ID: 614683
Sample Name:
3EqRILOXx1.exe
Cookbook: default.jbs
Time: 07:29:11
Date: 25/04/2022
Version: 34.0.0 Boulder Opal

Table of Contents

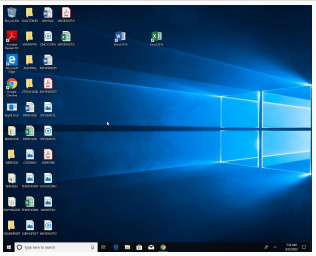
Windows Analysis Report

3EqRILOXx1.exe

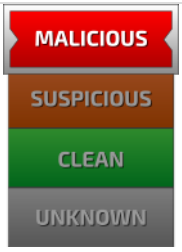
Overview

General Information

Sample Name:	3EqRILOXx1.exe
Analysis ID:	614683
MD5:	5ca02369b45067..
SHA1:	b11ff0b977b1686.
SHA256:	039c261036b80f..
Tags:	exe sansisc
Infos:	



Detection



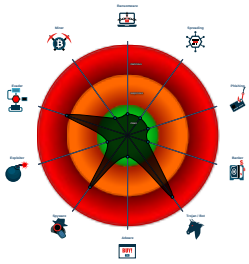
Snake Keylogger

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Multi AV Scanner detection for subm…
- Yara detected Snake Keylogger
- Malicious sample detected (through…
- Yara detected Telegram RAT
- Antivirus / Scanner detection for sub…
- Contains functionality to capture scr…
- .NET source code references suspic…
- Machine Learning detection for sam…
- May check the online IP address of…
- Uses 32bit PE files

Classification



Process Tree

- **System is w10x64**
- 3EqRILOXx1.exe (PID: 6192 cmdline: "C:\Users\user\Desktop\3EqRILOXx1.exe" MD5: 5CA02369B45067FE039314F38B286767)
  - dw20.exe (PID: 6484 cmdline: dw20.exe -x -s 1364 MD5: 8D10DA8A3E11747E51F23C882C22BBC3)
- **cleanup**

Malware Configuration

Threatname: Snake Keylogger

```
{
  "Exfil Mode": "FTP",
  "FTP Server": "ftp://103.147.185.85/",
  "Password": "bvhfgas7",
  "Port": 21
}
```

Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
3EqRILOXx1.exe	MAL_Envrial_Jan18_1	Detects Encrial credential stealer malware	Florian Roth	• 0x71d5e:$a2: \Comodo\Dragon\User Data\Default\Login Data • 0x70f47:$a3: \Google\Chrome\User Data\Default\Login Data • 0x7138e:$a4: \Orbitum\User Data\Default\Login Data • 0x7250f:$a5: \Kometa\User Data\Default\Login Data
3EqRILOXx1.exe	JoeSecurity_SnakeKeylogger	Yara detected Snake Keylogger	Joe Security	

Source	Rule	Description	Author	Strings
3EqRILOXx1.exe	JoeSecurity_TelegramRAT	Yara detected Telegram RAT	Joe Security	
3EqRILOXx1.exe	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
3EqRILOXx1.exe	INDICATOR_SUSPICIOUS_EXE_DotNetProcHook	Detects executables with potential process hoocking	ditekSHen	• 0x6c12a:$s1: UnHook • 0x6c131:$s2: SetHook • 0x6c139:$s3: CallNextHook • 0x6c146:$s4: _hook
Click to see the 1 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.318642073.0000000000782000.00000002.00000001.01000000.00000003.sdmp	JoeSecurity_SnakeKeylogger	Yara detected Snake Keylogger	Joe Security	
00000000.00000002.318642073.0000000000782000.00000002.00000001.01000000.00000003.sdmp	JoeSecurity_TelegramRAT	Yara detected Telegram RAT	Joe Security	
00000000.00000002.318642073.0000000000782000.00000002.00000001.01000000.00000003.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000000.00000002.318642073.0000000000782000.00000002.00000001.01000000.00000003.sdmp	MALWARE_Win_SnakeKeylogger	Detects Snake Keylogger	ditekSHen	• 0x6c7c9:$s8: GrabbedClp • 0x6ca71:$s9: StartKeylogger • 0x6f234:$x1: $%SMTPDV$ • 0x6dede:$x2: $#TheHashHere%& • 0x6decc:$x3: %FTPDV$ • 0x6f2c2:$x4: $%TelegramDv$ • 0x6cb00:$x5: KeyLoggerEventArgs • 0x6d1e8:$x5: KeyLoggerEventArgs • 0x6f260:$m1: \| Snake Keylogger • 0x6f322:$m1: | Snake Keylogger • 0x6f476:$m1: \| Snake Keylogger • 0x6f59c:$m1: | Snake Keylogger • 0x6f6f6:$m1: \| Snake Keylogger • 0x6f200:$m2: Clipboard Logs ID • 0x6f42c:$m2: Screenshot Logs ID • 0x6f540:$m2: keystroke Logs ID • 0x6f72c:$m3: SnakePW • 0x6f404:$m4: \SnakeKeylogger\
00000000.00000000.225338757.0000000000782000.00000002.00000001.01000000.00000003.sdmp	JoeSecurity_SnakeKeylogger	Yara detected Snake Keylogger	Joe Security	
Click to see the 7 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.0.3EqRILOXx1.exe.780000.0.unpack	MAL_Envrial_Jan18_1	Detects Encrial credential stealer malware	Florian Roth	• 0x71d5e:$a2: \Comodo\Dragon\User Data\Default\Login Data • 0x70f47:$a3: \Google\Chrome\User Data\Default\Login Data • 0x7138e:$a4: \Orbitum\User Data\Default\Login Data • 0x7250f:$a5: \Kometa\User Data\Default\Login Data
0.0.3EqRILOXx1.exe.780000.0.unpack	JoeSecurity_SnakeKeylogger	Yara detected Snake Keylogger	Joe Security	
0.0.3EqRILOXx1.exe.780000.0.unpack	JoeSecurity_TelegramRAT	Yara detected Telegram RAT	Joe Security	
0.0.3EqRILOXx1.exe.780000.0.unpack	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
0.0.3EqRILOXx1.exe.780000.0.unpack	INDICATOR_SUSPICIOUS_EXE_DotNetProcHook	Detects executables with potential process hoocking	ditekSHen	• 0x6c12a:$s1: UnHook • 0x6c131:$s2: SetHook • 0x6c139:$s3: CallNextHook • 0x6c146:$s4: _hook
Click to see the 7 entries				

Sigma Signatures

There are no malicious signatures, click here to show all signatures.

Snort Signatures

ETPRO TROJAN 404/Snake/Matiex Keylogger Style External IP Check - Source IP: 192.168.2.4 - Destination IP: 132.226.247.73

Timestamp:	04/25/22-07:30:14.530852 04/25/22-07:30:14.530852
SID:	2842536
Source Port:	49738
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

- Found malware configuration
- Multi AV Scanner detection for submitted file
- Antivirus / Scanner detection for submitted sample
- Machine Learning detection for sample

Networking

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- May check the online IP address of the machine

Key, Mouse, Clipboard, Microphone and Screen Capturing

- Contains functionality to capture screen (.Net source)

System Summary

- Malicious sample detected (through community Yara rule)

HIPS / PFW / Operating System Protection Evasion

- .NET source code references suspicious native API functions

Stealing of Sensitive Information

- Yara detected Snake Keylogger
- Yara detected Telegram RAT

Remote Access Functionality

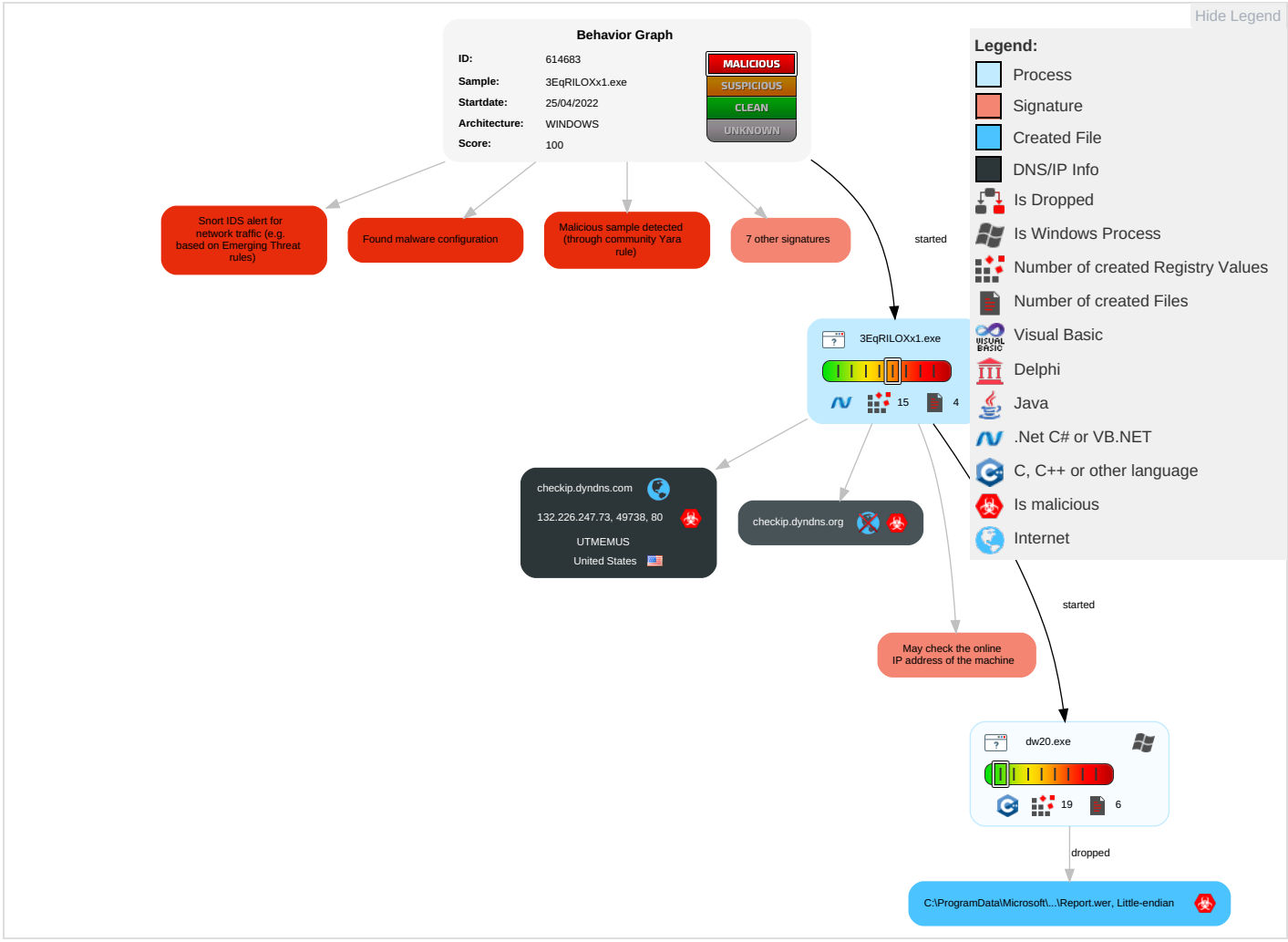
- Yara detected Snake Keylogger
- Yara detected Telegram RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	2 Command and Scripting Interpreter	Path Interception	1 Access Token Manipulation	1 Virtualization/Sandbox Evasion	OS Credential Dumping	1 Security Software Discovery	Remote Services	1 Screen Capture	Exfiltration Over Other Network Medium	2 Ingress Tool Transfer	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Native API	Boot or Logon Initialization Scripts	1 1 Process Injection	1 Disable or Modify Tools	LSASS Memory	1 Virtualization/Sandbox Evasion	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	2 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 Access Token Manipulation	Security Account Manager	1 Process Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 2 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 1 Process Injection	NTDS	1 Remote System 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 Deobfuscate/Decode Files or Information	LSA Secrets	1 System Network Configuration 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 Obfuscated Files or Information	Cached Domain Credentials	2 System Information 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	2 Software Packing	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

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
3EqRILOXx1.exe	69%	ReversingLabs	ByteCode-MSIL.Infostealer.Mintluks	
3EqRILOXx1.exe	100%	Avira	TR/ATRAPS.Gen	
3EqRILOXx1.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.0.3EqRILOXx1.exe.780000.0.unpack	100%	Avira	HEUR/AGEN.1203010		Download File
0.2.3EqRILOXx1.exe.780000.0.unpack	100%	Avira	HEUR/AGEN.1203010		Download File

Domains

Source	Detection	Scanner	Label	Link
checkip.dyndns.com	0%	Virustotal		Browse
checkip.dyndns.org	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://freegeoip.app/xml/	0%	URL Reputation	safe	
http://checkip.dyndns.org	0%	URL Reputation	safe	
http://checkip.dyndns.org/	0%	URL Reputation	safe	
http://checkip.dyndns.org/q	0%	URL Reputation	safe	
http://checkip.dyndns.orgx&Qq	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
checkip.dyndns.com	132.226.247.73	true	true	• 0%, Virustotal, Browse	unknown
checkip.dyndns.org	unknown	unknown	true	• 0%, Virustotal, Browse	unknown

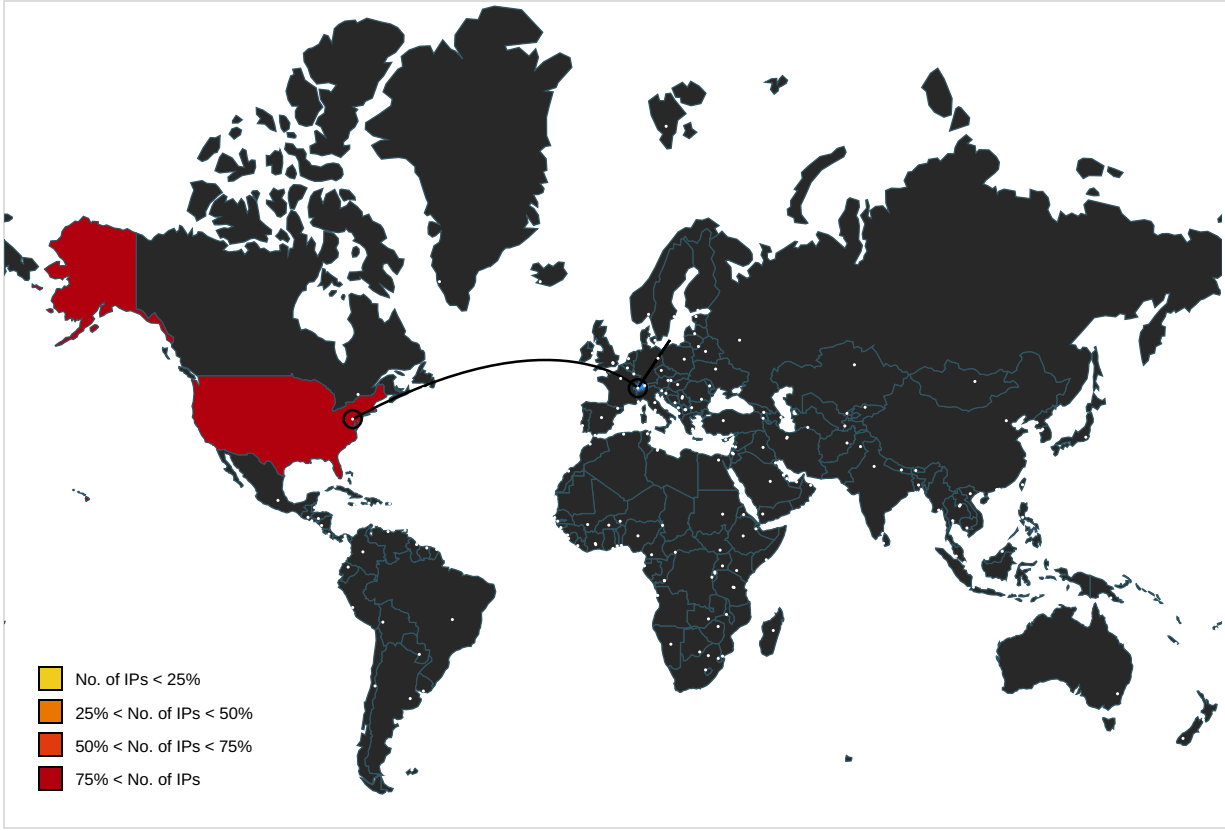
Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://checkip.dyndns.org/	true	• URL Reputation: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://freegeoip.app/xml/	3EqRILOXx1.exe	false	• URL Reputation: safe	unknown
http://checkip.dyndns.org	3EqRILOXx1.exe, 00000000.00000002.319518854.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://https://api.telegram.org/bot	3EqRILOXx1.exe	false		high
http://checkip.dyndns.org/q	3EqRILOXx1.exe	false	• URL Reputation: safe	unknown
http://checkip.dyndns.orgx&Qq	3EqRILOXx1.exe, 00000000.00000002.319518854.0000000002EC1000.00000004.00000800.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	low

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
132.226.247.73	checkip.dyndns.com	United States		16989	UTMEMUS	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	614683
Start date and time: 25/04/202207:29:11	2022-04-25 07:29:11 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 50s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	3EqRILOXx1.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:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@3/3@1/1
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 8.6% (good quality ratio 7.7%) • Quality average: 55.4% • Quality standard deviation: 28.5%

HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe, wuapihost.exe
- Excluded IPs from analysis (whitelisted): 52.182.143.212
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, fs.microsoft.com, onedsblobprdcus15.centralus.cloudapp.azure.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, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
07:30:55	API Interceptor	1x Sleep call for process: dw20.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:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_3EqRILOXx1.exe_ee11ed3d42939d22332a8251e19e2f7a90e88_00000000_1906d41a\Report.wer

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	65536
Entropy (8bit):	1.0655206820205292
Encrypted:	false
SSDEEP:	192:LwEji510DHHaKsn9fC59Fm1sNOAkRm5/u7sCS274lt1:sE+510jaKCg5/u7sCX4lt1

MD5:	F2243B207211AE71852BE57DF7C86BC4
SHA1:	3ABA79F29AE07D7448C93B2006647AB3230F78A8
SHA-256:	FBA21EFC03A5C054899A0815031322815DD79759370EB3A3546A650787A7FF17
SHA-512:	ECD985387E105E2067335DD2205933678FA4D1A500068565F56F201745B407FDDACD6A948D4E5F2C74E96570384FD6DD82FE318093B1DB995BE419F404425150
Malicious:	**true**
Reputation:	low
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.A.P.P.C.R.A.S.H.....E.v.e.n.t.T.i.m.e.=.1.3.2.9.5.3.3.8.2.2.2.0.3.7.7.2.5.6.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.9.5.3.3.8.2.2.2.7.4.0.8.4.8.8.....R.e.p.o.r.t.S.t.a.t.u.s.=.5.2.4.3.8.4.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.1.6.6.f.d.a.3.c.-.3.6.0.5.-.4.6.4.2.-.a.7.4.8.-.d.4.e.c.d.1.6.7.9.b.b.0.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....O.r.i.g.i.n.a.l.F.i.l.e.n.a.m.e.=.w.v.w.s.O.y.Z.p.B.T.r.B.O.U.x.p.i.Q.D.J.T...e.x.e.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.8.3.0.-.0.0.0.1.-.0.0.1.c.-.9.1.1.8.-.c.9.8.8.6.5.5.8.d.8.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.c.4.b.c.c.3.a.0.3.8.f.b.d.8.8.a.8.2.5.6.f.d.6.b.7.c.4.1.8.f.1.1.0.0.0.0.0.0.0.0.!.0.0.0.0.b.1.1.f.f.0.b.9.7.7.b.1.6.8.6.3.c.3.4.d.c.3.5.1.2.6.f.1.d.3.d.1.3.a.b.5.c.c.4.f.!.3.E.q.R.I.L.O.X.x.1...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.1././.0.9././.0.3.:.1.8.:.5.7.:.5.4.!.0.!.3.E.q.R.I.L.O.X.x.1...e.x.e.....B.o.o.

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5266.tmp.WERInternalMetadata.xml

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	7610
Entropy (8bit):	3.709037103507393
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNizj26B6Y4eSURgWgmf4T8Sv+p1V9b1fKHm:RrlsNi/26B6YhSURgWgmf4YSqV9pfz
MD5:	6FC24DEB25D133A71BDE3B90F4605205
SHA1:	D388155933CAE5A0A993EC13583628FA1D0F69F5
SHA-256:	B7499C986FF8920C3A82932AE9D03CFAC50D79E707CADF5BD69A64B7E398C08A
SHA-512:	669563F8FD5F0F1027E712D213220646D51A5E3F0F33EFD8BB83F419BE9FA62F5B357A27CCA0E7B4531DD62D51C684020266AFB7E65F5A409911E8E684D4AE47
Malicious:	false
Reputation:	low
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.</.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.</.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.</.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.</.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.</.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.</.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.</.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.</.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.</.L.C.I.D.>.....</.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.1.9.2.</.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5390.tmp.xml

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4600
Entropy (8bit):	4.515711899276359
Encrypted:	false
SSDEEP:	48:cvIwSD8zsFJgtWI9JVWgc8sqYjt8fm8M4JFKfeuJoF8D+q88xsJ1XE52tftud:uITff2kgrsqYWJFKLtDfuXk2tfld
MD5:	CF658A65942D584916E491A1A51BE94A
SHA1:	A4286EEB6E00E88349D4E2BC759DBAA4878DA2AD
SHA-256:	927152BBE0CE4E7A2C6B7BB9639EE32441FC908CC11864FC9F80C72C71091FC1
SHA-512:	C8B49B2A1E9712DC31A24B5EBBDA6EEE6A9F480042CABDB2044AD36BFCFA0422AD22B6543D67CF4654F041235636D355E3920F9263725ED8A8E88BF234D47CFB
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="1486961" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.7243202513703695

TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.79% • 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% • Win16/32 Executable Delphi generic (2074/23) 0.01%
File name:	3EqRILOXx1.exe
File size:	481280
MD5:	5ca02369b45067fe039314f38b286767
SHA1:	b11ff0b977b16863c34dc35126f1d3d13ab5cc4f
SHA256:	039c261036b80fd500607279933c43c4f1c78fdba1b54a9edbc8217df49ec154
SHA512:	302c954d724d00309a650661689316fd0898135463882af5ca787cdef4cf9c60e2144dc2f55f80ed6df5e7141730433e1c92ae68eb0f379f1473d050abf0d1a4
SSDEEP:	12288:eR3E3HDei3oXA2jCXgXLz/HQOqzjW/NP:eRU3Hq6oXA2jBXHnqzjG
TLSH:	7CA4E02D37E88900E2BED9B225B14011C7B9A802195FEE0D57D2F42D3E3D6948E5AFD7
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...2p2a.....L.....j... .....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x476aae
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61327032 [Fri Sep 3 18:57:54 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
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

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

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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x76a60	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x78000	0x606	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x7a000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x2000	0x8	.text
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x2008	0x48	.text
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x74ab4	0x74c00	False	0.836378730594	data	7.74079601316	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x78000	0x606	0x800	False	0.32568359375	data	3.50532555502	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x7a000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_VERSION	0x780a0	0x37c	data		
RT_MANIFEST	0x7841c	0x1ea	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

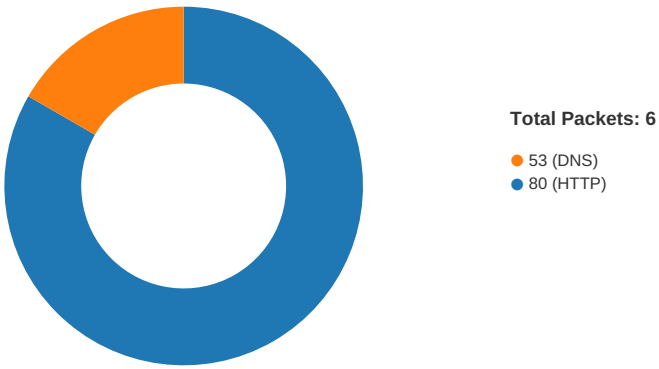
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2021
Assembly Version	1.0.0.0
InternalName	wvwsOyZpBTrBOUxpiQDJT.exe
FileVersion	1.0.0.0
CompanyName	
LegalTrademarks	
Comments	
ProductName	wvwsOyZpBTrBOUxpiQDJT
ProductVersion	1.0.0.0
FileDescription	wvwsOyZpBTrBOUxpiQDJT
OriginalFilename	wvwsOyZpBTrBOUxpiQDJT.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
04/25/22-07:30:14.530852 04/25/22-07:30:14.530852	TCP	2842536	ETPRO TROJAN 404/Snake/Matiex Keylogger Style External IP Check	49738	80	192.168.2.4	132.226.247.73

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 25, 2022 07:30:14.300725937 CEST	49738	80	192.168.2.4	132.226.247.73
Apr 25, 2022 07:30:14.530256033 CEST	80	49738	132.226.247.73	192.168.2.4
Apr 25, 2022 07:30:14.530395985 CEST	49738	80	192.168.2.4	132.226.247.73
Apr 25, 2022 07:30:14.530852079 CEST	49738	80	192.168.2.4	132.226.247.73
Apr 25, 2022 07:30:14.760173082 CEST	80	49738	132.226.247.73	192.168.2.4
Apr 25, 2022 07:30:21.409869909 CEST	80	49738	132.226.247.73	192.168.2.4
Apr 25, 2022 07:30:21.587019920 CEST	49738	80	192.168.2.4	132.226.247.73
Apr 25, 2022 07:30:56.630317926 CEST	49738	80	192.168.2.4	132.226.247.73

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Apr 25, 2022 07:30:14.181183100 CEST	64454	53	192.168.2.4	8.8.8.8
Apr 25, 2022 07:30:14.199006081 CEST	53	64454	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Apr 25, 2022 07:30:14.181183100 CEST	192.168.2.4	8.8.8.8	0xcf55	Standard query (0)	checkip.dyndns.org	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Apr 25, 2022 07:30:14.199006081 CEST	8.8.8.8	192.168.2.4	0xcf55	No error (0)	checkip.dyndns.org	checkip.dyndns.com		CNAME (Canonical name)	IN (0x0001)
Apr 25, 2022 07:30:14.199006081 CEST	8.8.8.8	192.168.2.4	0xcf55	No error (0)	checkip.dyndns.com		132.226.247.73	A (IP address)	IN (0x0001)
Apr 25, 2022 07:30:14.199006081 CEST	8.8.8.8	192.168.2.4	0xcf55	No error (0)	checkip.dyndns.com		132.226.8.169	A (IP address)	IN (0x0001)
Apr 25, 2022 07:30:14.199006081 CEST	8.8.8.8	192.168.2.4	0xcf55	No error (0)	checkip.dyndns.com		193.122.130.0	A (IP address)	IN (0x0001)
Apr 25, 2022 07:30:14.199006081 CEST	8.8.8.8	192.168.2.4	0xcf55	No error (0)	checkip.dyndns.com		193.122.6.168	A (IP address)	IN (0x0001)
Apr 25, 2022 07:30:14.199006081 CEST	8.8.8.8	192.168.2.4	0xcf55	No error (0)	checkip.dyndns.com		158.101.44.242	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- checkip.dyndns.org

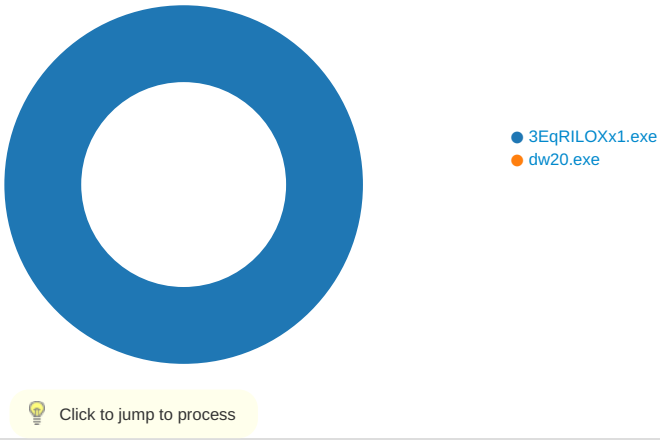
HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49738	132.226.247.73	80	C:\Users\user\Desktop\3EqRILOXx1.exe

Timestamp	kBytes transferred	Direction	Data
Apr 25, 2022 07:30:14.530852079 CEST	468	OUT	GET / HTTP/1.1 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR1.0.3705;) Host: checkip.dyndns.org Connection: Keep-Alive
Apr 25, 2022 07:30:21.409869909 CEST	1153	IN	HTTP/1.1 504 Gateway Time-out Date: Mon, 25 Apr 2022 05:30:21 GMT Content-Type: text/html Content-Length: 557 Connection: keep-alive Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 35 30 34 20 47 61 74 65 77 61 79 20 54 69 6d 65 2d 6f 75 74 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 35 30 34 20 47 61 74 65 77 61 79 20 54 69 6d 65 2d 6f 75 74 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a 3c 21 2d 2d 20 61 20 70 61 64 64 69 6e 67 20 74 6f 20 64 69 73 61 62 6c 65 20 4d 53 49 45 20 61 6e 64 20 43 68 72 6f 6d 65 20 66 72 69 65 6e 64 6c 79 20 65 72 72 6f 72 20 70 61 67 65 20 2d 2d 3e 0d 0a Data Ascii: <html><head><title>504 Gateway Time-out</title></head><body><center> 504 Gateway Time-out </center><hr><center></center></body></html>... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->... a padding to disable MSIE and Chrome friendly error page -->

Statistics

Behavior



System Behavior

Analysis Process: 3EqRILOXx1.exe PID: **6192**, Parent PID: **5664**

General

Target ID:	0
Start time:	07:30:11
Start date:	25/04/2022
Path:	C:\Users\user\Desktop\3EqRILOXx1.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\3EqRILOXx1.exe"
Imagebase:	0x780000
File size:	481280 bytes
MD5 hash:	5CA02369B45067FE039314F38B286767
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000000.00000002.318642073.0000000000782000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000000.00000002.318642073.0000000000782000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000002.318642073.0000000000782000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000000.00000002.318642073.0000000000782000.00000002.00000001.01000000.00000003.sdmp, Author: ditekSHen • Rule: JoeSecurity_SnakeKeylogger, Description: Yara detected Snake Keylogger, Source: 00000000.00000000.225338757.0000000000782000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_TelegramRAT, Description: Yara detected Telegram RAT, Source: 00000000.00000000.225338757.0000000000782000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000000.00000000.225338757.0000000000782000.00000002.00000001.01000000.00000003.sdmp, Author: Joe Security • Rule: MALWARE_Win_SnakeKeylogger, Description: Detects Snake Keylogger, Source: 00000000.00000000.225338757.0000000000782000.00000002.00000001.01000000.00000003.sdmp, Author: ditekSHen
Reputation:	low

File Activities

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: dw20.exe PID: **6484**, Parent PID: **6192**

General

Target ID:	4
Start time:	07:30:21
Start date:	25/04/2022
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
Wow64 process (32bit):	true
Commandline:	dw20.exe -x -s 1364
Imagebase:	0x10000000
File size:	33936 bytes
MD5 hash:	8D10DA8A3E11747E51F23C882C22BBC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Disassembly

No disassembly