ID: 756156
Sample Name: NHYGUnNN.exe
Cookbook: default.jbs
Time: 18:23:12
Date: 29/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

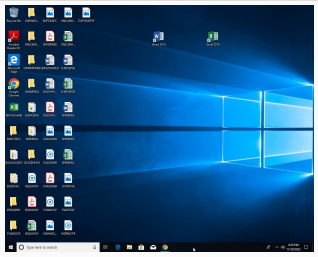
Windows Analysis Report

NHYGUnNN.exe

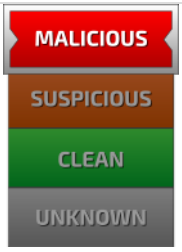
Overview

General Information

Sample Name:	NHYGUnNN.exe
Analysis ID:	756156
MD5:	4f9c8432b57fa1a..
SHA1:	e1cc52fd851621...
SHA256:	9f0d17930a9312..
Tags:	exe formbook
Infos:	



Detection



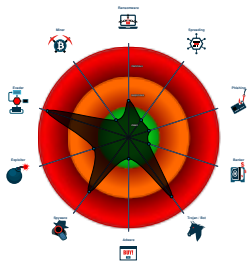
FormBook

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

Signatures

- Multi AV Scanner detection for subm...
- Yara detected FormBook
- Malicious sample detected (through...
- System process connects to networ...
- Snort IDS alert for network traffic
- Sample uses process hollowing tech...
- Tries to steal Mail credentials (via fi...
- Uses netstat to query active networ...
- Maps a DLL or memory area into an...
- Writes to foreign memory regions
- Machine Learning detection for sam...
- Allocates memory in foreign process...

Classification



Process Tree

- **System is w10x64**
- NHYGUnNN.exe (PID: 5380 cmdline: C:\Users\user\Desktop\NHYGUnNN.exe MD5: 4F9C8432B57FA1AA875071DE547BA947)
  - RegSvcs.exe (PID: 5148 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\Regsvcs.exe MD5: 2867A3817C9245F7CF518524DFD18F28)
    - explorer.exe (PID: 3452 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - NETSTAT.EXE (PID: 4844 cmdline: C:\Windows\SysWOW64\NETSTAT.EXE MD5: 4E20FF629119A809BC0E7EE2D18A7FDB)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.needook.com/4u5a/"
  ]
}
```

Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000002.497449022.0000000000FE0000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000A.00000002.497449022.0000000000FE0000.00000040.10000000.00040000.00000000.sdmp	Windows_Trojan_Formbook_1112e116	unknown	unknown	• 0x6631:$a1: 3C 30 50 4F 53 54 74 09 40 • 0x1f070:$a2: 74 0A 4E 0F B6 08 8D 44 08 01 75 F6 8D 70 01 0F B6 00 8D 55 • 0xa8cf:$a3: 1A D2 80 E2 AF 80 C2 7E EB 2A 80 FA 2F 75 11 8A D0 80 E2 01 • 0x17e07:$a4: 04 83 C4 0C 83 06 07 5B 5F 5E 8B E5 5D C3 8B 17 03 55 0C 6A 01 83
0000000A.00000002.497449022.0000000000FE0000.00000040.10000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x17c05:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x176b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x17d07:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x17e7f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa49a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x168fc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x1dde7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1edda:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000A.00000002.497449022.0000000000FE0000.00000040.10000000.00040000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x1a0e9:$sqlite3step: 68 34 1C 7B E1 • 0x1ac61:$sqlite3step: 68 34 1C 7B E1 • 0x1a12b:$sqlite3text: 68 38 2A 90 C5 • 0x1aca6:$sqlite3text: 68 38 2A 90 C5 • 0x1a142:$sqlite3blob: 68 53 D8 7F 8C • 0x1acbc:$sqlite3blob: 68 53 D8 7F 8C
0000000A.00000002.497017430.0000000000BC0000.00000040.80000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 18 entries				

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ETPRO TROJAN FormBook CnC Checkin (POST) - Source IP: 192.168.2.6 - Destination IP: 154.209.6.241

Timestamp:	192.168.2.6154.209.6.24149722802829004 11/29/22-18:25:42.914102
SID:	2829004
Source Port:	49722
Destination Port:	80
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Networking

System process connects to network (likely due to code injection or exploit)

Snort IDS alert for network traffic

Uses netstat to query active network connections and open ports

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Data Obfuscation

.NET source code contains potential unpacker

HIPS / PFW / Operating System Protection Evasion

System process connects to network (likely due to code injection or exploit)
Sample uses process hollowing technique
Maps a DLL or memory area into another process
Writes to foreign memory regions
Allocates memory in foreign processes
Injects a PE file into a foreign processes
Queues an APC in another process (thread injection)
Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information

Yara detected FormBook
Tries to steal Mail credentials (via file / registry access)
Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality

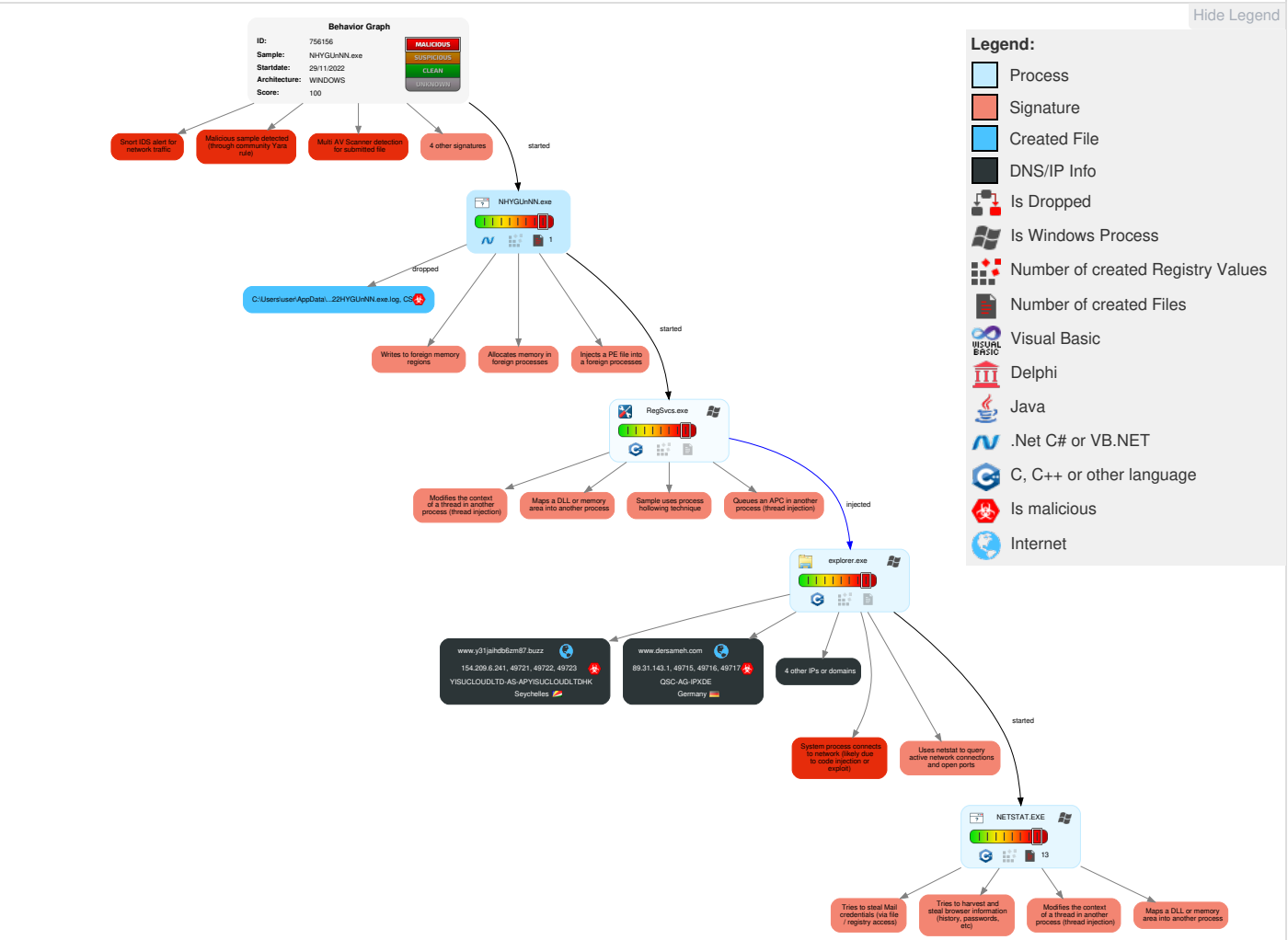
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Shared Modules	Path Interception	8 1 2 Process Injection	1 Masquerading	1 OS Credential Dumping	2 1 Security Software Discovery	Remote Services	1 Email Collection	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	1 Archive Collected Data	Exfiltration Over Bluetooth	3 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	3 1 Virtualization/Sandbox Evasion	Security Account Manager	3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	1 Data from Local System	Automated Exfiltration	4 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	8 1 2 Process Injection	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 1 4 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
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	4 Obfuscated Files or Information	Cached Domain Credentials	1 System Network Connections Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 2 Software Packing	DCSync	1 File and Directory Discovery	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	1 3 System Information Discovery	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue

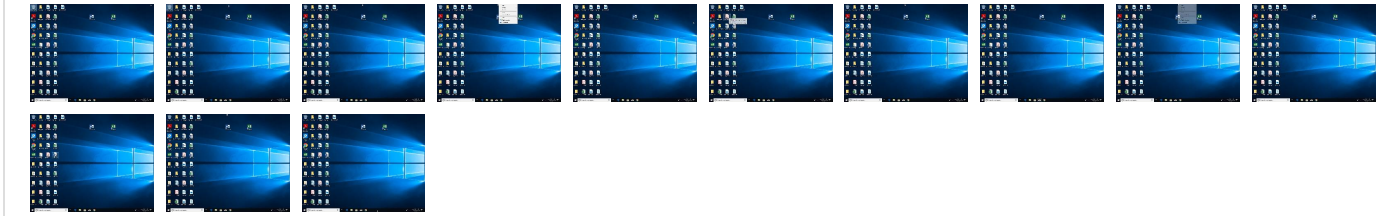
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
NHYGUnNN.exe	28%	ReversingLabs	ByteCode-MSIL.Trojan.Zilla	
NHYGUnNN.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
1.0.RegSvcs.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.marketmall.digital/4u5a/?GFQD=d2J0s&l0GX=+3a19pWtZng4d4VWOC/6zX+Mtu8c5OpbMBerEkzVlILtG/Qx1KaY9rLPGpDSvmBGoypiYd46AJSA/qrnjKpXW0Tn6YTEKB73Lei52b2L1E6m	0%	Avira URL Cloud	safe	
http://www.ope-cctv.com/4u5a/?GFQD=d2J0s&l0GX=PpVjBZYmN65mN/Cch5R9AL0rcoAD1Lxl4sTzWlpX/jy1IrupfQnyd2YG9N8O4SbWoFYU5LvyeEtp38l885KIODFzvvn/7iZ+w1zSOWQrPDed	0%	Avira URL Cloud	safe	
http://www.y31jaihdb6zm87.buzz/4u5a/	0%	Avira URL Cloud	safe	
www.needook.com/4u5a/	0%	Avira URL Cloud	safe	
http://www.dersameh.com/4u5a/?l0GX=DO8SLO7p+ieBn2EC0oYIAc7qa4Xo4oKKhL6K9ytUp3CH+6ohEz4QzFDvrvyjA4KB81/r5tutyqTX+rvP+Yb6ZUWqEETpfEhrV3qJRCQNMeQd&GFQD=d2J0s	0%	Avira URL Cloud	safe	
http://www.marketmall.digital/4u5a/	0%	Avira URL Cloud	safe	
http://www.darkchocolatebliss.com/4u5a/?GFQD=d2J0s&l0GX=pzMeEw2CLp9onsoEnnWxz7DjwWrmiPcXMIcMx0e8RMBYp3cHCqEf8wLsuyWBJtbijuVM0Zvb5p08kUy+wXRBHzYlQdhpzNTGfYmB4954z6O2	0%	Avira URL Cloud	safe	
http://www.darkchocolatebliss.com/4u5a/	0%	Avira URL Cloud	safe	
http://www.y31jaihdb6zm87.buzz/4u5a/?l0GX=odL+ljtDJZnnvHXGVqz6MYcHTNNFW2XRvrcwy4k99/9PUVuyA+q7lKaiZ8dF4agdsl/xXcCsqSWGiuLBWKJZJi8UVH1n7ApvhveD6637F7nt&GFQD=d2J0s	0%	Avira URL Cloud	safe	
http://www.dersameh.com/4u5a/	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.darkchocolatebliss.com	54.38.220.85	true	true		unknown
www.marketmall.digital	162.213.255.142	true	true		unknown
www.canadianlocalbusiness.com	172.67.148.132	true	true		unknown
www.y31jaihdb6zm87.buzz	154.209.6.241	true	true		unknown
www.ope-cctv.com	38.55.236.89	true	true		unknown
www.dersameh.com	89.31.143.1	true	true		unknown

Contacted URLs

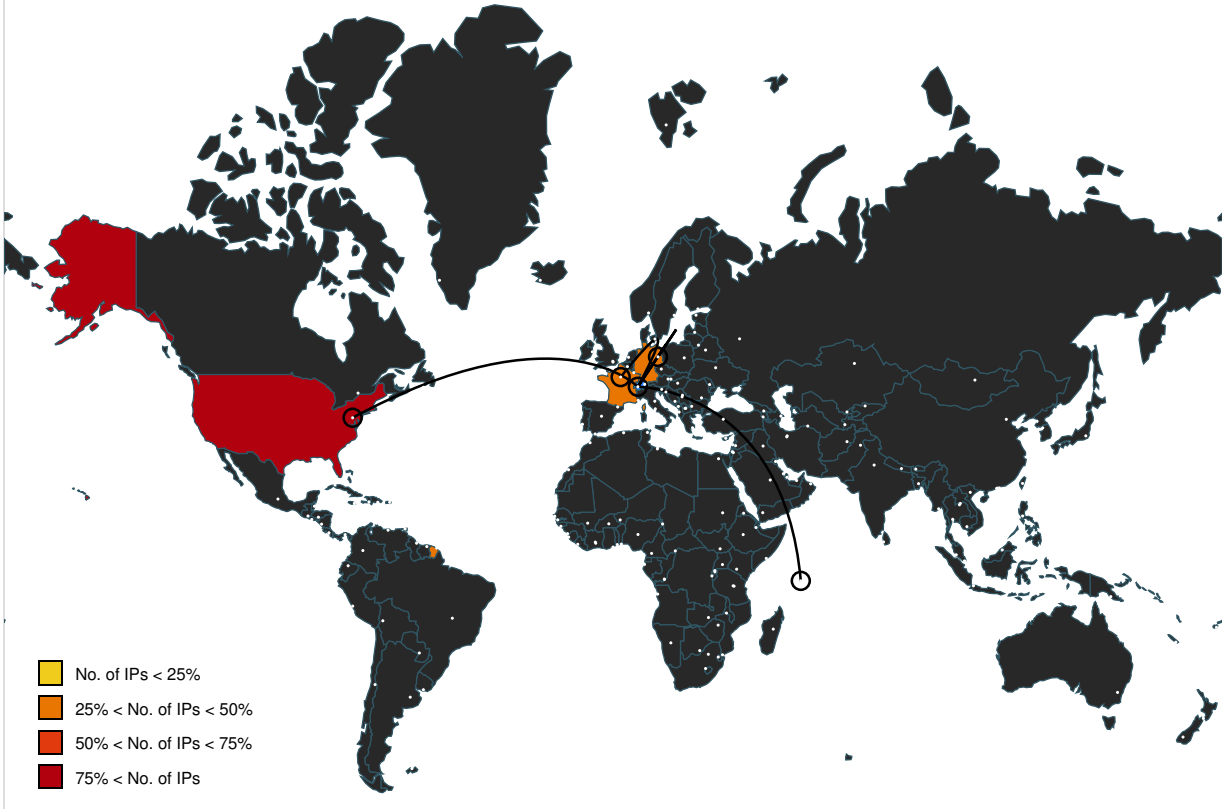
Name	Malicious	Antivirus Detection	Reputation
http://www.y31jaihdb6zm87.buzz/4u5a/	true	• Avira URL Cloud: safe	unknown
http://www.marketmall.digital/4u5a/?GFQD=d2J0s&l0GX=+3a19pWtZng4d4VWOC/6zX+Mtu8c5OpbMBerEkzVlILtG/Qx1KaY9rLPGpDSvmBGoypiYd46AJSA/qrnjKpXW0Tn6YTEKB73Lei52b2L1E6m	true	• Avira URL Cloud: safe	unknown
http://www.ope-cctv.com/4u5a/?GFQD=d2J0s&l0GX=PpVjBZYmN65mN/Cch5R9AL0rcoAD1Lxl4sTzWlpX/jy1IrupfQnyd2YG9N8O4SbWoFYU5LvyeEtp38l885KIODFzvvn/7iZ+w1zSOWQrPDed	true	• Avira URL Cloud: safe	unknown
http://www.dersameh.com/4u5a/?l0GX=DO8SLO7p+ieBn2EC0oYIAc7qa4Xo4oKKhL6K9ytUp3CH+6ohEz4QzFDvrvyjA4KB81/r5tutyqTX+rvP+Yb6ZUWqEETpfEhrV3qJRCQNMeQd&GFQD=d2J0s	true	• Avira URL Cloud: safe	unknown
http://www.marketmall.digital/4u5a/	true	• Avira URL Cloud: safe	unknown
www.needook.com/4u5a/	true	• Avira URL Cloud: safe	low
http://www.darkchocolatebliss.com/4u5a/?GFQD=d2J0s&l0GX=pzMeEw2CLp9onsoEnnWxz7DjwWrmiPcXMIcMx0e8RMBYp3cHCqEf8wLsuyWBJtbijuVM0Zvb5p08kUy+wXRBHzYlQdhpzNTGfYmB4954z6O2	true	• Avira URL Cloud: safe	unknown
http://www.y31jaihdb6zm87.buzz/4u5a/?l0GX=odL+ljtDJZnnvHXGVqz6MYcHTNNFW2XRvrcwy4k99/9PUVuyA+q7lKaiZ8dF4agdsl/xXcCsqSWGiuLBWKJZJi8UVH1n7ApvhveD6637F7nt&GFQD=d2J0s	true	• Avira URL Cloud: safe	unknown
http://www.dersameh.com/4u5a/	true	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.darkchocolatebliss.com/4u5a/	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://ac.ecosia.org/autocomplete?q=	1--Lt08NN.10.dr	false		high
http://https://search.yahoo.com?fr=crmas_sfp	1--Lt08NN.10.dr	false		high
http://www.autoitscript.com/autoit3/J	explorer.exe, 00000002.00000000.29511176 4.0000000000AC8000.00000004.00000020.000 20000.00000000.sdmp, explorer.exe, 00000 002.00000000.274166451.0000000000AC8000. 00000004.00000020.00020000.00000000.sdmp, explorer.exe, 00000002.00000000.304813988.000000 0008442000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 00000002.0000 0000.240724345.0000000000AC8000.00000004 .00000020.00020000.00000000.sdmp, explorer.exe, 00000002.00000000.283521778.00000000084420 00.00000004.00000001.00020000.00000000.sdmp, explorer.exe, 00000002.00000000.253709611.000 0000008442000.00000004.00000001.00020000 .00000000.sdmp	false		high
http://https://duckduckgo.com/chrome_newtab	1--Lt08NN.10.dr	false		high
http://https://duckduckgo.com/ac/?q=	1--Lt08NN.10.dr	false		high
http://https://www.google.com/images/branding/product/ico/googleg_lodp.ico	1--Lt08NN.10.dr	false		high
http://https://search.yahoo.com?fr=crmas_sfpf	1--Lt08NN.10.dr	false		high
http://https://duckduckgo.com/favicon.icohttps://duckduckgo.com/?q=	1--Lt08NN.10.dr	false		high
http://https://search.yahoo.com/favicon.icohttps://search.yahoo.com/search	1--Lt08NN.10.dr	false		high
http://https://cdn.ecosia.org/assets/images/ico/favicon.icohttps://www.ecosia.org/search?q=	1--Lt08NN.10.dr	false		high
http://https://search.yahoo.com/sugg/chrome?output=fxjson&appid=crmas_sfp&command=	1--Lt08NN.10.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
38.55.236.89	www.ope-cctv.com	United States		174	COGENT-174US	true
89.31.143.1	www.dersameh.com	Germany		15598	QSC-AG-IPXDE	true
172.67.148.132	www.canadianlocalbusiness.com	United States		13335	CLOUDFLARENETUS	true
54.38.220.85	www.darkchocolatebliss.com	France		16276	OVHFR	true
162.213.255.142	www.marketmall.digital	United States		22612	NAMECHEAP-NETUS	true
154.209.6.241	www.y31jaihdb6zm87.buzz	Seychelles		136970	YISUCLOUDLTD-AS-APYISUCLOUDLTDHK	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	756156
Start date and time:	2022-11-29 18:23:12 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	NHYGUnNN.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 104, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	12
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.evad.winEXE@4/2@6/6
EGA Information:	• Successful, ratio: 66.7%
HDC Information:	• Successful, ratio: 41.7% (good quality ratio 36.2%) • Quality average: 71.1% • Quality standard deviation: 33.6%
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe

Warnings

- Exclude process from analysis (whitelisted): MpCmdRun.exe, SgrmBroker.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): client.wns.windows.com, fs.microsoft.com, ctldl.windowsupdate.com
- Execution Graph export aborted for target NHYGUnNN.exe, PID 5380 because it is empty
- Not all processes where analyzed, report is missing behavior information
- Report creation exceeded maximum time and may have missing d isassembly code information.

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\NHYGUnNN.exe
File Type:	CSV text
Category:	dropped
Size (bytes):	226
Entropy (8bit):	5.354940450065058
Encrypted:	false
SSDEEP:	6:Q3La/xw5DLIP12MUAvvR+uTL2wlAsDZilv:Q3La/KDLI4MWuPTxAlv
MD5:	B10E37251C5B495643F331DB2EEC3394
SHA1:	25A5FFE4C2554C2B9A7C2794C9FE215998871193
SHA-256:	8A6B926C70F8DCFD915D68F167A1243B9DF7B9F642304F570CE584832D12102D
SHA-512:	296BC182515900934AA96E996FC48B565B7857801A07FEFA0D3D1E0C165981B266B084E344DB5B53041D1171F9C6708B4EE0D444906391C4FC073BCC23B92C37
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_64\System\10a17139182a9efd561f01fada9688a5\System.ni.dll",0..

C:\Users\user\AppData\Local\Temp\1--Lt08NN

Process:	C:\Windows\SysWOW64\NETSTAT.EXE
File Type:	SQLite 3.x database, last written using SQLite version 3038005, page size 2048, file counter 3, database pages 45, cookie 0x3d, schema 4, UTF-8, version-valid-for 3
Category:	dropped
Size (bytes):	94208
Entropy (8bit):	1.2891393435168748
Encrypted:	false
SSDEEP:	192:Qo1/8dpUXbSzTPJPe6lVuvCySEwn7PrH944:QS/inmjVuaySEwn7b944
MD5:	037D23498B81732EEAAAD0E8015F3F85
SHA1:	E7719865D7717A4B36D85609F3EC25C10934587F
SHA-256:	83AA9D5727AD94D394C57A969A7C53C37F79513316FA5E0283A750C886F342D4
SHA-512:	BFFFB8C7759B65BABD232200305699551AC9BF9BF2C778D5DA124A677900869254C6AB4439BF2A99E08690C29C5A2B17EEEBA7382CF4EAAB12168462A49B3D7D
Malicious:	false
Reputation:	moderate, very likely benign file

Preview:	SQLite format 3.....@ .....-.....=.....[5.....*..... ....

Static File Info

General

File type:	PE32+ executable (GUI) x86-64 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.833885184563826
TrID:	• Win64 Executable GUI Net Framework (217006/5) 47.53% • Win64 Executable GUI (202006/5) 44.25% • Win64 Executable (generic) Net Framework (21505/4) 4.71% • Win64 Executable (generic) (12005/4) 2.63% • Generic Win/DOS Executable (2004/3) 0.44%
File name:	NHYGUnNN.exe
File size:	275456
MD5:	4f9c8432b57fa1aa875071de547ba947
SHA1:	e1cc52fd851621743ba562a65161bfafed8e6b2b
SHA256:	9f0d17930a9312b8d8dfb23119b57fed676a1bb15fc1582754ab94201651b221
SHA512:	ced221c2e5225a8ead486e52f1c5307b24dbaff8864c7262f2d6f58cad3184753d1f2afe525c3afa122ddcafeab38845dafd2f7a22169bfac026375e7962481d
SSDEEP:	6144:RhwendE8+/O+oImP2Qcy7ZwpeA9pg6Cer0K7+UUcT9gxyRClRcOpoik:EAHdP7ZwpeApT0K7+UUQ99RORcOpoR
TLSH:	B24401917785748FC98ECF3B86A03859097991733B0BD39B94423CA9491E3DE5E13BA3
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d.....c.....0.....0..... ....@..... .....`...@.....@..... .....

File Icon

Icon Hash:	30f0c4ccccc6b010

Static PE Info

General

Entrypoint:	0x400000
Entrypoint Section:	
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, LOCAL_SYMS_STRIPPED, LARGE_ADDRESS_AWARE
DLL Characteristics:	HIGH_ENTROPY_VA, DYNAMIC_BASE, NX_COMPAT, NO_SEH, TERMINAL_SERVER_AWARE
Time Stamp:	0x6385B386 [Tue Nov 29 07:23:50 2022 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	

Entrypoint Preview

Instruction
dec ebp
pop edx
nop
add byte ptr [ebx], al
add byte ptr [eax], al

Instruction
add byte ptr [eax+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	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x46000	0x1714	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x3e660	0x1c	.text
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
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	0x41628	0x41800	False	0.9183936665076335	data	7.879743437690199	IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_MEM_READ
.reloc	0x44000	0xc	0x200	False	0.044921875	data	0.10191042566270775	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ
.rsrc	0x46000	0x1714	0x1800	False	0.265625	data	4.38448712577448	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

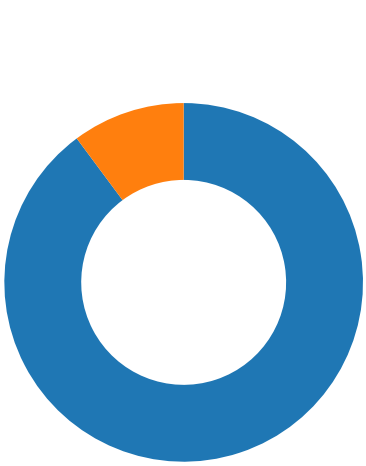
Name	RVA	Size	Type	Language	Country
RT_ICON	0x46130	0x10a8	Device independent bitmap graphic, 32 x 64 x 32, image size 4096		
RT_GROUP_ICON	0x471d8	0x14	data		
RT_VERSION	0x471ec	0x33c	data		
RT_MANIFEST	0x47528	0x1ea	XML 1.0 document, Unicode text, UTF-8 (with BOM) text, with CRLF line terminators		

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.6154.209.6.24149722802829004 11/29/22-18:25:42.914102	TCP	2829004	ETPRO TROJAN FormBook CnC Checkin (POST)	49722	80	192.168.2.6	154.209.6.241

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 18:25:06.857711077 CET	49714	80	192.168.2.6	38.55.236.89
Nov 29, 2022 18:25:07.176563978 CET	80	49714	38.55.236.89	192.168.2.6
Nov 29, 2022 18:25:07.177164078 CET	49714	80	192.168.2.6	38.55.236.89
Nov 29, 2022 18:25:07.177280903 CET	49714	80	192.168.2.6	38.55.236.89
Nov 29, 2022 18:25:07.495994091 CET	80	49714	38.55.236.89	192.168.2.6
Nov 29, 2022 18:25:07.496047974 CET	80	49714	38.55.236.89	192.168.2.6
Nov 29, 2022 18:25:07.496076107 CET	80	49714	38.55.236.89	192.168.2.6
Nov 29, 2022 18:25:07.496227980 CET	49714	80	192.168.2.6	38.55.236.89
Nov 29, 2022 18:25:07.496602058 CET	49714	80	192.168.2.6	38.55.236.89
Nov 29, 2022 18:25:07.815313101 CET	80	49714	38.55.236.89	192.168.2.6
Nov 29, 2022 18:25:12.533631086 CET	49715	80	192.168.2.6	89.31.143.1
Nov 29, 2022 18:25:12.553531885 CET	80	49715	89.31.143.1	192.168.2.6
Nov 29, 2022 18:25:12.553693056 CET	49715	80	192.168.2.6	89.31.143.1
Nov 29, 2022 18:25:12.554054976 CET	49715	80	192.168.2.6	89.31.143.1
Nov 29, 2022 18:25:12.573877096 CET	80	49715	89.31.143.1	192.168.2.6
Nov 29, 2022 18:25:12.576395035 CET	80	49715	89.31.143.1	192.168.2.6
Nov 29, 2022 18:25:12.576421022 CET	80	49715	89.31.143.1	192.168.2.6
Nov 29, 2022 18:25:12.576509953 CET	49715	80	192.168.2.6	89.31.143.1
Nov 29, 2022 18:25:13.563682079 CET	49715	80	192.168.2.6	89.31.143.1
Nov 29, 2022 18:25:14.580615997 CET	49716	80	192.168.2.6	89.31.143.1
Nov 29, 2022 18:25:14.601016045 CET	80	49716	89.31.143.1	192.168.2.6
Nov 29, 2022 18:25:14.601304054 CET	49716	80	192.168.2.6	89.31.143.1
Nov 29, 2022 18:25:14.601547003 CET	49716	80	192.168.2.6	89.31.143.1
Nov 29, 2022 18:25:14.621640921 CET	80	49716	89.31.143.1	192.168.2.6
Nov 29, 2022 18:25:14.621699095 CET	80	49716	89.31.143.1	192.168.2.6
Nov 29, 2022 18:25:14.623873949 CET	80	49716	89.31.143.1	192.168.2.6
Nov 29, 2022 18:25:14.623893976 CET	80	49716	89.31.143.1	192.168.2.6
Nov 29, 2022 18:25:16.626898050 CET	49717	80	192.168.2.6	89.31.143.1
Nov 29, 2022 18:25:16.647209883 CET	80	49717	89.31.143.1	192.168.2.6
Nov 29, 2022 18:25:16.647319078 CET	49717	80	192.168.2.6	89.31.143.1
Nov 29, 2022 18:25:16.654036999 CET	49717	80	192.168.2.6	89.31.143.1
Nov 29, 2022 18:25:16.675849915 CET	80	49717	89.31.143.1	192.168.2.6
Nov 29, 2022 18:25:16.677865982 CET	80	49717	89.31.143.1	192.168.2.6
Nov 29, 2022 18:25:16.677930117 CET	80	49717	89.31.143.1	192.168.2.6
Nov 29, 2022 18:25:16.677973986 CET	80	49717	89.31.143.1	192.168.2.6
Nov 29, 2022 18:25:16.678021908 CET	80	49717	89.31.143.1	192.168.2.6
Nov 29, 2022 18:25:16.678031921 CET	49717	80	192.168.2.6	89.31.143.1
Nov 29, 2022 18:25:16.678061962 CET	49717	80	192.168.2.6	89.31.143.1
Nov 29, 2022 18:25:16.678066969 CET	80	49717	89.31.143.1	192.168.2.6
Nov 29, 2022 18:25:16.678113937 CET	80	49717	89.31.143.1	192.168.2.6
Nov 29, 2022 18:25:16.678148985 CET	80	49717	89.31.143.1	192.168.2.6

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 18:25:16.678157091 CET	49717	80	192.168.2.6	89.31.143.1
Nov 29, 2022 18:25:16.678191900 CET	49717	80	192.168.2.6	89.31.143.1
Nov 29, 2022 18:25:16.678610086 CET	49717	80	192.168.2.6	89.31.143.1
Nov 29, 2022 18:25:16.698600054 CET	80	49717	89.31.143.1	192.168.2.6
Nov 29, 2022 18:25:21.757518053 CET	49718	80	192.168.2.6	54.38.220.85
Nov 29, 2022 18:25:21.776348114 CET	80	49718	54.38.220.85	192.168.2.6
Nov 29, 2022 18:25:21.776595116 CET	49718	80	192.168.2.6	54.38.220.85
Nov 29, 2022 18:25:21.776768923 CET	49718	80	192.168.2.6	54.38.220.85
Nov 29, 2022 18:25:21.795433998 CET	80	49718	54.38.220.85	192.168.2.6
Nov 29, 2022 18:25:21.795470953 CET	80	49718	54.38.220.85	192.168.2.6
Nov 29, 2022 18:25:21.795599937 CET	49718	80	192.168.2.6	54.38.220.85
Nov 29, 2022 18:25:22.783147097 CET	49718	80	192.168.2.6	54.38.220.85
Nov 29, 2022 18:25:22.801913977 CET	80	49718	54.38.220.85	192.168.2.6
Nov 29, 2022 18:25:23.803277016 CET	49719	80	192.168.2.6	54.38.220.85
Nov 29, 2022 18:25:23.821763039 CET	80	49719	54.38.220.85	192.168.2.6
Nov 29, 2022 18:25:23.821918011 CET	49719	80	192.168.2.6	54.38.220.85
Nov 29, 2022 18:25:23.822163105 CET	49719	80	192.168.2.6	54.38.220.85
Nov 29, 2022 18:25:23.840464115 CET	80	49719	54.38.220.85	192.168.2.6
Nov 29, 2022 18:25:23.840503931 CET	80	49719	54.38.220.85	192.168.2.6
Nov 29, 2022 18:25:23.840524912 CET	80	49719	54.38.220.85	192.168.2.6
Nov 29, 2022 18:25:25.846643925 CET	49720	80	192.168.2.6	54.38.220.85
Nov 29, 2022 18:25:25.865328074 CET	80	49720	54.38.220.85	192.168.2.6
Nov 29, 2022 18:25:25.865495920 CET	49720	80	192.168.2.6	54.38.220.85
Nov 29, 2022 18:25:25.865695000 CET	49720	80	192.168.2.6	54.38.220.85
Nov 29, 2022 18:25:25.883969069 CET	80	49720	54.38.220.85	192.168.2.6
Nov 29, 2022 18:25:25.884027958 CET	80	49720	54.38.220.85	192.168.2.6
Nov 29, 2022 18:25:25.884074926 CET	80	49720	54.38.220.85	192.168.2.6
Nov 29, 2022 18:25:25.884263992 CET	49720	80	192.168.2.6	54.38.220.85
Nov 29, 2022 18:25:25.884419918 CET	49720	80	192.168.2.6	54.38.220.85
Nov 29, 2022 18:25:25.902769089 CET	80	49720	54.38.220.85	192.168.2.6
Nov 29, 2022 18:25:31.069607019 CET	49721	80	192.168.2.6	154.209.6.241
Nov 29, 2022 18:25:31.454494953 CET	80	49721	154.209.6.241	192.168.2.6
Nov 29, 2022 18:25:31.454699993 CET	49721	80	192.168.2.6	154.209.6.241
Nov 29, 2022 18:25:31.457118988 CET	49721	80	192.168.2.6	154.209.6.241
Nov 29, 2022 18:25:32.221436024 CET	49721	80	192.168.2.6	154.209.6.241
Nov 29, 2022 18:25:32.471544981 CET	49721	80	192.168.2.6	154.209.6.241
Nov 29, 2022 18:25:32.606439114 CET	80	49721	154.209.6.241	192.168.2.6
Nov 29, 2022 18:25:32.606645107 CET	80	49721	154.209.6.241	192.168.2.6
Nov 29, 2022 18:25:32.606683016 CET	80	49721	154.209.6.241	192.168.2.6
Nov 29, 2022 18:25:32.606717110 CET	49721	80	192.168.2.6	154.209.6.241
Nov 29, 2022 18:25:32.606791973 CET	49721	80	192.168.2.6	154.209.6.241
Nov 29, 2022 18:25:32.856290102 CET	80	49721	154.209.6.241	192.168.2.6
Nov 29, 2022 18:25:32.856455088 CET	49721	80	192.168.2.6	154.209.6.241
Nov 29, 2022 18:25:33.490314960 CET	49722	80	192.168.2.6	154.209.6.241
Nov 29, 2022 18:25:36.508388996 CET	49722	80	192.168.2.6	154.209.6.241
Nov 29, 2022 18:25:42.519331932 CET	49722	80	192.168.2.6	154.209.6.241
Nov 29, 2022 18:25:42.913681030 CET	80	49722	154.209.6.241	192.168.2.6
Nov 29, 2022 18:25:42.913929939 CET	49722	80	192.168.2.6	154.209.6.241
Nov 29, 2022 18:25:42.914102077 CET	49722	80	192.168.2.6	154.209.6.241
Nov 29, 2022 18:25:43.308163881 CET	80	49722	154.209.6.241	192.168.2.6
Nov 29, 2022 18:25:43.308239937 CET	49722	80	192.168.2.6	154.209.6.241
Nov 29, 2022 18:25:43.925580978 CET	49722	80	192.168.2.6	154.209.6.241
Nov 29, 2022 18:25:44.097312927 CET	49722	80	192.168.2.6	154.209.6.241
Nov 29, 2022 18:25:44.491835117 CET	80	49722	154.209.6.241	192.168.2.6
Nov 29, 2022 18:25:44.491909027 CET	80	49722	154.209.6.241	192.168.2.6
Nov 29, 2022 18:25:44.492044926 CET	49722	80	192.168.2.6	154.209.6.241
Nov 29, 2022 18:25:44.494973898 CET	49722	80	192.168.2.6	154.209.6.241
Nov 29, 2022 18:25:44.942090988 CET	49723	80	192.168.2.6	154.209.6.241
Nov 29, 2022 18:25:45.283199072 CET	80	49722	154.209.6.241	192.168.2.6

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 29, 2022 18:25:06.826121092 CET	59504	53	192.168.2.6	8.8.8.8
Nov 29, 2022 18:25:06.849574089 CET	53	59504	8.8.8.8	192.168.2.6
Nov 29, 2022 18:25:12.510191917 CET	65198	53	192.168.2.6	8.8.8.8
Nov 29, 2022 18:25:12.532123089 CET	53	65198	8.8.8.8	192.168.2.6
Nov 29, 2022 18:25:21.723710060 CET	62910	53	192.168.2.6	8.8.8.8
Nov 29, 2022 18:25:21.755763054 CET	53	62910	8.8.8.8	192.168.2.6
Nov 29, 2022 18:25:30.897186995 CET	63863	53	192.168.2.6	8.8.8.8
Nov 29, 2022 18:25:31.068085909 CET	53	63863	8.8.8.8	192.168.2.6
Nov 29, 2022 18:25:50.761020899 CET	63229	53	192.168.2.6	8.8.8.8
Nov 29, 2022 18:25:50.808146954 CET	53	63229	8.8.8.8	192.168.2.6
Nov 29, 2022 18:26:01.743686914 CET	62538	53	192.168.2.6	8.8.8.8
Nov 29, 2022 18:26:01.772579908 CET	53	62538	8.8.8.8	192.168.2.6

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 29, 2022 18:25:06.826121092 CET	192.168.2.6	8.8.8.8	0x2214	Standard query (0)	www.ope-cctv.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 18:25:12.510191917 CET	192.168.2.6	8.8.8.8	0x7524	Standard query (0)	www.dersameh.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 18:25:21.723710060 CET	192.168.2.6	8.8.8.8	0x2444	Standard query (0)	www.darkchocolatebliss.com	A (IP address)	IN (0x0001)	false
Nov 29, 2022 18:25:30.897186995 CET	192.168.2.6	8.8.8.8	0xa02a	Standard query (0)	www.y31jaihdb6zm87.buzz	A (IP address)	IN (0x0001)	false
Nov 29, 2022 18:25:50.761020899 CET	192.168.2.6	8.8.8.8	0xeb7d	Standard query (0)	www.marketmall.digital	A (IP address)	IN (0x0001)	false
Nov 29, 2022 18:26:01.743686914 CET	192.168.2.6	8.8.8.8	0xd179	Standard query (0)	www.canadianlocalbusiness.com	A (IP address)	IN (0x0001)	false

DNS Answers

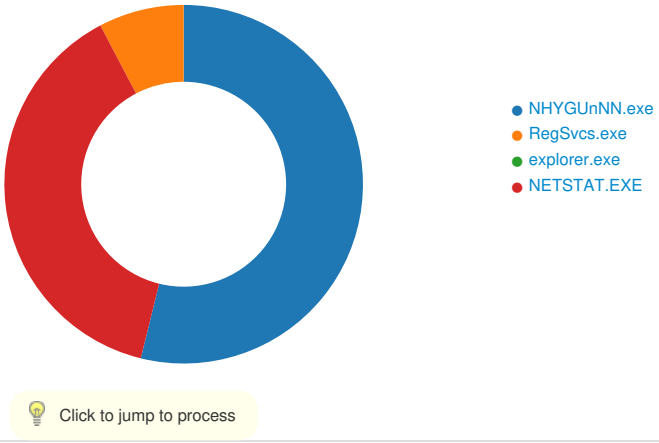
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 29, 2022 18:25:06.849574089 CET	8.8.8.8	192.168.2.6	0x2214	No error (0)	www.ope-cctv.com		38.55.236.89	A (IP address)	IN (0x0001)	false
Nov 29, 2022 18:25:12.532123089 CET	8.8.8.8	192.168.2.6	0x7524	No error (0)	www.dersameh.com		89.31.143.1	A (IP address)	IN (0x0001)	false
Nov 29, 2022 18:25:21.755763054 CET	8.8.8.8	192.168.2.6	0x2444	No error (0)	www.darkchocolatebliss.com		54.38.220.85	A (IP address)	IN (0x0001)	false
Nov 29, 2022 18:25:31.068085909 CET	8.8.8.8	192.168.2.6	0xa02a	No error (0)	www.y31jaihdb6zm87.buzz		154.209.6.241	A (IP address)	IN (0x0001)	false
Nov 29, 2022 18:25:50.808146954 CET	8.8.8.8	192.168.2.6	0xeb7d	No error (0)	www.marketmall.digital		162.213.255.142	A (IP address)	IN (0x0001)	false
Nov 29, 2022 18:26:01.772579908 CET	8.8.8.8	192.168.2.6	0xd179	No error (0)	www.canadianlocalbusiness.com		172.67.148.132	A (IP address)	IN (0x0001)	false
Nov 29, 2022 18:26:01.772579908 CET	8.8.8.8	192.168.2.6	0xd179	No error (0)	www.canadianlocalbusiness.com		104.21.29.63	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- www.ope-cctv.com
- www.dersameh.com
- www.darkchocolatebliss.com
- www.y31jaihdb6zm87.buzz
- www.marketmall.digital
- www.canadianlocalbusiness.com

Statistics

Behavior



System Behavior

Analysis Process: NHYGUnNN.exe PID: **5380**, Parent PID: **3452**

General

Target ID:	0
Start time:	18:24:01
Start date:	29/11/2022
Path:	C:\Users\user\Desktop\NHYGUnNN.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\NHYGUnNN.exe
Imagebase:	0x12a25d20000
File size:	275456 bytes
MD5 hash:	4F9C8432B57FA1AA875071DE547BA947
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	low

File Activities

Analysis Process: RegSvcs.exe PID: **5148**, Parent PID: **5380**

General

Target ID:	1
Start time:	18:24:03
Start date:	29/11/2022
Path:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\RegSvcs.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v4.0.30319\Regsvcs.exe
Imagebase:	0x830000
File size:	45152 bytes
MD5 hash:	2867A3817C9245F7CF518524DFD18F28
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000001.00000002.318189289.0000000000DB0000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000001.00000002.317923143.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000001.00000002.317923143.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000001.00000002.317923143.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000001.00000002.317923143.0000000000401000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	41DF9E	NtReadFile

Analysis Process: explorer.exe PID: **3452**, Parent PID: **5148**

General

Target ID:	2
Start time:	18:24:05
Start date:	29/11/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff647860000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000000.291033635.0000000013485000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 00000002.00000000.291033635.0000000013485000.00000040.00000001.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.291033635.0000000013485000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.291033635.0000000013485000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: NETSTAT.EXE PID: **4844**, Parent PID: **3452**

General

Target ID:	10
Start time:	18:24:38
Start date:	29/11/2022
Path:	C:\Windows\SysWOW64\NETSTAT.EXE
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\NETSTAT.EXE
Imagebase:	0x1010000
File size:	32768 bytes
MD5 hash:	4E20FF629119A809BC0E7EE2D18A7FDB
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.497449022.0000000000FE0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000A.00000002.497449022.0000000000FE0000.00000040.10000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.497449022.0000000000FE0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.497449022.0000000000FE0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.497017430.0000000000BC0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000A.00000002.497017430.0000000000BC0000.00000040.80000000.00040000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.497017430.0000000000BC0000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.497017430.0000000000BC0000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000002.497846833.0000000003060000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Formbook_1112e116, Description: unknown, Source: 0000000A.00000002.497846833.0000000003060000.00000004.00000800.00020000.00000000.sdmp, Author: unknown • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000002.497846833.0000000003060000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000002.497846833.0000000003060000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Regsvcs.exe	access denied	1	BDC897	NtDeleteFile
C:\Users\user\AppData\Local\Temp\1--Lt08NN	object name not found	1	BDC897	NtDeleteFile
C:\Users\user\AppData\Local\Temp\1--Lt08NN	sharing violation	1	BDC897	NtDeleteFile
C:\Users\user\AppData\Local\Temp\1--Lt08NN	sharing violation	1	BDC897	NtDeleteFile

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1622408	success or wait	1	BDC867	NtReadFile

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Disassembly

No disassembly