Heur.MSIL.Bladabindi.1.9100.exe
Imagebase:	0x870000
File size:	835072 bytes
MD5 hash:	D773DA82F041DD37630E773240A97878
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: 00000003.00000000.484536622.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.484536622.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000000.482330735.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.482330735.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.692625873.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000002.692625873.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000000.483269443.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.483269443.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000002.695684477.0000000002C61000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000003.00000002.695684477.0000000002C61000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: MALWARE_Win_AgentTeslaV3, Description: AgentTeslaV3 infostealer payload, Source: 00000003.00000002.695684477.0000000002C61000.00000004.00000800.00020000.00000000.sdmp, Author: ditekSHen • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000003.00000000.481183749.0000000000402000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000003.00000000.481183749.0000000000402000.00000040.00000400.00020000.00000000.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	6E68CF06	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	6E68CF06	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Windows\System32\drivers\etc\hosts	824	11	0d 0a 31 32 37 2e 30 2e 30 2e 31	127.0.0.1	success or wait	1	6D4D1B4F	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	6E665705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E665705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E5C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E66CA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E5C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E5C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E5C03DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E5C03DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E665705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E665705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6D4D1B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6D4D1B4F	ReadFile

Disassembly

No disassembly