

JoeSandbox Cloud BASIC



ID: 483790

Sample Name:

wogZe27GBB.exe

Cookbook: default.jbs

Time: 14:00:47

Date: 15/09/2021

Version: 33.0.0 White Diamond

Table of Contents

Table of Contents	2
Windows Analysis Report wogZe27GBB.exe	4
Overview	4
General Information	4
Detection	4
Compliance	4
Signatures	4
Classification	4
Process Tree	4
Malware Configuration	4
Yara Overview	4
Sigma Overview	4
Jbx Signature Overview	5
AV Detection:	5
Compliance:	5
Persistence and Installation Behavior:	5
Malware Analysis System Evasion:	5
Anti Debugging:	5
HIPS / PFW / Operating System Protection Evasion:	5
Mitre Att&ck Matrix	5
Behavior Graph	6
Screenshots	6
Thumbnails	7
Antivirus, Machine Learning and Genetic Malware Detection	7
Initial Sample	7
Dropped Files	7
Unpacked PE Files	8
Domains	8
URLs	8
Domains and IPs	8
Contacted Domains	9
Contacted URLs	9
URLs from Memory and Binaries	9
Contacted IPs	9
Public	9
Private	9
General Information	10
Simulations	10
Behavior and APIs	10
Joe Sandbox View / Context	10
IPs	10
Domains	10
ASN	11
JA3 Fingerprints	11
Dropped Files	11
Created / dropped Files	11
Static File Info	13
General	13
File Icon	13
Static PE Info	13
General	13
Authenticode Signature	14
Entrypoint Preview	14
Rich Headers	14
Data Directories	14
Sections	14
Resources	14
Imports	14
Possible Origin	14
Network Behavior	14
Network Port Distribution	14
TCP Packets	14
UDP Packets	14
DNS Queries	14
DNS Answers	15
HTTP Request Dependency Graph	15
HTTP Packets	15
HTTPS Proxied Packets	19
Code Manipulations	22
Statistics	23
Behavior	23
System Behavior	23
Analysis Process: wogZe27GBB.exe PID: 7160 Parent PID: 6004	23
General	23

File Activities	23
File Created	23
File Deleted	23
File Written	23
File Read	23
Analysis Process: UniPrint.exe PID: 4260 Parent PID: 7160	23
General	23
File Activities	23
Analysis Process: UniPrint.exe PID: 5356 Parent PID: 5060	24
General	24
File Activities	24
File Read	24
Registry Activities	24
Key Created	24
Key Value Created	24
Analysis Process: svchost.exe PID: 4296 Parent PID: 568	24
General	24
File Activities	24
Analysis Process: svchost.exe PID: 5904 Parent PID: 568	24
General	24
Analysis Process: svchost.exe PID: 6852 Parent PID: 568	25
General	25
File Activities	25
Analysis Process: UniPrint.exe PID: 6952 Parent PID: 3424	25
General	25
File Activities	25
Analysis Process: UniPrint.exe PID: 7016 Parent PID: 5060	25
General	25
File Activities	26
Analysis Process: UniPrint.exe PID: 7080 Parent PID: 3424	26
General	26
File Activities	26
Analysis Process: svchost.exe PID: 6408 Parent PID: 568	26
General	26
File Activities	26
Analysis Process: UniPrint.exe PID: 6484 Parent PID: 5060	26
General	26
Analysis Process: svchost.exe PID: 5248 Parent PID: 568	27
General	27
Disassembly	27
Code Analysis	27

Windows Analysis Report wogZe27GBB.exe

Overview

General Information

Sample Name:

wogZe27GBB.exe

Analysis ID:

483790

MD5:

5efc68abd7fec41...

SHA1:

34b243a0b3e322...

SHA256:

0f655a8ac0d7fdc...

Tags:

exe

MappingOOO

signed

Infos:

Most interesting Screenshot:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Score: 72

Range: 0 - 100

Whitelist ed: false

Confiden ce: 100%

Compliance

HIGH

MODERATE

LOW

Score: 17

Range: 0 - 100

Signatures

Multi AV Scanner detection for subm...

Multi AV Scanner detection for dropp...

Tries to detect sandboxes and other...

Creates processes via WMI

DLL side loading technique detected

Contains functionality to detect slee...

Uses 32bit PE files

Queries the volume information (nam...

Antivirus or Machine Learning detec...

Contains functionality to check if a d...

Contains functionality to query locale...

May sleep (evasive loops) to hinder ...

Contains functionality to shutdown / ...

Uses code obfuscation techniques (...)

Classification

Process Tree

System is w10x64

wogZe27GBB.exe

(PID: 7160 cmdline: 'C:\Users\user\Desktop\wogZe27GBB.exe' MD5: 5EFC68ABD7FEC415E34980D95A06A66A)

UniPrint.exe

(PID: 4260 cmdline: 'C:\Users\user\AppData\Roaming\ViberPC\lcons\UniPrint.exe' f MD5: EBDBA07BFABCF24F5D79EF27247EA643)

UniPrint.exe

(PID: 5356 cmdline: C:\Users\user\AppData\Roaming\ViberPC\lcons\UniPrint.exe MD5: EBDBA07BFABCF24F5D79EF27247EA643)

svchost.exe

(PID: 4296 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)

svchost.exe

(PID: 5904 cmdline: c:\windows\syswow64\svchost.exe -k 'usbportsmanagergrp' -svcr 'uniprint.exe' -s USBManager MD5: FA6C268A5B5BDA067A901764D203D433)

svchost.exe

(PID: 6852 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)

UniPrint.exe

(PID: 6952 cmdline: 'C:\Users\user\AppData\Roaming\ViberPC\lcons\UniPrint.exe' f MD5: EBDBA07BFABCF24F5D79EF27247EA643)

UniPrint.exe

(PID: 7016 cmdline: C:\Users\user\AppData\Roaming\ViberPC\lcons\UniPrint.exe MD5: EBDBA07BFABCF24F5D79EF27247EA643)

UniPrint.exe

(PID: 7080 cmdline: 'C:\Users\user\AppData\Roaming\ViberPC\lcons\UniPrint.exe' f MD5: EBDBA07BFABCF24F5D79EF27247EA643)

svchost.exe

(PID: 6408 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)

UniPrint.exe

(PID: 6484 cmdline: C:\Users\user\AppData\Roaming\ViberPC\lcons\UniPrint.exe MD5: EBDBA07BFABCF24F5D79EF27247EA643)

svchost.exe

(PID: 5248 cmdline: C:\Windows\System32\svchost.exe -k netsvcs -p MD5: 32569E403279B3FD2EDB7EBD036273FA)

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:



Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Compliance:



Uses 32bit PE files

EXE planting / hijacking vulnerabilities found

DLL planting / hijacking vulnerabilities found

Uses secure TLS version for HTTPS connections

PE / OLE file has a valid certificate

Binary contains paths to debug symbols

Persistence and Installation Behavior:



Creates processes via WMI

Malware Analysis System Evasion:



Contains functionality to detect sleep reduction / modifications

Anti Debugging:



Tries to detect sandboxes and other dynamic analysis tools (window names)

HIPS / PFW / Operating System Protection Evasion:



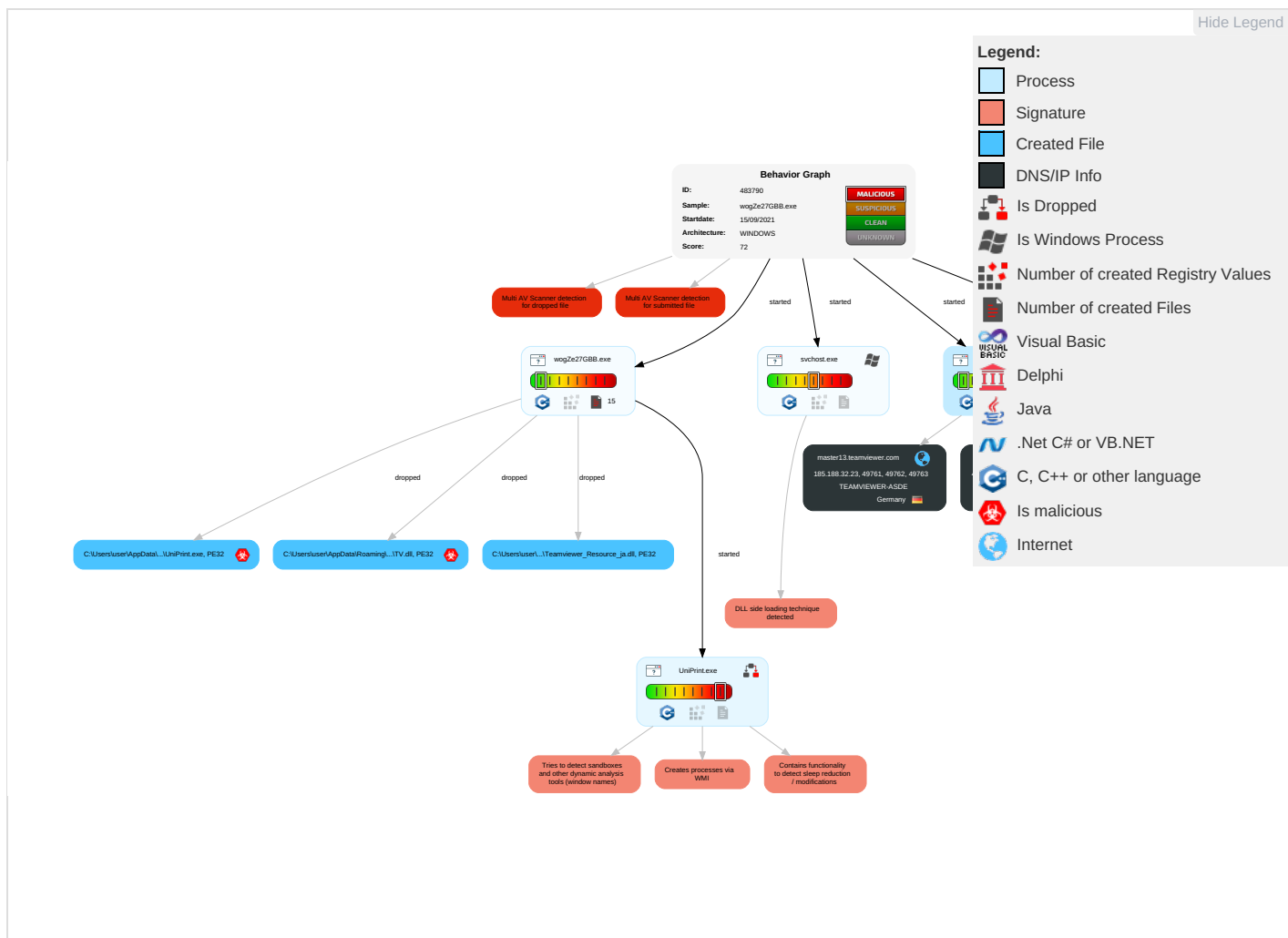
DLL side loading technique detected

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	C a
Valid Accounts 2	Windows Management Instrumentation 1 1	DLL Side-Loading 1 1	DLL Side-Loading 1 1	Deobfuscate/Decode Files or Information 1	Input Capture 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	I r T
Default Accounts	Native API 1	DLL Search Order Hijacking 2	DLL Search Order Hijacking 2	Obfuscated Files or Information 2	LSASS Memory	Account Discovery 1	Remote Desktop Protocol	Screen Capture 1	Exfiltration Over Bluetooth	E C
Domain Accounts	Service Execution 1 2	Create Account 1	Valid Accounts 2	Software Packing 1	Security Account Manager	File and Directory Discovery 3	SMB/Windows Admin Shares	Input Capture 1	Automated Exfiltration	N A L F
Local Accounts	At (Windows)	Valid Accounts 2	Access Token Manipulation 2 1	DLL Side-Loading 1 1	NTDS	System Information Discovery 2 6	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer	A L F

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	C a
Cloud Accounts	Cron	Windows Service 2 2	Windows Service 2 2	DLL Search Order Hijacking 2	LSA Secrets	Query Registry 1	SSH	Keylogging	Data Transfer Size Limits	F C
Replication Through Removable Media	Launchd	Registry Run Keys / Startup Folder 1	Process Injection 1 2	Masquerading 1	Cached Domain Credentials	Security Software Discovery 3 4 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	M C
External Remote Services	Scheduled Task	Startup Items	Registry Run Keys / Startup Folder 1	Valid Accounts 2	DCSync	Virtualization/Sandbox Evasion 1 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	C L
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 1 1	Proc Filesystem	Process Discovery 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	A L
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Access Token Manipulation 2 1	/etc/passwd and /etc/shadow	System Owner/User Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	V
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Process Injection 1 2	Network Sniffing	Remote System Discovery 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	F F
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	System Network Configuration Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	M

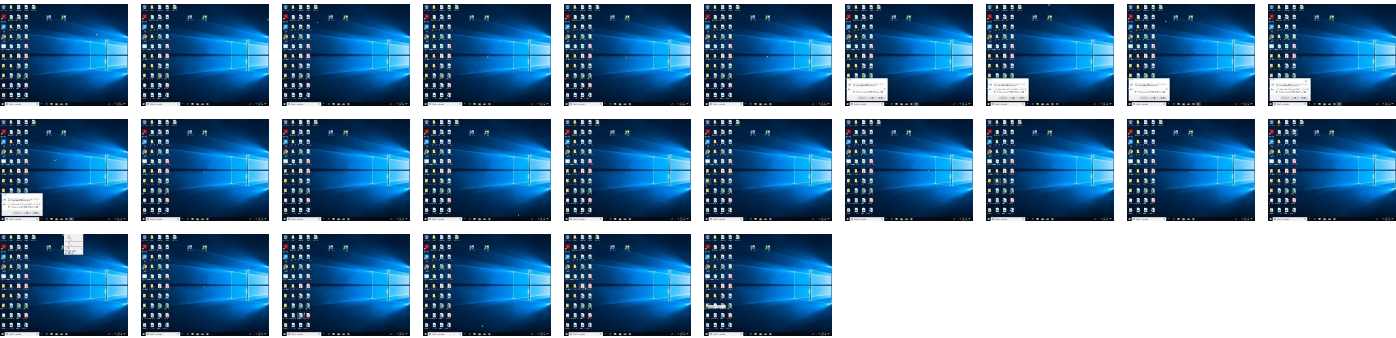
Behavior Graph



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
wogZe27GBB.exe	54%	Virusotal		Browse
wogZe27GBB.exe	9%	Metadefender		Browse
wogZe27GBB.exe	62%	ReversingLabs	Win32.Worm.AutoRun	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\ViberPC\icons\TV.dll	6%	Metadefender		Browse
C:\Users\user\AppData\Roaming\ViberPC\icons\TV.dll	51%	ReversingLabs	Win32.Trojan.Phonzy	
C:\Users\user\AppData\Roaming\ViberPC\icons\Teamviewer_Resource_ja.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\ViberPC\icons\Teamviewer_Resource_ja.dll	0%	ReversingLabs		
C:\Users\user\AppData\Roaming\ViberPC\icons\UniPrint.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Roaming\ViberPC\icons\UniPrint.exe	0%	ReversingLabs		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
0.2.wogZe27GBB.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen2		Download File
0.0.wogZe27GBB.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://widolapsed.info/apsed.info/B8C631A8/TTP-Out)LMEMX	0%	Avira URL Cloud	safe	
http://188.172.235.146/din.aspx?s=12251267&m=fast&client=DynGate&p=10000002 .	0%	Avira URL Cloud	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://188.172.235.146/din.aspx?s=12251267&m=fast&client=DynGate&p=100000023321935-2125563209-405306	0%	Avira URL Cloud	safe	
http://https://widolapsed.info/B8C631A8/i	0%	Avira URL Cloud	safe	
http://188.172.235.146/dout.aspx?s=12251267&p=10000002&client=DynGate:%	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSACodeSigningCA.crt0#	0%	URL Reputation	safe	
http://https://widolapsed.info/8C631A8/ELBASE.dll.mui01	0%	Avira URL Cloud	safe	
http://188.172.235.146/din.aspx?s=00000000&m=fast&client=DynGate&rnd=975066281&p=100000012	0%	Avira URL Cloud	safe	
http://188.172.235.146/	0%	Avira URL Cloud	safe	
http://188.172.235.146/EM	0%	Avira URL Cloud	safe	
http://188.172.235.146/dout.aspx?s=12251267&p=10000002&client=DynGateZ	0%	Avira URL Cloud	safe	
http://188.172.235.146/din.aspx?s=12251267&m=fast&client=DynGate&p=10000002	0%	Avira URL Cloud	safe	
http://https://widolapsed.info/B8C631A8/8	0%	Avira URL Cloud	safe	
http://188.172.235.146/dout.aspx?s=12251267&p=10000001&client=DynGate	0%	Avira URL Cloud	safe	
http://mastr13.teamv	0%	Avira URL Cloud	safe	
http://188.172.235.146/dout.aspx?s=12251267&p=10000001&client=DynGatepzm	0%	Avira URL Cloud	safe	
http://188.172.235.146/din.aspx?s=00000000&m=fast&client=DynGate&rnd=975066281&p=10000001	0%	Avira URL Cloud	safe	
http://188.172.235.146/dout.aspx?s=12251267&p=10000002&client=DynGate	0%	Avira URL Cloud	safe	
http://go.teamviewer.comn0	0%	Avira URL Cloud	safe	
http://https://displaycatalog.m(	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://188.172.235.146/dout.aspx?s=12251267&p=10000002&client=DynGatellow	0%	Avira URL Cloud	safe	
http://https://widolapsed.info/	0%	Avira URL Cloud	safe	
http://crl.verisign.corl0	0%	Avira URL Cloud	safe	
http://188.172.235.146/dout.aspx?s=12251267&p=10000002&client	0%	Avira URL Cloud	safe	
http://crl.ver(	0%	Avira URL Cloud	safe	
http://https://widolapsed.info/B8C631A8/B	0%	Avira URL Cloud	safe	
http://crl.sectigo.com/SectigoRSACodeSigningCA.crl0s	0%	URL Reputation	safe	
http://https://widolapsed.info/B8C631A8/(c~	0%	Avira URL Cloud	safe	
http://https://www.tiktok.com/legal/report/feedback	0%	URL Reputation	safe	
http://https://www.verisign.c	0%	Avira URL Cloud	safe	
http://https://widolapsed.info/B8C631A8/	0%	Avira URL Cloud	safe	
http://https://widolapsed.info/B8C631A8/ELBASE.dll.mui01	0%	Avira URL Cloud	safe	
http://https://widolapsed.info/apsed.info/qWave	0%	Avira URL Cloud	safe	
http://188.172.235.146/din.aspx?s=12251267&m=fast&client=DynGate&p=1000	0%	Avira URL Cloud	safe	
http://188.172.235.146/din.aspx?s=00000000&m=fast&client=DynGate&rnd=975066281&p=10000001K	0%	Avira URL Cloud	safe	
http://188.172.235.146/din.aspx?s=12251267&m=fast&client=DynGate&p=10000002Z	0%	Avira URL Cloud	safe	
http://crl.verisign.co	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
widolapsed.info	45.153.241.148	true	false		high
master13.teamviewer.com	185.188.32.23	true	false		high
ping3.dyngate.com	unknown	unknown	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://master13.teamviewer.com/din.aspx?s=00000000&client=DynGate&rnd=279943160&p=10000001	false		high
http://master13.teamviewer.com/dout.aspx?s=42047145&p=10000001&client=DynGate&data=FyQSbQCjHqkys5MkoZ6YmBgcGRsZGpmckySiHpgTJqChnpng8MrGzGjExHByxGZkbr5kcmpsaHBgbGRsTJqSiHpg8MrGzGjExHByxGZkbr5kcmpsaHBgbGRsTJ6meq7S3GZcYmJMrHpialgXGxwbkCip	false		high
http://master13.teamviewer.com/din.aspx?s=42047152&client=DynGate&p=10000002	false		high
http://master13.teamviewer.com/din.aspx?s=42047159&client=DynGate&p=10000002	false		high
http://master13.teamviewer.com/dout.aspx?s=42047152&p=10000001&client=DynGate&data=FyQS8QAjHqmyuig6sTY0saWyyJMkoZ6YmBgcGRsZGpmckySiHpmcmJgam5oanBMmpKlemDwysbMaMTEcHLEZmRuvrmRyamxocGBsZGxMrHpialgXGxwbkCipkyE0tzC5PJ6DAQAAAFIAACkpoJiAAgAACIAAAH7LQs0qhaWs0MJjaOW1RZp/s+y/lyn5XEbeVZg9sKBJ5zPw4VSW4zdwQ3dPOJPU35FNklfclLZEzewXzbzR9HNSPt0dvZIMVjxbsFa8mt4ylfhUHNJCrU/eCKZvcgbkPO7XECRgFWPWpqy/DxavH2VA1uMNeC6MgWi1tqYJIUpU	false		high
http://188.172.235.146/din.aspx?s=12251267&m=fast&client=DynGate&p=10000002	false	Avira URL Cloud: safe	unknown
http://master13.teamviewer.com/dout.aspx?s=42047224&p=10000001&client=DynGate&data=FyQS6wChTjSytzoeqisoqZMjHqY3s7S3EyOrnpgTI6umMrsyth6aGBgTJDSyMqe3NjS3Mqm6MLo6uZ6YyEYqQkignqqoemRMkoZ6YmBgcGRsZGpmckySiHpmcmJgam5oanBMLsrK4MLY0uzKemJMMMLczurCzsp61MJmmNLGytzmyqjy4Mp6YEyakoh6YPDKxsxoxMRwcsRmZG6+ZHJqbGhwYGxkbEyc3p7Mgsbo0uzKlsrK4MLY0uzKemBMpOrc6NLaynpqTKbq4ODE5OjKylzKwujq5MrmemJMqlagnqqoemBMrHpialgXGxwbkCip	false		high
http://master13.teamviewer.com/dout.aspx?s=42047159&p=10000001&client=DynGate&data=FyQS9ACjHqmyuim0s7cwujq5MqWyyJMkoZ6YmBgcGRsZGpmckySiHpmcmJgam5oanBMmpKlemDwysbMaMTEcHLEZmRuvrmRyamxocGBsZGxMrHpialgXGxwbkCipkyE0tzC5PJ6DAQAAABIAACkpoJiAAgAACIAAABKJHDw2LgVxSDgQRZJcruSvmCif9Gt2TW3hKr1gLfUfE+41DTTElJH9R8iP3LoBGOJ+mt3JU9XCLVeH0PEl9syAw5y9+liHYCQSiHVEX/VS+caNKAiNEKBpchoIJAACiCwW843p+TOKZHDf08qX87SA1CKgBTr4AFtosrqQ/gO/pU	false		high
http://188.172.235.146/dout.aspx?s=12251267&p=10000001&client=DynGate	false	Avira URL Cloud: safe	unknown
http://188.172.235.146/din.aspx?s=00000000&m=fast&client=DynGate&rnd=975066281&p=10000001	false	Avira URL Cloud: safe	unknown
http://188.172.235.146/dout.aspx?s=12251267&p=10000002&client=DynGate	false	Avira URL Cloud: safe	unknown
http://master13.teamviewer.com/din.aspx?s=00000000&client=DynGate&rnd=991669640&p=10000001	false		high
http://master13.teamviewer.com/din.aspx?s=42047145&client=DynGate&p=10000002	false		high
http://https://widolapsed.info/B8C631A8/	false	Avira URL Cloud: safe	unknown
http://master13.teamviewer.com/din.aspx?s=42047224&client=DynGate&p=10000002	false		high

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
188.172.235.146	unknown	Austria		42473	AS-ANEXIAANEXIAInternetdienstleistungsGmbHAT	false
185.188.32.23	master13.teamviewer.com	Germany		43304	TEAMVIEWER-ASDE	false
45.153.241.148	widolapsed.info	Germany		30823	COMBAHTONcombahtonGmbHDE	false

Private

IP
192.168.2.1
127.0.0.1

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	483790
Start date:	15.09.2021
Start time:	14:00:47
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 15m 11s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	wogZe27GBB.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
Run name:	Run with higher sleep bypass
Number of analysed new started processes analysed:	23
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:	mal72.evad.winEXE@13/7@4/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 28.3% (good quality ratio 27.6%) • Quality average: 83.4% • Quality standard deviation: 24.3%
HCA Information:	Failed
Cookbook Comments:	• Adjust boot time • Enable AMSI • Sleeps bigger than 120000ms are automatically reduced to 1000ms • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
14:02:08	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce UniPrint.exe "C:\Users\user\AppData\Roaming\ViberPC\icons\UniPrint.exe" f
14:02:16	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\RunOnce UniPrint.exe "C:\Users\user\AppData\Roaming\ViberPC\icons\UniPrint.exe" f

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\lsrC1CA.tmp	
Process:	C:\Users\user\Desktop\wogZe27GBB.exe
File Type:	data
Category:	dropped
Size (bytes):	5131242
Entropy (8bit):	6.736055511669049
Encrypted:	false
SSDEEP:	98304:xfmzCAW6LcJjdgHPmMogx1WZRkPapqj+ZG/D+AKbS5CjH:xfmzCgEqHuMogsRkyq0X
MD5:	1E6978657EEB4A9F6B4E84C62B228EE4
SHA1:	496A37AE9417163CFF53FBFEA9BA5BD1AC6BAFAE
SHA-256:	0FFB6906EA4C7B9A2E97FE0B8A205E00C8E5B1A7E03038627B1E6681CC66B986
SHA-512:	412332869C2B7C90A5409338EBBFF96786AEADDA54A0BA1F0D96035E929D7DFB773A2E02F8C588F15739A3CE0211DAE6074EEFE94AE18F85B5C4FA2C6BCBC6B
Malicious:	false
Reputation:	unknown
Preview:	D.....\$......b.....J...V.....

C:\Users\user\AppData\Roaming\ViberPC\icons\TV.dll		 
Process:	C:\Users\user\Desktop\wogZe27GBB.exe	
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows	
Category:	dropped	
Size (bytes):	73696	
Entropy (8bit):	6.629217484187715	
Encrypted:	false	
SSDEEP:	768:DWNCi7sBlpvYqSRw6zhD16poDVDREv1Mme9MfPGz49jjZLq00RKi5jYjflLhs8WhU:A6BmmPX6mDVdme9uGzWH10l+Uje8WhU	
MD5:	AC34AB95CBC23CDF332BEA2CC0FFBF35	
SHA1:	43ED3DD9863791294064D2F85F3DF3F08D572037	
SHA-256:	4BA3BD623A9919A357708DA57BBB9C978706DAD8D57DA64E89C780147843C7CE	
SHA-512:	3740DFD9F8ED967953C6A3522D66B5E547D3BB2A4C618FD667A817F6283E4353E2B81E994938E989AEA89BFD7A23E41309647EDCD1F6F0A075436E5B1FEE7B0	
Malicious:	true	
Antivirus:	- Antivirus: Metadefender, Detection: 6%, Browse - Antivirus: ReversingLabs, Detection: 51%	
Reputation:	unknown	
Preview:	MZ.....@.....!.L!This program cannot be run in DOS mode...\$......N.@...../.....Rich...PE..L...QQ.a.....!.....L.....-s....@.....`...D.....0.....0..... .....text.....`..rdata.....@..@.data.....@....rsrc.....@..@.reloc.....@..B.....	

C:\Users\user\AppData\Roaming\ViberPC\icons\TeamViewer.ini	
Process:	C:\Users\user\AppData\Roaming\ViberPC\icons\UniPrint.exe
File Type:	data
Category:	modified
Size (bytes):	226
Entropy (8bit):	3.2302371579115574
Encrypted:	false
SSDEEP:	6:y3ADAEyIA3m7D5KTLp3cQYdlRAeYIA3m7D5KLP3gk+AeYIA3m7D5KLP3gkp:E7NQalM7NM397NM3p

C:\Users\user\AppData\Roaming\ViberPC\Icons\TeamViewer.ini	
MD5:	D391CD3A0498B19D1DC083B30D010F4F
SHA1:	8BAFA1893DA6E63EC995E97C436E0E88BBC6E866
SHA-256:	5DD9E60CE43560D86998187E42C1B427FA034B126B90F3FFECB7282169F52D97
SHA-512:	0279F2164530EBDB9694E00CA2921BB1A9DE424E65435ABC858FB38AFBA6A94CDAA4A6747E9EA541DED19E9B1C1D15DA00632A7AC5E1D1DED1B20A71A809B1B6
Malicious:	false
Reputation:	unknown
Preview:	h.d.n.=.r.e.n.e.a.g.e.m.o.n.e.s...i.n.f.o.....h.p.n.=./B.8.C.6.3.1.A.8./.....h.s.n.=.1.....h.t.=.3.6.....r.e.n.e.a.g.e.m.o.n.e.s...i.n.f.o./B.8.C.6.3.1.A.8./1.3.6.r.e.n.e.a.g.e.m.o.n.e.s...i.n.f.o./B.8.C.6.3.1.A.8./1.3.6.

C:\Users\user\AppData\Roaming\ViberPC\Icons\Teamviewer_Resource_ja.dll		
Process:	C:\Users\user\Desktop\wogZe27GBB.exe	
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows	
Category:	dropped	
Size (bytes):	607528	
Entropy (8bit):	6.564133582926054	
Encrypted:	false	
SSDEEP:	6144:r5hmfFy7ZJ0uUCAD06v7JHZctms+2lifZ0iMe8dYySkYQKMDqtAu3NhGy6wSP:Vhmf4ACAzneosEi6YhvAuUGyUrNJbL	
MD5:	554EE592B125CFDF81B376B5C24AA61C	
SHA1:	666D2C04171246734575D4453289AA2D9AF93B97	
SHA-256:	B296EF421D5B7F569E623D41A42D87A064C4358CFA89A192988F854929E3ABD1	
SHA-512:	6C3111BF9D26929D426797EBDD8D804B34E2E8F593BF488298E70964538F2DA3D971C4ED3C3237C829AE7DE4FDB8D4316D84F153E93E3788808547A8538B73F5	
Malicious:	false	
Antivirus:	- Antivirus: Metadefender, Detection: 0%, Browse - Antivirus: ReversingLabs, Detection: 0%	
Reputation:	unknown	
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.....-T.L...L...L...F.L...B.L:Rich.L:.....PE.L.....LK.....!.....0.....0..(.....rsrc.....@..@.reloc.....@..B.....	

C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe		
Process:	C:\Users\user\Desktop\wogZe27GBB.exe	
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows	
Category:	dropped	
Size (bytes):	4375848	
Entropy (8bit):	6.621789733656387	
Encrypted:	false	
SSDEEP:	98304:6jdgHPmMogx1WZRkPapqj+ZG/D+AKbS5m:4qHuMogsRkyq0N	
MD5:	EBDBA07BFABCF24F5D79EF27247EA643	
SHA1:	A3A7498F02BAB188B3944382BBA4D016D63607D1	
SHA-256:	D2CDCA8EFA27089D3DEAD0CCEAFBE470B3815C9C2A362C007D1F516E5379AC92	
SHA-512:	412B42C540A9FE41709453D725B7A1E888849326A70A411E645F29240D730D69EBCF4B26E6870D33E0A395C612470BD00064025D22B0C6BCD211242E8EF6CEA6	
Malicious:	true	
Antivirus:	- Antivirus: Metadefender, Detection: 0%, Browse - Antivirus: ReversingLabs, Detection: 0%	
Reputation:	unknown	
Preview:	MZ.....@.....!..L!This program cannot be run in DOS mode...\$.....o...o...o.....o.....2.o.....q.o.F.2...o...n...o.F.o...o...o.....o.Rich...o.....PE..L.....LK.....3.....F.....03...@.....K.....ZC.....@.....K.8'.....B.(.....pe4.....X:.....X:@.....03.....text...3.....3.....`rdata.&...03.....3.....@..@.data...h...P@..".*@.....@...tls.....K.....LB.....@....rsrc...8'...K..b...NB.....@..@.....	

C:\Users\user\AppData\Roaming\ViberPC\Icons\vpn.cab		
Process:	C:\Users\user\Desktop\wogZe27GBB.exe	
File Type:	Microsoft Cabinet archive data, 71196 bytes, 8 files	
Category:	dropped	
Size (bytes):	71196	
Entropy (8bit):	7.996182851828797	
Encrypted:	true	
SSDEEP:	1536:qUTRtkxXFuG1DKNYCqRBiFxmZPQCJh/njgG5+jC5hA101pNO0:qUNtax12mCqRBiyQG/jgG5+j2NO0	
MD5:	8A84AA1B9F20DC194947D7AC592D818E	
SHA1:	4A77AB0D59F39BF600BB89D9121446F6AA2D139B	
SHA-256:	8A740BE5D92B734E77B210354988DFD49F31C49814240513CF4B0353A8CE6DFB	
SHA-512:	B3F90ADB48861CD775F15E75885C81A130D62DFE429A5833FA1CE0BC203EEA15BD8A7306618B1F4D27810493300400C8B149D58032F90F0E9D93B04F9B8F1050	

C:\Users\user1\AppData\Roaming\ViberPC\icons\vpn.cab	
Malicious:	false
Reputation:	unknown
Preview:	MSCF.....JA..H.....).....k<b..64\teamviewervpn.cat.....).....k<b..64\TeamViewerVPN.inf.(....>.....k<b..64\teamviewervpn.sys.<.....k<b..64\install.exe..).....k<b..86\teamviewervpn.cat.....~.....k<b..86\TeamViewerVPN.inf..b...B....k<b..86\teamviewervpn.sys.....k<b..86\install.exe.h.t"X<.[.....`.....@...N.f[.U.....\$. ..L.F..4... ...U\$Q/...%J).D...@F.....f...9.../...@...x;N..w..2...i1P....O....T..T.y...`...;.\$&....@.....@...~..J.44...@...M....X\0c].W...,].x..+P..N..S0@B.;?.(..B....%{. (T....U.5..=3'xci.;...P\$.H)...1...h_e_{...Q_}...K....U.s...._WRWIS.8._...D.NI..> O<.q...\$0.EA*8d.../..=2q...g..._Hs['+...`>U..)X.G*8....>..I4 ....).Ps.a.8.....4.0`_ .. t%...P.qgr.'..~.d..f....o...w..q.....O.K..Y.8..M.D...p.....~.....O?.....}@.....>....O..N...c./p..[....._=-S...Q..p.O...@.WL.....*..).%1...3a.....u...).K.Y...s..E....".e.....X0(IR...1. ..\.6...(i

Static File Info

General	
File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.995528478877956
TrID:	- Win32 Executable (generic) a (10002005/4) 92.16% - NSIS - Nullsoft Scriptable Install System (846627/2) 7.80% - 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:	wogZe27GBB.exe
File size:	1773472
MD5:	5efc68abd7fec415e34980d95a06a66a
SHA1:	34b243a0b3e322b8983b528caa5849395360a91d
SHA256:	0f655a8ac0d7fdc7ac44fdd9799129848faf9c73bfa0e108fd903de439447232
SHA512:	92aa33884c54bdb2608994b3e4c9b0909b002a38344bae2b4fb01c9a713542cf8a51684a0e3d614730340a995bb918dedb5e4c801ba9e3afa834399f38232079
SSDEEP:	49152:tMvOJUaiTddo110aPENuUn/vrmUJjeftHj9uDd:tHjiTvLn3rb4jkjd
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....\$......1...:u..iu.. iu...i..w..iu...i...id..!l...i...it..iRichu..i.....PE.. .L.....*J.....\.....

File Icon

	
Icon Hash:	8282c2d2d2c292a1

Static PE Info

General	
Entrypoint:	0x40323c
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x4A2AE2A2 [Sat Jun 6 21:41:54 2009 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:	5bd07784f328e868356a895d4ab1a505

Authenticode Signature	
Signature Valid:	true
Signature Issuer:	CN=Sectigo RSA Code Signing CA, O=Sectigo Limited, L=Salford, S=Greater Manchester, C=GB
Signature Validation Error:	The operation completed successfully
Error Number:	0
Not Before, Not After	4/21/2021 2:00:00 AM 4/22/2022 1:59:59 AM
Subject Chain	CN=Mapping OOO, O=Mapping OOO, L=Saint Petersburg, C=RU
Version:	3
Thumbprint MD5:	B9C33DB697628B5EB88B4004D0D6900E
Thumbprint SHA-1:	D9F41380CE8E8E22E2EF7F558D6D17BB94AA28BE
Thumbprint SHA-256:	7B5C783B055EB8BA37480ED0E990E3A4631D38531485ECF3875FE213B2FB661D
Serial:	00A46F9D8784778BAA48167C48BBC56F30

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5a5a	0x5c00	False	0.660453464674	data	6.41769823686	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1190	0x1200	False	0.375217013889	SysEx File -	4.24219639454	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1af98	0x400	False	0.55859375	data	4.70902740305	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x24000	0x20000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x44000	0x13d8	0x1400	False	0.2705078125	data	3.94953591447	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

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

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 15, 2021 14:02:03.784799099 CEST	192.168.2.4	8.8.8.8	0xbcd1	Standard query (0)	ping3.dyngate.com	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 15, 2021 14:02:03.823643923 CEST	192.168.2.4	8.8.8.8	0xfb8b	Standard query (0)	ping3.dyngate.com	A (IP address)	IN (0x0001)
Sep 15, 2021 14:02:04.040373087 CEST	192.168.2.4	8.8.8.8	0x4123	Standard query (0)	master13.teamviewer.com	A (IP address)	IN (0x0001)
Sep 15, 2021 14:02:08.655509949 CEST	192.168.2.4	8.8.8.8	0x9803	Standard query (0)	widolapsed.info	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 15, 2021 14:02:03.814250946 CEST	8.8.8.8	192.168.2.4	0xbcd1	Name error (3)	ping3.dyngate.com	none	none	A (IP address)	IN (0x0001)
Sep 15, 2021 14:02:03.849232912 CEST	8.8.8.8	192.168.2.4	0xfb8b	Name error (3)	ping3.dyngate.com	none	none	A (IP address)	IN (0x0001)
Sep 15, 2021 14:02:04.073539972 CEST	8.8.8.8	192.168.2.4	0x4123	No error (0)	master13.teamviewer.com		185.188.32.23	A (IP address)	IN (0x0001)
Sep 15, 2021 14:02:08.683300018 CEST	8.8.8.8	192.168.2.4	0x9803	No error (0)	widolapsed.info		45.153.241.148	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

widolapsed.info
master13.teamviewer.com
188.172.235.146

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49767	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49838	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49843	45.153.241.148	443	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49761	185.188.32.23	80	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 14:02:04.163152933 CEST	1208	OUT	GET /din.aspx?s=00000000&client=DynGate&md=991669640&p=10000001 HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: master13.teamviewer.com Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 14:02:04.184066057 CEST	1208	IN	HTTP/1.1 200 OK Pragma: no-cache Cache-control: no-cache, no-store Content-Type: application/octet-stream Content-length: 10 Data Raw: 17 24 34 32 30 34 37 31 34 35 Data Ascii: \$42047145
Sep 15, 2021 14:02:04.214737892 CEST	1208	OUT	GET /dout.aspx?s=42047145&p=10000001&client=DynGate&data=FyQSBQcJHqkys5MkoZ6YmBgcGRsZGpmckySiHpgTJqChnpg8MrGzGjExHByxGZkbr5kcmpsaHBgbGRsTJqSiHpg8MrGzGjExHByxGZkbr5kcmpsaHBgbGRsTJ6meq7S3GZcYmJMrHpiXgXGxwbkCip HTTP/1.1 Accept: */* Content-Type: application/octet-stream Content-Transfer-Encoding: binary User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: master13.teamviewer.com Connection: Keep-Alive Cache-Control: no-cache
Sep 15, 2021 14:02:04.235718012 CEST	1208	IN	HTTP/1.1 200 OK Pragma: no-cache Cache-control: no-cache, no-store Content-length: 0
Sep 15, 2021 14:02:04.241089106 CEST	1209	OUT	GET /din.aspx?s=42047145&client=DynGate&p=10000002 HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: master13.teamviewer.com Connection: Keep-Alive Cache-Control: no-cache
Sep 15, 2021 14:02:04.262003899 CEST	1209	IN	HTTP/1.1 200 OK Pragma: no-cache Cache-control: no-cache, no-store Content-Type: application/octet-stream Content-length: 16 Data Raw: 17 24 13 0b 00 18 20 19 9c 98 98 1a 9b 9a 1a 9c Data Ascii: \$

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49762	185.188.32.23	80	C:\Users\user\AppData\Roaming\ViberPC\icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 14:02:04.293028116 CEST	1210	OUT	GET /din.aspx?s=00000000&client=DynGate&rnd=991669640&p=10000001 HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: master13.teamviewer.com Connection: Keep-Alive Cache-Control: no-cache
Sep 15, 2021 14:02:04.314116955 CEST	1210	IN	HTTP/1.1 200 OK Pragma: no-cache Cache-control: no-cache, no-store Content-Type: application/octet-stream Content-length: 10 Data Raw: 17 24 34 32 30 34 37 31 35 32 Data Ascii: \$42047152
Sep 15, 2021 14:02:04.327481985 CEST	1211	OUT	GET /dout.aspx?s=42047152&p=10000001&client=DynGate&data=FyQS8QAJHqmyuig6sTY0saWyvJMkoZ6YmBgcGRsZGpmckySiHpmcmJgam5oanBMmpKlemDwysbMaMTEcHLEZmRuvrmRyamaxocGBsZGxMrHpiXgXGxwbkCipkyE0tzC5PJ6DAQAAAFIAACKpoJiAAgAACIAAAH7LQs0qhaWs0MJaOW1RZp/s+y/yn5XEbeVZg9sKBj5zPw4VSW4zdwQ3dPOJPU35FNklfclZEzewXzbzR9HNSPt0dvZIMvjxbsFa8mt4y/fhUHNJCruEcKZvCgbkPO7XECRgFWPWpqy/DxavH2VA1uMNeC6MgWi1tqYJlUpU HTTP/1.1 Accept: */* Content-Type: application/octet-stream Content-Transfer-Encoding: binary User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: master13.teamviewer.com Connection: Keep-Alive Cache-Control: no-cache
Sep 15, 2021 14:02:04.348402023 CEST	1211	IN	HTTP/1.1 200 OK Pragma: no-cache Cache-control: no-cache, no-store Content-length: 0
Sep 15, 2021 14:02:04.349881887 CEST	1211	OUT	GET /din.aspx?s=42047152&client=DynGate&p=10000002 HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: master13.teamviewer.com Connection: Keep-Alive Cache-Control: no-cache

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 14:02:04.372112036 CEST	1211	IN	HTTP/1.1 200 OK Pragma: no-cache Cache-control: no-cache, no-store Content-Type: application/octet-stream Content-length: 9 Data Raw: 17 24 13 04 00 98 20 27 a5 Data Ascii: \$ '

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49763	185.188.32.23	80	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 14:02:04.397053957 CEST	1212	OUT	GET /din.aspx?s=00000000&client=DynGate&rnd=991669640&p=10000001 HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: master13.teamviewer.com Connection: Keep-Alive Cache-Control: no-cache
Sep 15, 2021 14:02:04.418442011 CEST	1212	IN	HTTP/1.1 200 OK Pragma: no-cache Cache-control: no-cache, no-store Content-Type: application/octet-stream Content-length: 10 Data Raw: 17 24 34 32 30 34 37 31 35 39 Data Ascii: \$42047159
Sep 15, 2021 14:02:04.422777891 CEST	1213	OUT	GET /dout.aspx?s=42047159&p=10000001&client=DynGate&data=FyQS9ACjHqmyuim0s7cwujq5MqWyyJMkoZ6YmBgcGRsZGpmckySiHpmcmJgam5oanBMmpKlemDwysbMaMTechLEZmRuvrmRyamxocGBsZGxMrHpiAlxgXGxwbkCipkyE0tzC5PJ6DAQAAABIAACkpoJiAAgAACIAAABKJHDw2LgVxSDgQRZJcruSvmCif9Gt2TW3hKr1gLFUfE+41DTTElJH9R8iP3LoBGOJ+mtJU9XCLVeH0PEl9syAw5y9+liHYCQSiHVEX/VS+caNKAIINEKBpchOIJAAICwW843p+TOKZHDfo8qX87SA1CKgBTr4AFtosrqQ/gO/pU HTTP/1.1 Accept: */* Content-Type: application/octet-stream Content-Transfer-Encoding: binary User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: master13.teamviewer.com Connection: Keep-Alive Cache-Control: no-cache
Sep 15, 2021 14:02:04.443669081 CEST	1213	IN	HTTP/1.1 200 OK Pragma: no-cache Cache-control: no-cache, no-store Content-length: 0
Sep 15, 2021 14:02:05.181092978 CEST	1213	OUT	GET /din.aspx?s=42047159&client=DynGate&p=10000002 HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: master13.teamviewer.com Connection: Keep-Alive Cache-Control: no-cache
Sep 15, 2021 14:02:05.202090025 CEST	1214	IN	HTTP/1.1 200 OK Pragma: no-cache Cache-control: no-cache, no-store Content-Type: application/octet-stream Content-length: 9 Data Raw: 17 24 13 04 00 98 20 27 a5 Data Ascii: \$ '

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.4	49764	185.188.32.23	80	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 14:02:05.470541954 CEST	1214	OUT	GET /din.aspx?s=00000000&client=DynGate&rnd=279943160&p=10000001 HTTP/1.1 Accept: */* User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: master13.teamviewer.com Connection: Keep-Alive Cache-Control: no-cache
Sep 15, 2021 14:02:05.504560947 CEST	1214	IN	HTTP/1.1 200 OK Pragma: no-cache Cache-control: no-cache, no-store Content-Type: application/octet-stream Content-length: 10 Data Raw: 17 24 34 32 30 34 37 32 32 34 Data Ascii: \$42047224

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 14:02:05.885689974 CEST	1215	OUT	GET /dout.aspx?s=42047224&p=10000001&client=DynGate&data=FyQS6wChTjSytzoeqisoqZMjHqY3s7S3EyOrnpgTI6u mMrsyth6aGBgTJDsyMqe3NjS3Mqm6MLo6uZ6YeyQqKignqqoemRMkoZ6YmBgcGRsZGpmckySiHpmcmJgam5oanBMls rK4MLY0uzKemJmMMLczurCzsp61MJMmNLGytzmyqjy4Mp6Yeyakoh6YPDKxssoxMRwcsRmZG6+ZHJqbG hwYGxkbEyc3p7Mgsbo0uzKlsrK4MLY0uzKemBMPorc6NLaynpqTKbq4ODe5OjKylzKwujq5MrmemJMqlagnqqoemBM rHpiXgXGxwbkCip HTTP/1.1 Accept: /*/* Content-Type: application/octet-stream Content-Transfer-Encoding: binary User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: master13.teamviewer.com Connection: Keep-Alive Cache-Control: no-cache
Sep 15, 2021 14:02:05.909208059 CEST	1215	IN	HTTP/1.1 200 OK Pragma: no-cache Cache-control: no-cache, no-store Content-length: 0
Sep 15, 2021 14:02:06.948101997 CEST	1216	OUT	GET /din.aspx?s=42047224&client=DynGate&p=10000002 HTTP/1.1 Accept: /*/* User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: master13.teamviewer.com Connection: Keep-Alive Cache-Control: no-cache
Sep 15, 2021 14:02:06.972300053 CEST	1216	IN	HTTP/1.1 200 OK Pragma: no-cache Cache-control: no-cache, no-store Content-Type: application/octet-stream Content-length: 413 Data Raw: 17 24 13 98 01 98 20 27 a5 af 98 98 18 18 18 2f 96 af 99 2f af 98 9c 1c 17 18 9b 99 17 19 19 9a 97 18 9a 1b 1d 1c 18 2f 99 98 9b 9a 19 af 98 af 96 98 af 98 17 18 17 18 17 18 2f af 98 9c 1a 97 18 9c 1c 17 19 99 17 19 99 af 98 9c 1a 97 18 9c 1c 17 19 99 17 19 19 af 98 2f 99 9c 98 98 1a 9b 9a 1a 9c 2f 98 af 98 2f 98 2f 98 2f 98 9c 9a 19 9b 9c 9b 9b 19 1a af af 98 9c 1c 17 1b 1a 97 1b 9b 17 18 9a 18 96 18 9c 1c 17 18 9b 99 17 19 1a 1b 17 18 9b 98 96 19 9b 97 19 1a 99 17 19 1a 1b 97 18 98 1c 96 18 9c 1c 17 18 9b 99 17 19 18 99 97 1b 99 16 18 9c 1c 17 18 9b 99 17 19 19 9a 97 18 9a 1b 16 19 18 99 97 19 19 1b 97 18 9b 1c 17 18 9a 1a 96 1c 9a 17 18 9b 17 1b 17 18 9b 9a 16 18 9c 1c 17 18 9b 99 17 19 1a 1a 97 18 9a 18 96 19 18 99 97 19 19 1b 97 18 9b 19 97 18 99 9b 96 18 9c 1c 17 18 9b 99 17 18 9c 9c 17 18 99 99 96 18 9a 9c 17 18 9b 9b 17 1c 1b 17 1b 96 19 9b 97 19 1a 99 17 19 19 99 17 18 98 19 96 18 9b 9c 17 19 1a 9a 97 18 9a 9a 97 18 9b 9a 96 18 9a 9c 97 18 99 19 17 18 9c 19 17 19 18 1c 96 19 18 9b 97 18 9a 1b 17 19 18 97 18 99 9a 16 18 9c 1c 17 18 9b 9 9 17 19 19 19 97 18 98 99 96 19 18 9b 97 18 9a 1b 17 18 99 97 18 99 9b 16 19 9b 97 19 1a 99 17 19 19 1a 17 1b 1c af b2 b3 17 b1 31 98 33 9a a1 a4 b4 26 36 a8 18 21 a0 a0 a0 af Data Ascii: \$ '/////////13&6!

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
7	192.168.2.4	49765	188.172.235.146	80	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data
Sep 15, 2021 14:02:07.205918074 CEST	1217	OUT	GET /din.aspx?s=00000000&m=fast&client=DynGate&rnd=975066281&p=10000001 HTTP/1.1 Accept: /*/* User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: 188.172.235.146 Connection: Keep-Alive Cache-Control: no-cache
Sep 15, 2021 14:02:07.232043982 CEST	1217	IN	HTTP/1.1 200 OK Pragma: no-cache Cache-control: no-cache, no-store Content-Type: application/octet-stream Content-length: 17 Data Raw: 17 24 66 61 73 74 31 32 32 35 31 32 36 37 Data Ascii: \$fast12251267
Sep 15, 2021 14:02:07.350502014 CEST	1219	OUT	POST /dout.aspx?s=12251267&p=10000002&client=DynGate HTTP/1.1 Accept: /*/* Content-Type: application/octet-stream Content-Transfer-Encoding: binary User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; DynGate) Host: 188.172.235.146 Content-Length: 500000 Connection: Keep-Alive Cache-Control: no-cache

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
8	192.168.2.4	49766	188.172.235.146	80	C:\Users\user\AppData\Roaming\ViberPC\Icons\UniPrint.exe

Timestamp	kBytes transferred	Direction	Data
-----------	--------------------	-----------	------

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: wogZe27GBB.exe PID: 7160 Parent PID: 6004

General

Start time:	14:01:48
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\wogZe27GBB.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\wogZe27GBB.exe'
Imagebase:	0x400000
File size:	1773472 bytes
MD5 hash:	5EFC68ABD7FEC415E34980D95A06A66A
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

File Written

File Read

Analysis Process: UniPrint.exe PID: 4260 Parent PID: 7160

General

Start time:	14:01:51
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Roaming\ViberPC\icons\UniPrint.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\ViberPC\icons\UniPrint.exe' f
Imagebase:	0x400000
File size:	4375848 bytes
MD5 hash:	EBDBA07BFABCF24F5D79EF27247EA643
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Antivirus matches:	- Detection: 0%, Metadefender, Browse - Detection: 0%, ReversingLabs
Reputation:	low

File Activities

Show Windows behavior

Analysis Process: UniPrint.exe PID: 5356 Parent PID: 5060**General**

Start time:	14:01:58
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Roaming\ViberPC\icons\UniPrint.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\ViberPC\icons\UniPrint.exe
Imagebase:	0x400000
File size:	4375848 bytes
MD5 hash:	EBDBA07BFABCF24F5D79EF27247EA643
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

File Activities

Show Windows behavior

File Read**Registry Activities**

Show Windows behavior

Key Created**Key Value Created****Analysis Process: svchost.exe PID: 4296 Parent PID: 568****General**

Start time:	14:01:59
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 5904 Parent PID: 568**General**

Start time:	14:02:06
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\svchost.exe
Wow64 process (32bit):	true
Commandline:	c:\windows\syswow64\svchost.exe -k 'usbportsmanagergrp' -svcr 'uniprint.exe' -s USBManager

Imagebase:	0xb60000
File size:	44520 bytes
MD5 hash:	FA6C268A5B5BDA067A901764D203D433
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: svchost.exe PID: 6852 Parent PID: 568

General

Start time:	14:02:14
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: UniPrint.exe PID: 6952 Parent PID: 3424

General

Start time:	14:02:17
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Roaming\ViberPC\icons\UniPrint.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\ViberPC\icons\UniPrint.exe' f
Imagebase:	0x400000
File size:	4375848 bytes
MD5 hash:	EBDBA07BFABCF24F5D79EF27247EA643
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: UniPrint.exe PID: 7016 Parent PID: 5060

General

Start time:	14:02:22
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Roaming\ViberPC\icons\UniPrint.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\ViberPC\icons\UniPrint.exe
Imagebase:	0x400000
File size:	4375848 bytes
MD5 hash:	EBDBA07BFABCF24F5D79EF27247EA643

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

File Activities

Show Windows behavior

Analysis Process: UniPrint.exe PID: 7080 Parent PID: 3424

General

Start time:	14:02:26
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Roaming\ViberPC\icons\UniPrint.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\ViberPC\icons\UniPrint.exe' f
Imagebase:	0x400000
File size:	4375848 bytes
MD5 hash:	EBDBA07BFABCF24F5D79EF27247EA643
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: svchost.exe PID: 6408 Parent PID: 568

General

Start time:	14:02:29
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: UniPrint.exe PID: 6484 Parent PID: 5060

General

Start time:	14:02:32
Start date:	15/09/2021
Path:	C:\Users\user\AppData\Roaming\ViberPC\icons\UniPrint.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\ViberPC\icons\UniPrint.exe
Imagebase:	0x400000
File size:	4375848 bytes
MD5 hash:	EBDBA07BFABCF24F5D79EF27247EA643
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: svchost.exe PID: 5248 Parent PID: 568

General

Start time:	14:02:39
Start date:	15/09/2021
Path:	C:\Windows\System32\svchost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\svchost.exe -k netsvcs -p
Imagebase:	0x7ff6eb840000
File size:	51288 bytes
MD5 hash:	32569E403279B3FD2EDB7EBD036273FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Disassembly

Code Analysis