ID: 458121
Sample Name: yw6At7QnNh
Cookbook: default.jbs
Time: 21:04:10
Date: 02/08/2021
Version: 33.0.0 White Diamond

Table of Contents

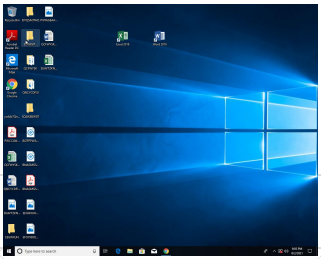
Windows Analysis Report yw6At7QnNh

Overview

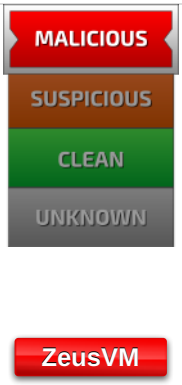
General Information

Sample Name:	yw6At7QnNh (renamed file extension from none to exe)
Analysis ID:	458121
MD5:	8ba293749c97cb..
SHA1:	6a7492a26d0a16..
SHA256:	e2075b32b9716d..
Tags:	exe uncategorized
Infos:	

Most interesting Screenshot:



Detection

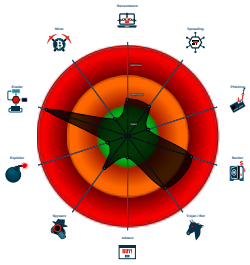


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Detected ZeusVM e-Banking Trojan
- Detected unpacking (changes PE se…
- Detected unpacking (overwrites its o…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Contain functionality to detect virtua…
- Contains VNC / remote desktop func…
- Contains functionality to inject code …
- Injects a PE file into a foreign proce…
- Machine Learning detection for samp…

Classification



Process Tree

- **System is w10x64**
- yw6At7QnNh.exe (PID: 3420 cmdline: 'C:\Users\user\Desktop\yw6At7QnNh.exe' MD5: 8BA293749C97CBF48F30F02C66D3406D)
  - yw6At7QnNh.exe (PID: 5952 cmdline: 'C:\Users\user\Desktop\yw6At7QnNh.exe' MD5: 8BA293749C97CBF48F30F02C66D3406D)
    - yw6At7QnNh.exe (PID: 1536 cmdline: 'C:\Users\user\Desktop\yw6At7QnNh.exe' MD5: 8BA293749C97CBF48F30F02C66D3406D)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

No yara matches

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus / Scanner detection for submitted sample

Antivirus detection for dropped file

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for sample

Compliance:

Detected unpacking (overwrites its own PE header)

E-Banking Fraud:

Detected ZeusVM e-Banking Trojan

Data Obfuscation:

Detected unpacking (changes PE section rights)

Detected unpacking (overwrites its own PE header)

Malware Analysis System Evasion:

Contain functionality to detect virtual machines

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

HIPS / PFW / Operating System Protection Evasion:

Contains functionality to inject code into remote processes

Injects a PE file into a foreign processes

Remote Access Functionality:

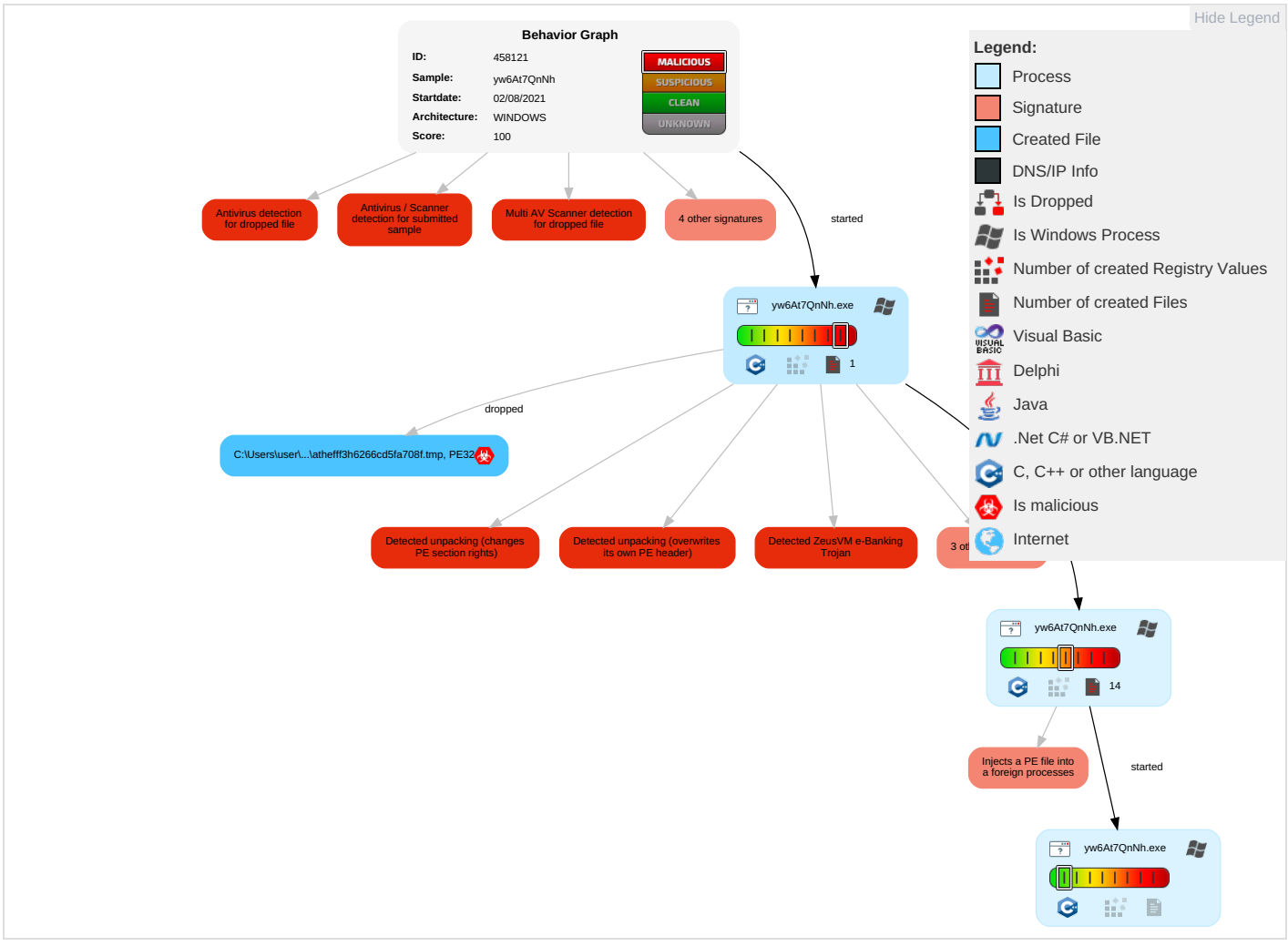
Contains VNC / remote desktop functionality (version string found)

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
Valid Accounts 1	Native API 1	Application Shimming 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1	Input Capture 1 1	System Time Discovery 2	Remote Desktop Protocol 1	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Eave Insec Netw Comr
Default Accounts	Scheduled Task/Job	Create Account 1	Valid Accounts 1	Obfuscated Files or Information 2	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Input Capture 1 1	Exfiltration Over Bluetooth	Encrypted Channel 2	Explc Redir Calls
Domain Accounts	At (Linux)	Valid Accounts 1	Access Token Manipulation 1 1	Install Root Certificate 1	Security Account Manager	File and Directory Discovery 1	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Remote Access Software 1	Explc Track Locat
Local Accounts	At (Windows)	Logon Script (Mac)	Process Injection 2 1 1	Software Packing 2 2	NTDS	System Information Discovery 4	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM (Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Network Share Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Mani Devic Comr
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Valid Accounts 1	Cached Domain Credentials	Security Software Discovery 3 1 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamn Denia Servi

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netw Effec
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1	DCSync	Virtualization/Sandbox Evasion 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogu Acce
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Access Token Manipulation 1 1	Proc Filesystem	Process Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Dowr Insec Proto
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 2 1 1	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogu Base

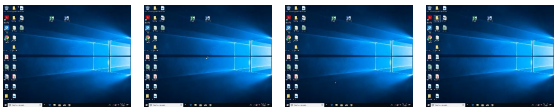
Behavior Graph



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
yw6At7QnNh.exe	81%	Virustotal		Browse
yw6At7QnNh.exe	61%	Metadefender		Browse
yw6At7QnNh.exe	92%	ReversingLabs	Win32.Trojan.Zeus	
yw6At7QnNh.exe	100%	Avira	TR/Dropper.Gen	
yw6At7QnNh.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\ athefff3h6266cd5fa708f.tmp	100%	Avira	TR/Agent.hjvc	
C:\Users\user\AppData\Local\Temp\ athefff3h6266cd5fa708f.tmp	5%	Virustotal		Browse
C:\Users\user\AppData\Local\Temp\ athefff3h6266cd5fa708f.tmp	53%	ReversingLabs	Win32.Trojan.Zeus	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.2.yw6At7QnNh.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1115251		Download File
1.2.yw6At7QnNh.exe.10000000.4.unpack	100%	Avira	TR/Agent.hjvc		Download File
3.2.yw6At7QnNh.exe.400000.0.unpack	100%	Avira	TR/Kazy.MK		Download File
3.1.yw6At7QnNh.exe.400000.0.unpack	100%	Avira	TR/Kazy.MK		Download File
1.2.yw6At7QnNh.exe.400000.0.unpack	100%	Avira	TR/Agent.hjvc		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458121
Start date:	02.08.2021
Start time:	21:04:10
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 52s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	yw6At7QnNh (renamed file extension from none to 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:	4
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.bank.troj.evad.winEXE@5/2@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 78.7% (good quality ratio 73.1%) • Quality average: 81.9% • Quality standard deviation: 29.7%
HCA Information:	• Successful, ratio: 72% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Stop behavior analysis, all processes terminated
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\ athefff3h6266cd5fa708f.tmp	
Process:	C:\Users\user\Desktop\yw6At7QnNh.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3072
Entropy (8bit):	2.4857544881426725
Encrypted:	false
SSDEEP:	12:etGSGsXpFmGEqIUfIjjObu0Nql2nLEu98DwhKQstDISMhTF0L/x8O6r:etGSB54qIUwnO/AHDw0jukx
MD5:	79460E0544E0DFFE86DD51BBA404A2D3
SHA1:	ED294E22259F0DE6BAC6DD7A701B19B3CDCDA900
SHA-256:	2AFD890122BBA0EED6193476D04266B4A5B7A4DE53CB514BD9EAF4243D9FC973
SHA-512:	E2511BCC767B9EA93D378AA5D3D81A08D39701E9920019C9125BED88CDE1DE02BFABD8A5242710E86B4D20A75A65607DE442772753AB47230DEA4A9BA36F563A
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Virustotal, Detection: 5%, Browse • Antivirus: ReversingLabs, Detection: 53%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....N.. ... ...!.. ...3... .I.+... .I.$... .Rich.. .....PE..L....t{N.....!..... ....P..... ..L.... ..(.....@..... .....text..... .. ..`.r data..... .....@..@.data.....0.....@....reloc..(....@.....@..B..... ....

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\414045e2d09286d5db2581e0d955d358_d06ed635-68f6-4e9a-955c-4899f5f57b9a	
Process:	C:\Users\user\Desktop\yw6At7QnNh.exe
File Type:	data

C:\Users\user\AppData\Roaming\Microsoft\Crypto\RSA\S-1-5-21-3853321935-2125563209-4053062332-1002\414045e2d09286d5db2581e0d955d358_d06ed635-68f6-4e9a-955c-4899f5f57b9a	
Category:	dropped
Size (bytes):	46
Entropy (8bit):	1.0424600748477153
Encrypted:	false
SSDEEP:	3:/lbON:u
MD5:	89CA7E02D8B79ED50986F098D5686EC9
SHA1:	A602E0D4398F00C827BFCF711066E67718CA1377
SHA-256:	30AC626CBD4A97DB480A0379F6D2540195F594C967B7087A26566E352F24C794
SHA-512:	C5F453E32C0297E51BE43F84A7E63302E7D1E471FADF8BB789C22A4D6E03712D26E2B039D6FBDBD9EBD35C4E93EC27F03684A7BBB67C4FADCCE9F6279417BDE
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.....user.

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.5870490062472085
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	yw6At7QnNh.exe
File size:	225792
MD5:	8ba293749c97cbf48f30f02c66d3406d
SHA1:	6a7492a26d0a16320daa2cb187232fc0053f4f5f
SHA256:	e2075b32b9716dc41ef667a74c1ae2c2841a5b9fd3046db0bdcd96c581778253
SHA512:	041e3f65fcb877eb19f5d63cb79d2eb6327ee4b06191a3a4202a736fb6215cd2b2b5c436c081b0165acf2b1b0341c8c551bbf166f8f46ce48fedd7d23ff74049
SSDEEP:	6144:ERAL6uxQIBpPnki+81Rnn1BgUUhgmfwgA3Bfdw+:z4MT+81RnnHLUhgrL3tdw+
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....Hs..Hs..Hs..Hs..Ks...o..Gs...l...s..*l..Os..Hs...s...l..[s...u..Is..RichHs.....PE..L...G.{N.....

File Icon

Icon Hash:	0000000000000000

Static PE Info

General

Entrypoint:	0x401c01
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	
Time Stamp:	0x4E7B9D47 [Thu Sep 22 20:40:39 2011 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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:	0f16db1e18559cc080852e2e8fd0038e

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xa21e	0xa400	False	0.593225990854	data	6.56845565551	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0xc000	0x1d40	0x1e00	False	0.365364583333	data	4.48192698758	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xe000	0x2a6c	0x1000	False	0.281005859375	data	3.38536461745	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x11000	0x29828	0x29a00	False	0.905352618243	data	7.80378630892	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: yw6At7QnNh.exe PID: 3420 Parent PID: 5572

General

Start time:	21:04:57
Start date:	02/08/2021
Path:	C:\Users\user\Desktop\yw6At7QnNh.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\yw6At7QnNh.exe'
Imagebase:	0x400000
File size:	225792 bytes
MD5 hash:	8BA293749C97CBF48F30F02C66D3406D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

Analysis Process: yw6At7QnNh.exe PID: 5952 Parent PID: 3420

General

Start time:	21:04:57
Start date:	02/08/2021
Path:	C:\Users\user\Desktop\yw6At7QnNh.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\yw6At7QnNh.exe'
Imagebase:	0x400000
File size:	225792 bytes
MD5 hash:	8BA293749C97CBF48F30F02C66D3406D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

Analysis Process: yw6At7QnNh.exe PID: 1536 Parent PID: 5952

General

Start time:	21:04:58
Start date:	02/08/2021
Path:	C:\Users\user\Desktop\yw6At7QnNh.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\yw6At7QnNh.exe'
Imagebase:	0x400000
File size:	225792 bytes
MD5 hash:	8BA293749C97CBF48F30F02C66D3406D
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Code Analysis