ID: 510425
Sample Name:
NvkGETsSDb.exe
Cookbook: default.jbs
Time: 19:35:13
Date: 27/10/2021
Version: 33.0.0 White Diamond

Table of Contents

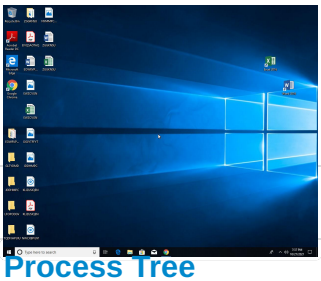
Windows Analysis Report NvkGETsSDb.exe

Overview

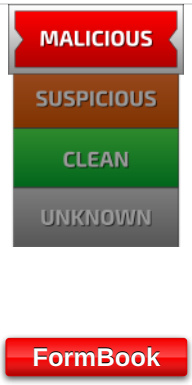
General Information

Sample Name:	NvkGETsSDb.exe
Analysis ID:	510425
MD5:	e17b528f9c19265.
SHA1:	f4dfc93942ed0c0..
SHA256:	83708560ecc442..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



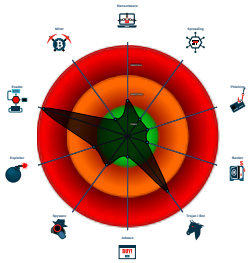
FormBook

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Yara detected AntiVM3
- System process connects to networ…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Tries to detect sandboxes and other…
- Modifies the prolog of user mode fun…
- Self deletion via cmd delete

Classification



Process Tree

- **System is w10x64**
- NvkGETsSDb.exe (PID: 2500 cmdline: 'C:\Users\user\Desktop\NvkGETsSDb.exe' MD5: E17B528F9C192653DC9777BD46E48D82)
  - NvkGETsSDb.exe (PID: 3092 cmdline: C:\Users\user\Desktop\NvkGETsSDb.exe MD5: E17B528F9C192653DC9777BD46E48D82)
    - explorer.exe (PID: 3472 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - ipconfig.exe (PID: 6236 cmdline: C:\Windows\SysWOW64\ipconfig.exe MD5: B0C7423D02A007461C850CD0DFE09318)
        - cmd.exe (PID: 6268 cmdline: /c del 'C:\Users\user\Desktop\NvkGETsSDb.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 6344 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.agentpathleurre.space/s18y/"
  ],
  "decoy": [
    "jokes-online.com",
    "dzzdjn.com",
    "lizzieerhardtebnaryepptts.com",
    "interfacehand.xyz",
    "sale-m.site",
    "block-facebook.com",
    "dicasdamadrinha.com",
    "maythewind.com",
    "hasari.net",
    "omnists.com",
    "thevalley-eg.com",
    "rdfj.xyz",
    "szhfcy.com",
    "alkalineage.club",
    "fdf.xyz",
    "absorplus.com",
    "poldolongo.com",
    "badassshirts.club",
    "ferienwohnungenmv.com",
    "bilboondokoak.com",
    "ambrosiaaudio.com",
    "lifeneurologyclub.com",
    "femboys.world",
    "blehmails.com",
    "gametimebg.com",
    "duytienauto.net",
    "owerful.com",
    "amedicalsupplyco.com",
    "americonnlogistics.com",
    "ateamautoglassga.com",
    "clickstool.com",
    "fzdzcnj.com",
    "txtgo.xyz",
    "izassist.com",
    "3bangzhu.com",
    "myesstyle.com",
    "aek181129aek.xyz",
    "daoxinghumaotest.com",
    "jxdg.xyz",
    "restorationculturecon.com",
    "thenaturalnutrient.com",
    "sportsandgames.info",
    "spiderwebinar.net",
    "erqgseidx.com",
    "donutmastermind.com",
    "aidatislemleri-govtr.com",
    "weetsist.com",
    "sunsetschoolportaits.com",
    "exodusguarant.tech",
    "gsnbls.top",
    "huangdashi33.xyz",
    "amazonretoure.net",
    "greathomeinlakewood.com",
    "lenovoidc.com",
    "qiuhenglawfirm.com",
    "surveyorslimited.com",
    "carterscts.com",
    "helmosy.online",
    "bakersfieldlaughingstock.com",
    "as-payjrku.icu",
    "mr-exclusive.com",
    "givepy.info",
    "ifvita.com",
    "obesocarpinteria.online"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.315401814.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000002.00000002.315401814.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000002.00000002.315401814.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$sqlite3step: 68 34 1C 7B E1 • 0x1895c:$sqlite3step: 68 34 1C 7B E1 • 0x18878:$sqlite3text: 68 38 2A 90 C5 • 0x1899d:$sqlite3text: 68 38 2A 90 C5 • 0x1888b:$sqlite3blob: 68 53 D8 7F 8C • 0x189b3:$sqlite3blob: 68 53 D8 7F 8C
00000010.00000002.516991020.00000000028C0000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000010.00000002.516991020.00000000028C0000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 30 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.2.NvkGETsSDb.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.NvkGETsSDb.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
2.2.NvkGETsSDb.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$sqlite3step: 68 34 1C 7B E1 • 0x1895c:$sqlite3step: 68 34 1C 7B E1 • 0x18878:$sqlite3text: 68 38 2A 90 C5 • 0x1899d:$sqlite3text: 68 38 2A 90 C5 • 0x1888b:$sqlite3blob: 68 53 D8 7F 8C • 0x189b3:$sqlite3blob: 68 53 D8 7F 8C
2.2.NvkGETsSDb.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
2.2.NvkGETsSDb.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8b08:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x148b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x143a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x149b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14b2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x979a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1361c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa493:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1ab27:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1bb2a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 23 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Networking:

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

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

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

Persistence and Installation Behavior:

Uses ipconfig to lookup or modify the Windows network settings

Hooking and other Techniques for Hiding and Protection:

Modifies the prolog of user mode functions (user mode inline hooks)

Self deletion via cmd delete

Malware Analysis System Evasion:

Yara detected AntiVM3

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

Tries to detect virtualization through RDTSC time measurements

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

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

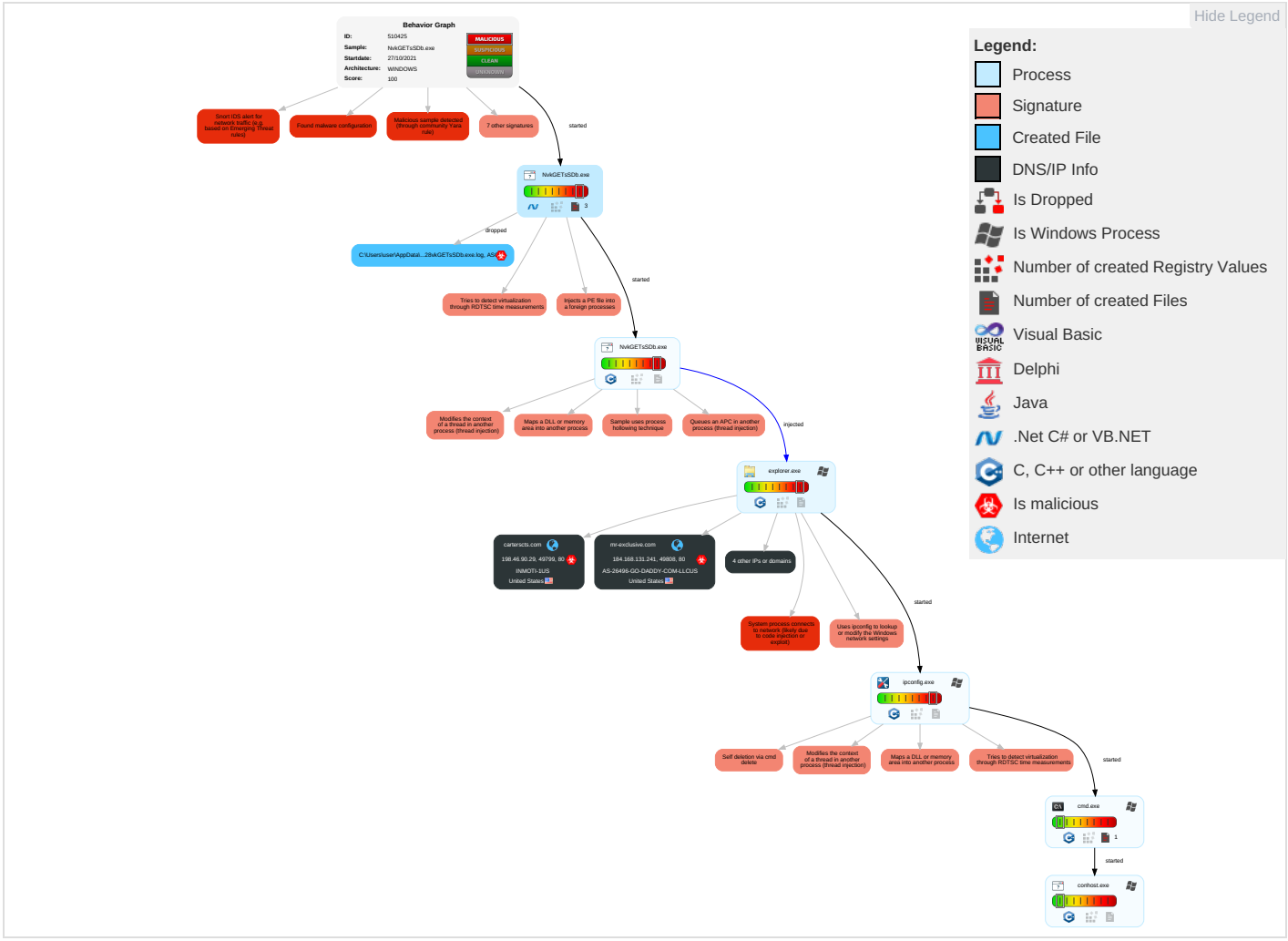
Remote Access Functionality:

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
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 6 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 2 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop Insecure Network Communica
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 3	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 3	Exploit SS7 Track Devic Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 3 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 3	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 6 1 2	LSA Secrets	System Network Configuration Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Information Discovery 1 1 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poir
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade Insecure Protocols
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	File Deletion 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellu Base Statio

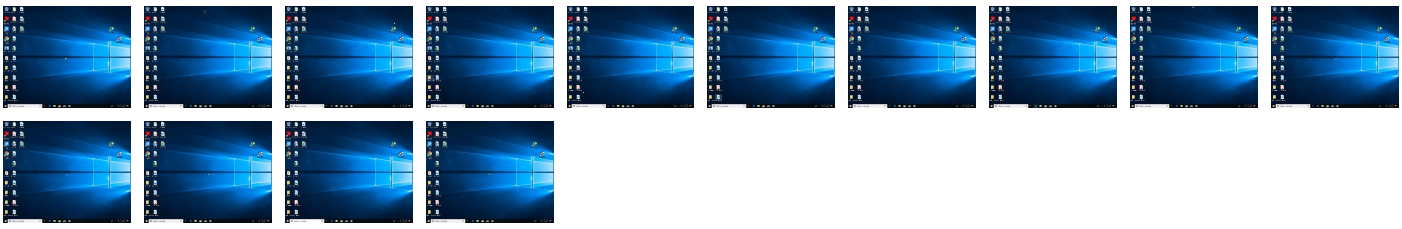
Behavior Graph



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
NvkGETsSDb.exe	15%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.NvkGETsSDb.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.0.NvkGETsSDb.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.0.NvkGETsSDb.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
2.0.NvkGETsSDb.exe.400000.4.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.mr-exclusive.com/s18y/?eXwdIN10=Pa4nojFHNdgR9BnFd7o8aKQocYkXN/E4z79GVA9AtWALsHU61u0W5ib2TTz7NOJsFj7K&3fU4r=D2MpiZv	0%	Avira URL Cloud	safe	
http://www.carterscts.com/s18y/?eXwdIN10=4Ci6vsYQWs8id7GhdYTjZRJculBFGSFOZGvHXdH6NGfnjVfmX1rRX92W0hUQgL+8jwmH&3fU4r=D2MpiZv	0%	Avira URL Cloud	safe	
www.agentpathleurre.space/s18y/	0%	Avira URL Cloud	safe	
http://www.collada.org/2005/11/COLLADASchema9Done	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mr-exclusive.com	184.168.131.241	true	true		unknown
carterscts.com	198.46.90.29	true	true		unknown
www.lenovoidc.com	unknown	unknown	true		unknown
www.mr-exclusive.com	unknown	unknown	true		unknown
www.carterscts.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.mr-exclusive.com/s18y/?eXwdIN10=Pa4nojFHNdgR9BnFd7o8aKQocYkXN/E4z79GVA9AtWALsHU61u0W5ib2TTz7NOJsFj7K&3fU4r=D2MpiZv	true	• Avira URL Cloud: safe	unknown
http://www.carterscts.com/s18y/?eXwdIN10=4Ci6vsYQWs8id7GhdYTjZRJculBFGSFOZGvHXdH6NGfnjVfmX1rRX92W0hUQgL+8jwmH&3fU4r=D2MpiZv	true	• Avira URL Cloud: safe	unknown
www.agentpathleurre.space/s18y/	true	• Avira URL Cloud: safe	low

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
184.168.131.241	mr-exclusive.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true
198.46.90.29	carterscts.com	United States		54641	INMOTI-1US	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	510425
Start date:	27.10.2021
Start time:	19:35:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 3s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	NvkGETsSDb.exe
Cookbook file name:	default.jbs

Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	26
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.evad.winEXE@7/1@3/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 56.1% (good quality ratio 52.5%) • Quality average: 72.6% • Quality standard deviation: 30.1%
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

Simulations

Behavior and APIs

Time	Type	Description
19:36:14	API Interceptor	1x Sleep call for process: NvkGETsSDb.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
184.168.131.241	AWB#708900271021,PDF.exe	Get hash	malicious	Browse	• www.boney4districtb.com/r2j4/?StNH=9r_X3ZFHtftXupP&UBj4d=LFAiXYmTCBeaiZVkmnENbyVkuv8MJYAEPmtNc8t5EMgtzVldrMk49PHJW+dEvs3sanQW
	_Payment Advise.doc	Get hash	malicious	Browse	• www.mckinneysfinest.com/k8u7/?gxo8Eb=stx06pLxG2uhHt&sRGLI=1bPiF0ymqUrevqPd4b9E+KBaEtHs6PvOSmp56O1TuFjTMCdLZCrwRu1kAfrIR9Q7KIC8fA==

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO03214890.exe	Get hash	malicious	Browse	• www.soulshine.today/rgv6/?l6bdp0F=WOgTlg0CsEDUEOPolUd3k4KrX1bkYNUSVHt3Voxul06FzSdhm4lRQ5zn06mtwv+q2ZPBPfPQRA==&uN90=Wv0xlDNhhL
	8A1A2kc6oG.exe	Get hash	malicious	Browse	• www.voteyatooma.com/fkt8/?tZg=GtK4AtM022&CrX=ofUS4x3nAebXS2gtlT7bCxF16YnqpMlcDxownTpTVGIuSS8RbFZpuU5Akchb7PYnpNHErMlOzQ==
	Dekont_20211910_Halbank.exe	Get hash	malicious	Browse	• www.royzoom.com/gab8/?NT3PVbt=ZIawR5WfQNh0tP8w4y/ZuRppdufcVyCLEE56Lf8Rl/+sRJFnSkjsl6Qg2BPlTh8S00GI&Z0DX=Ozr8Ub4PIpQTxx
	aOThyqtdnKntCHP.exe	Get hash	malicious	Browse	• www.dunedinhyperlocal.com/u4an/?8p=QzQ5ef7S9XxyRV9FzLuAV3Nyo+3E4vM7eDSIUEhkPsMNsjJnUVEtYk+AmU1/T2lyDvv2d6Or5g==&m2Mpy=4hoLs8sX9d
	EvxSSUyNfJ.exe	Get hash	malicious	Browse	• www.crgcatherine.com/ed9s/?r2Jt_Nb=lkqAHEYv8Zhi7fgrvevu0+VWnA2QaRYdkwf/BKiZqTsQIANP75p6RpBVhevD4imC+4UX&2d=B2JdPjgh
	triage_dropped_file.exe	Get hash	malicious	Browse	• www.hillcresthomegroup.com/fqiq/?oJE=e8IUz+kwT1xqAO5a7dDPCxDZEZgLUw6RtmSKZk1zt2cQgLHUKUCbR0r9TDFhVb4eVEB6&u6KLb=Wp6xUr6h5

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	FzvFtf2XXK.exe	Get hash	malicious	Browse	• www.sunshinefamilysupport.com/b2c0/?7nwTnlOP=OHhY/R7Pi7l9OOhmJJK1Xj4hyqShMd99eYdWuTQY8l2Zovp1jXuaaoSrFJSTx4r5Bl+0&yHY8=LDH0Pf4X32D4h
	REQ20211028624480320 73.exe	Get hash	malicious	Browse	• www.royzoom.com/gab8/?s48Dlz=ZIawR5WfQNh0tP8w4y/ZuRppdufcVyCLEE56Lf8Rl/+sRJFnSkjsl6Qg2Cv1cAsqqRvP&u2=3fo4s8O0
	jjBv8SpZXm.exe	Get hash	malicious	Browse	• www.avachaturbate.com/merc/?o67T=4TgGASrpG4NKs6fUTtEcg+jBUQzM4DK+NTe2Wif+5fnmqwYoqXUOY0xuCl11FpRRnfjB&V8=VfRPdzpxb4pXml
	PURCHASE ORDER.doc	Get hash	malicious	Browse	• www.4346emerald.com/ed9s/?3f8=4FJV/9v6vDki4c21a5N90qkBdO4moNaH31u52SaxnSM3kgwCG5H+93GFyEYXEd492VfcKw==&9rKXL=T2JtB4vhllhha2
	Scan_202005.exe	Get hash	malicious	Browse	• www.uperionorthamerica.com/pfrp/?PX=4hD0VrfPzva&0HQ=XNgnKB9mKucGSZ8xF6uYha143jCut8oDi/mwkVenOaidzNCLjJufmPtr+aig6m5szVrzgj/7tA==
	Lv9eznkydx.exe	Get hash	malicious	Browse	• cloudkiss.net/index.php
	PO.exe	Get hash	malicious	Browse	• www.annotake.com/odse/?yV4DLTZ=DNEOORvJOpllxzl1Ce3DiLTsHhO7HE2vhB8+VMP16POjOpH2kdX3F5WxV/E/FzaUR6ROSWAzkw==&2d=AdrxUv8x

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Contract 20123.xlsx	Get hash	malicious	Browse	• www.foxyladynails.com/scb0/?9ra=CGto01zpETy1wfVoDXG+ZhJsaDV0+AaThApfSytOfvXIKJYrj/MmsJyuEoGCVCFDrTIVqw==&e8whC=zxoxTPdPU
	OXkB3xMeAr.exe	Get hash	malicious	Browse	• www.thursdaynightthriller.com/nk6l/?WDKHz8DP=AN7S2hjzcv8Gc4uLzN77TguLKoDYI21oeP+/6IjuWfZR4q7OI4m7rj64+wbHO5IIW+km&3f3H7J=F48x3ps
	devis.exe	Get hash	malicious	Browse	• www.mississippiscorecard.com/s3dy/?n6Al5z7=atIJKMh/Nf1NytC3eVMa1G/pJNMMD998UDoVneC8L7BXz/kf7GlY/rbrOCQYh/uS11gd&4h=8phDpf6PHDn
	2WK7SGkGVZ.exe	Get hash	malicious	Browse	• www.sunshinefamilysupport.com/b2c0/?7nlpd=OHhY/R7Pi7l9OOhmJJK1Xj4hyqShMd99eYdWuTQY8l2Zovp1jXuaaoSrFJSTx4r5BI+0&_xllR=SL0l7NVxUdmdjv
	5v6RwaCMPI.exe	Get hash	malicious	Browse	• www.groupninemed.com/noha/?T8PhURl=lvCRxprl/4VR5AH+cYxnjQze0QPiFV0jDZjzPWMdHMoixCNRtg260CKerfKoVKuB1UPz&n0D0K=xDKPRVRherJ0

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-26496-GO-DADDY-COM-LLCUS	AWB#708900271021,PDF.exe	Get hash	malicious	Browse	• 184.168.131.241
	2jFfKOEefN.exe	Get hash	malicious	Browse	• 72.167.241.180
	jGK42jrs2j.exe	Get hash	malicious	Browse	• 72.167.78.83
	PAYMENT INSTRUCTIONS COPY.exe	Get hash	malicious	Browse	• 182.50.132.92
	PMYIIWQ10054.pdf.vbs	Get hash	malicious	Browse	• 107.180.48.126
	Order of CB-15GL PO530_pdf.exe	Get hash	malicious	Browse	• 72.167.241.180
	Lebanon Khayat Trading Company.exe	Get hash	malicious	Browse	• 182.50.132.92
	DRAFT CONTRACT 0000499000-1100928777-pdf.exe	Get hash	malicious	Browse	• 173.201.185.67

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Swift copy.exe	Get hash	malicious	Browse	• 182.50.132.92
	ATGSVCN64670.pdf.vbs	Get hash	malicious	Browse	• 107.180.48.126
	ACUEAQN44306.pdf.vbs	Get hash	malicious	Browse	• 107.180.48.126
	BYWDAMU4436.vbs	Get hash	malicious	Browse	• 107.180.48.126
	F9ObnUc4ol.exe	Get hash	malicious	Browse	• 50.62.168.3
	_Payment Advise.doc	Get hash	malicious	Browse	• 184.168.131.241
	Q-700004637 1004913.exe	Get hash	malicious	Browse	• 107.180.56.180
	SHIPPING DOCUMENT.exe	Get hash	malicious	Browse	• 173.201.181.36
	uu5009125.exe	Get hash	malicious	Browse	• 208.109.9.44
	ATT12068.html	Get hash	malicious	Browse	• 107.180.27.238
	REMITTANCE-54324.exe	Get hash	malicious	Browse	• 107.180.56.180
	ABONOF2201.exe	Get hash	malicious	Browse	• 107.180.56.180
INMOTI-1US	iAcd5qX0Zb.exe	Get hash	malicious	Browse	• 198.46.90.29
	Details OF Payment.exe	Get hash	malicious	Browse	• 104.193.142.174
	aD74smrP3Q.exe	Get hash	malicious	Browse	• 198.46.90.29
	70654 SSEBACT.exe	Get hash	malicious	Browse	• 104.193.142.174
	987421.exe	Get hash	malicious	Browse	• 173.231.223.186
	70654 SSEBACT.exe	Get hash	malicious	Browse	• 104.193.142.174
	70654 SSEBACT.exe	Get hash	malicious	Browse	• 104.193.142.174
	BANKING INFORMATION.exe	Get hash	malicious	Browse	• 104.193.142.174
	COSCOSH SHANGHAI SHIP MANAGEMENT CO LTD.exe	Get hash	malicious	Browse	• 104.193.142.174
	Angebot Anfrage Maschinensucher YOM.exe	Get hash	malicious	Browse	• 173.205.124.65
	COSCOSH SHANGHAI SHIP MANAGEMENT CO LTD.exe	Get hash	malicious	Browse	• 104.193.142.174
	SecuriteInfo.com.__vbaHresultCheckObj.9268.exe	Get hash	malicious	Browse	• 104.247.76.214
	TRANSFER REQUEST FORM.exe	Get hash	malicious	Browse	• 104.193.142.174
	TRANSFER REQUEST FORM.exe	Get hash	malicious	Browse	• 104.193.142.174
	Equiniti.AP Summary.3405.html	Get hash	malicious	Browse	• 173.231.220.228
	ugsuHxq7Ey.exe	Get hash	malicious	Browse	• 209.182.206.86
	waff.xls	Get hash	malicious	Browse	• 173.231.245.32
	QOJ48GT1(09-17-2021).vbs	Get hash	malicious	Browse	• 199.250.202.192
	QJfoKgzkov.exe	Get hash	malicious	Browse	• 199.250.199.190
	orderDetails.xlsx	Get hash	malicious	Browse	• 199.250.194.93

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\Desktop\NvkGETsSDb.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\NvkGETsSDb.exe.log	
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	6.723899910809643
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% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	NvkGETsSDb.exe
File size:	533504
MD5:	e17b528f9c192653dc9777bd46e48d82
SHA1:	f4dfc93942ed0c091340057f1164b1e1e6f4a148
SHA256:	83708560ecc442b5b6dadbdf5af39ae4f1e843664c932a9de3eff1e38bf6d4a5
SHA512:	d041efc3a98c8fc690841669f3e9722c43bbee4c6eac7191056b7dff5b8c27d938bf9f7de3409f27239cadf46c70696c12a9c98e86f772339e902b295060ae29
SSDEEP:	12288:ouQwyxAyhGdds0/v8mEMRp9LviDdzs/4cuKr:LyAL/vVRfl
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...qzya.....0.....:8... ...@....@.. .....@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x48383a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61797A71 [Wed Oct 27 16:12:33 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0

General

File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x81840	0x81a00	False	0.692274514826	data	6.73403579099	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x84000	0x5d4	0x600	False	0.43359375	data	4.18320178133	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x86000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/27/21-19:37:46.597276	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49808	80	192.168.2.5	184.168.131.241
10/27/21-19:37:46.597276	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49808	80	192.168.2.5	184.168.131.241
10/27/21-19:37:46.597276	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49808	80	192.168.2.5	184.168.131.241

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 27, 2021 19:37:27.807337046 CEST	192.168.2.5	8.8.8.8	0x95b3	Standard query (0)	www.carterscts.com	A (IP address)	IN (0x0001)
Oct 27, 2021 19:37:46.396549940 CEST	192.168.2.5	8.8.8.8	0x312d	Standard query (0)	www.mr-exclusive.com	A (IP address)	IN (0x0001)
Oct 27, 2021 19:38:07.052898884 CEST	192.168.2.5	8.8.8.8	0xbee1	Standard query (0)	www.lenovoidc.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 27, 2021 19:37:27.974387884 CEST	8.8.8.8	192.168.2.5	0x95b3	No error (0)	www.carterscts.com	carterscts.com		CNAME (Canonical name)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 27, 2021 19:37:27.974387884 CEST	8.8.8.8	192.168.2.5	0x95b3	No error (0)	carterscts.com		198.46.90.29	A (IP address)	IN (0x0001)
Oct 27, 2021 19:37:46.432111979 CEST	8.8.8.8	192.168.2.5	0x312d	No error (0)	www.mr-exclusive.com	mr-exclusive.com		CNAME (Canonical name)	IN (0x0001)
Oct 27, 2021 19:37:46.432111979 CEST	8.8.8.8	192.168.2.5	0x312d	No error (0)	mr-exclusive.com		184.168.131.241	A (IP address)	IN (0x0001)
Oct 27, 2021 19:38:07.451025963 CEST	8.8.8.8	192.168.2.5	0xbee1	Name error (3)	www.lenovoidc.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.carterscts.com
- www.mr-exclusive.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.5	49799	198.46.90.29	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 27, 2021 19:37:28.090456009 CEST	3714	OUT	GET /s18y/?eXwdIN10=4Ci6vsYQWs8id7GhdYTjZRJculBFGSFOZGvHXdH6NGfnjVfmX1rRX92W0hUQgL+8jwmH&3fU4r=D2MpiZv HTTP/1.1 Host: www.carterscts.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Oct 27, 2021 19:37:28.198955059 CEST	3714	IN	HTTP/1.1 404 Not Found Server: nginx/1.21.3 Date: Wed, 27 Oct 2021 17:37:28 GMT Content-Type: text/html; charset=iso-8859-1 Content-Length: 236 Connection: close Vary: Accept-Encoding Data Raw: 3c 68 74 6d 6c 3e 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 45 72 72 6f 72 20 34 30 34 20 2d 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 74 69 74 6c 65 3e 3c 68 65 61 64 3e 3c 62 6f 64 79 3e 3c 68 31 3e 45 72 72 6f 72 20 34 30 34 20 2d 20 4e 6f 74 20 46 6f 75 6e 64 3c 2f 68 31 3e 3c 70 3e 54 68 65 20 64 6f 63 75 6d 65 6e 74 20 79 6f 75 20 61 72 65 20 6c 6f 6f 6b 69 6e 67 20 66 6f 72 20 6d 61 79 20 68 61 76 65 20 62 65 65 6e 20 72 65 6d 6f 76 65 64 20 6f 72 20 72 65 2d 6e 61 6d 65 64 2e 20 50 6c 65 61 73 65 20 63 6f 6e 74 61 63 74 20 74 68 65 20 77 65 62 20 73 69 74 65 20 6f 77 6e 65 72 20 66 6f 72 20 66 75 72 74 68 65 72 20 61 73 73 69 73 74 61 6e 63 65 2e 3c 2f 70 3e 3c 2f 62 6f 64 79 3e 3c 2f 68 74 6d 6c 3e Data Ascii: <html><head><title>Error 404 - Not Found</title><head><body> Error 404 - Not Found The document you are looking for may have been removed or re-named. Please contact the web site owner for further assistance. </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.5	49808	184.168.131.241	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 27, 2021 19:37:46.597275972 CEST	3980	OUT	GET /s18y/?eXwdIN10=Pa4nojFHNdgR9BnFd7o8aKQocYkXN/E4z79GVA9AtWALsHU61u0W5ib2TTz7NOJsFj7K&3fU4r=D2MpiZv HTTP/1.1 Host: www.mr-exclusive.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Oct 27, 2021 19:37:46.781284094 CEST	3981	IN	HTTP/1.1 302 Found Server: nginx/1.20.1 Date: Wed, 27 Oct 2021 17:37:46 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Location: https://www.afternic.com/forsale/mr-exclusive.com?utm_source=TDFS&utm_medium=sn_affiliate_click&utm_campaign=TDFS_GoDaddy_DLS&traffic_type=TDFS&traffic_id=GoDaddy_DLS Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Code Manipulations

User Modules

Hook Summary

Function Name	Hook Type	Active in Processes
PeekMessageA	INLINE	explorer.exe
PeekMessageW	INLINE	explorer.exe
GetMessageW	INLINE	explorer.exe
GetMessageA	INLINE	explorer.exe

Processes

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: NvkGETsSDb.exe PID: 2500 Parent PID: 6096

General

Start time:	19:36:12
Start date:	27/10/2021
Path:	C:\Users\user\Desktop\NvkGETsSDb.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\NvkGETsSDb.exe'
Imagebase:	0x180000
File size:	533504 bytes
MD5 hash:	E17B528F9C192653DC9777BD46E48D82
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.256996800.00000000028A1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.257370628.00000000038A9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.257370628.00000000038A9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.257370628.00000000038A9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: NvkGETsSDb.exe PID: 3092 Parent PID: 2500

General

Start time:	19:36:14
Start date:	27/10/2021
Path:	C:\Users\user\Desktop\NvkGETsSDb.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\NvkGETsSDb.exe
Imagebase:	0x9e0000
File size:	533504 bytes
MD5 hash:	E17B528F9C192653DC9777BD46E48D82
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.315401814.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.315401814.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.315401814.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000000.253147010.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.253147010.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.253147010.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.315756855.0000000000FD0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.315756855.0000000000FD0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.315756855.0000000000FD0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000000.253638394.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000000.253638394.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000000.253638394.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000002.00000002.315792746.0000000001000000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000002.00000002.315792746.0000000001000000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000002.00000002.315792746.0000000001000000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3472 Parent PID: 3092

General

Start time:	19:36:17
Start date:	27/10/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff693d90000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.303659400.000000000F70F000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.303659400.000000000F70F000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.303659400.000000000F70F000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000000.288307054.000000000F70F000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000000.288307054.000000000F70F000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000000.288307054.000000000F70F000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: ipconfig.exe PID: 6236 Parent PID: 3472

General

Start time:	19:36:42
Start date:	27/10/2021
Path:	C:\Windows\SysWOW64\ipconfig.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\ipconfig.exe
Imagebase:	0x200000
File size:	29184 bytes
MD5 hash:	B0C7423D02A007461C850CD0DFE09318
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000002.516991020.00000000028C0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.516991020.00000000028C0000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.516991020.00000000028C0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000002.514736730.0000000000150000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.514736730.0000000000150000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.514736730.0000000000150000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000010.00000002.515839448.0000000002700000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000010.00000002.515839448.0000000002700000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000010.00000002.515839448.0000000002700000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 6268 Parent PID: 6236

General

Start time:	19:36:46
Start date:	27/10/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\NvkGETsSDb.exe'
Imagebase:	0x150000
File size:	232960 bytes
MD5 hash:	F3BDBE3BB6F734E357235F4D5898582D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 6344 Parent PID: 6268

General

Start time:	19:36:48
Start date:	27/10/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	C, C++ or other language
Reputation:	high

Disassembly

Code Analysis