ID: 523630
Sample Name: important invoice presentation nov 2021.pif
Cookbook: default.jbs
Time: 14:31:45
Date: 17/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

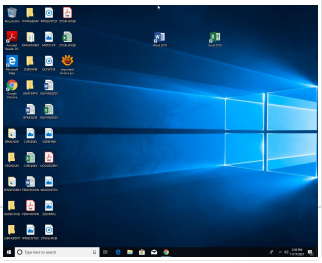
Windows Analysis Report important invoice presentatio…

Overview

General Information

Sample Name:	important invoice presentation nov 2021.pif (renamed file extension from pif to exe)
Analysis ID:	523630
MD5:	1364844e0bfb349.
SHA1:	ffc57ad66c9a376..
SHA256:	004f011b37e4446.
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

NetWire

Score:	84
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Compliance

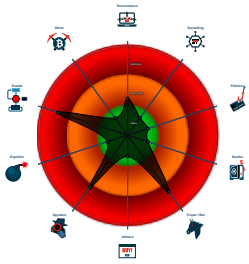
HIGH
MODERATE
LOW

Score:	46
Range:	0 - 100

Signatures

- Found malware configuration
- Malicious sample detected (through …
- Yara detected NetWire RAT
- Sigma detected: Copying Sensitive …
- Maps a DLL or memory area into an…
- Overwrites code with unconditional j…
- Initial sample is a PE file and has a …
- Found evasive API chain (may stop…
- Writes to foreign memory regions
- Contains functionality to log keystro…
- Found stalling execution ending in A…
- Sigma detected: Xwizard DLL Sidelo…
- Allocates memory in foreign process…

Classification



Process Tree

- **System is w10x64**
- important invoice presentation nov 2021.exe (PID: 6968 cmdline: "C:\Users\user\Desktop\important invoice presentation nov 2021.exe" MD5: 1364844E0BFB349272C5050FB0E677E3)
  - cmd.exe (PID: 3576 cmdline: cmd /c xcopy "C:\Users\user\Desktop\important invoice presentation nov 2021.exe" "%ProgramFiles%\Security\" /y /i /c /q MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 5272 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - xcopy.exe (PID: 6100 cmdline: xcopy "C:\Users\user\Desktop\important invoice presentation nov 2021.exe" "C:\Program Files (x86)\Security\" /y /i /c /q MD5: 9F3712DDC0D7FE3D75B8A06C6EE8E68C)
  - cmd.exe (PID: 5536 cmdline: cmd /c schtasks /create /sc ONLOGON /tn "Security" /tr "%ProgramFiles%\Security\important invoice presentation nov 2021.exe" /it /f MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 3168 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 5660 cmdline: schtasks /create /sc ONLOGON /tn "Security" /tr "C:\Program Files (x86)\Security\important invoice presentation nov 2021.exe" /it /f MD5: 15FF7D8324231381BAD48A052F85DF04)
  - xwizard.exe (PID: 5612 cmdline: C:\Windows\System32\xwizard.exe MD5: 17059CA3DDD41B52DE4140705B38AE53)
- important invoice presentation nov 2021.exe (PID: 2872 cmdline: C:\Program Files (x86)\Security\important invoice presentation nov 2021.exe MD5: 1364844E0BFB349272C5050FB0E677E3)
  - cmd.exe (PID: 5704 cmdline: cmd /c xcopy "C:\Program Files (x86)\Security\important invoice presentation nov 2021.exe" "%ProgramFiles%\Security\" /y /i /c /q MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 3132 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - xcopy.exe (PID: 4920 cmdline: xcopy "C:\Program Files (x86)\Security\important invoice presentation nov 2021.exe" "C:\Program Files (x86)\Security\" /y /i /c /q MD5: 9F3712DDC0D7FE3D75B8A06C6EE8E68C)
  - cmd.exe (PID: 3032 cmdline: cmd /c schtasks /create /sc ONLOGON /tn "Security" /tr "%ProgramFiles%\Security\important invoice presentation nov 2021.exe" /it /f MD5: F3BDBE3BB6F734E357235F4D5898582D)
    - conhost.exe (PID: 4388 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
    - schtasks.exe (PID: 2032 cmdline: schtasks /create /sc ONLOGON /tn "Security" /tr "C:\Program Files (x86)\Security\important invoice presentation nov 2021.exe" /it /f MD5: 15FF7D8324231381BAD48A052F85DF04)
  - xwizard.exe (PID: 2040 cmdline: C:\Windows\System32\xwizard.exe MD5: 17059CA3DDD41B52DE4140705B38AE53)
- **cleanup**

Malware Configuration

Threatname: NetWire

```
{
  "C2 list": [
    "calibare5454.pro:3360"
  ],
  "Password": "Password",
  "Host ID": "HostId-%Rand%",
  "Mutex": "wAnRkHLX",
  "Install Path": "-",
  "Startup Name": "-",
  "ActiveX Key": "-",
  "KeyLog Directory": "-"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000001E.00000002.688394318.000000000422000.00000004.00020000.sdmp	JoeSecurity_NetWire_1	Yara detected NetWire RAT	Joe Security	
0000001E.00000002.688394318.000000000422000.00000004.00020000.sdmp	netwire	detect netwire in memory	JPCERT/CC Incident Response Group	• 0x580:$v1: HostId-%Rand%
00000001.00000002.507835553.000000001C8F0000.00000040.00000001.sdmp	JoeSecurity_NetWire_1	Yara detected NetWire RAT	Joe Security	
0000000E.00000002.863773731.000000000422000.00000004.00020000.sdmp	JoeSecurity_NetWire_1	Yara detected NetWire RAT	Joe Security	
0000000D.00000002.683551594.000000001CF00000.00000040.00000001.sdmp	JoeSecurity_NetWire_1	Yara detected NetWire RAT	Joe Security	

Click to see the 5 entries

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.important invoice presentation nov 2021.exe.1c8f0000.1.raw.unpack	JoeSecurity_NetWire_1	Yara detected NetWire RAT	Joe Security	
14.2.xwizard.exe.400000.0.unpack	JoeSecurity_NetWire_1	Yara detected NetWire RAT	Joe Security	
13.2.important invoice presentation nov 2021.exe.1cf00000.1.raw.unpack	JoeSecurity_NetWire_1	Yara detected NetWire RAT	Joe Security	
30.2.xwizard.exe.400000.0.unpack	JoeSecurity_NetWire_1	Yara detected NetWire RAT	Joe Security	
30.2.xwizard.exe.400000.0.unpack	netwire	detect netwire in memory	JPCERT/CC Incident Response Group	• 0x20f80:$v1: HostId-%Rand%

Sigma Overview

System Summary:

Sigma detected: Copying Sensitive Files with Credential Data

Sigma detected: Xwizard DLL Sideloading

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Compliance:

Uses 32bit PE files

PE / OLE file has a valid certificate

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

Networking:

C2 URLs / IPs found in malware configuration

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Contains functionality to log keystrokes

System Summary:

Malicious sample detected (through community Yara rule)

Initial sample is a PE file and has a suspicious name

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

Overwrites code with unconditional jumps - possibly settings hooks in foreign process

Malware Analysis System Evasion:

Found evasive API chain (may stop execution after checking mutex)

Found stalling execution ending in API Sleep call

HIPS / PFW / Operating System Protection Evasion:

Maps a DLL or memory area into another process

Writes to foreign memory regions

Allocates memory in foreign processes

Remote Access Functionality:

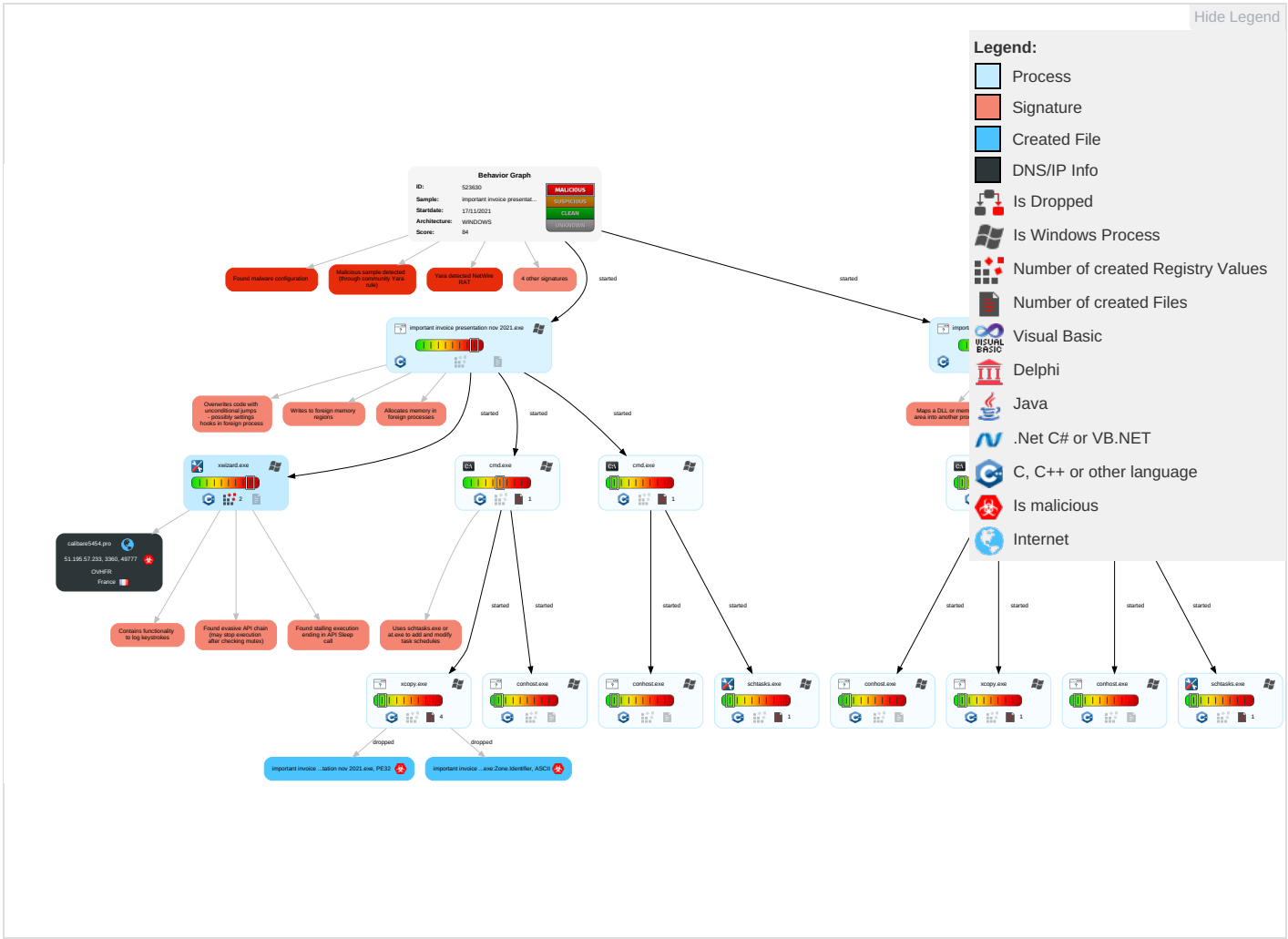
Yara detected NetWire RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Valid Accounts	Native API 1 1	Scheduled Task/Job 1	Process Injection 3 1 2	Disable or Modify Tools 1	Credential API Hooking 1	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 1	Eavesd Insecur Networ Commu
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1	Input Capture 1 2 1	Account Discovery 1	Remote Desktop Protocol	Screen Capture 1	Exfiltration Over Bluetooth	Encrypted Channel 2	Exploit Redirec Calls/SI

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 2	Security Account Manager	File and Directory Discovery 2	SMB/Windows Admin Shares	Credential API Hooking 1	Automated Exfiltration	Non-Standard Port 1	Exploit Track D Locatio
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1	NTDS	System Information Discovery 1 5	Distributed Component Object Model	Input Capture 1 2 1	Scheduled Transfer	Non-Application Layer Protocol 1	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Security Software Discovery 3 1	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 1 1	Manipu Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Process Injection 3 1 2	Cached Domain Credentials	Process Discovery 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammin Denial Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgr Insecur Protoco
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	Remote System Discovery 1	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Base St

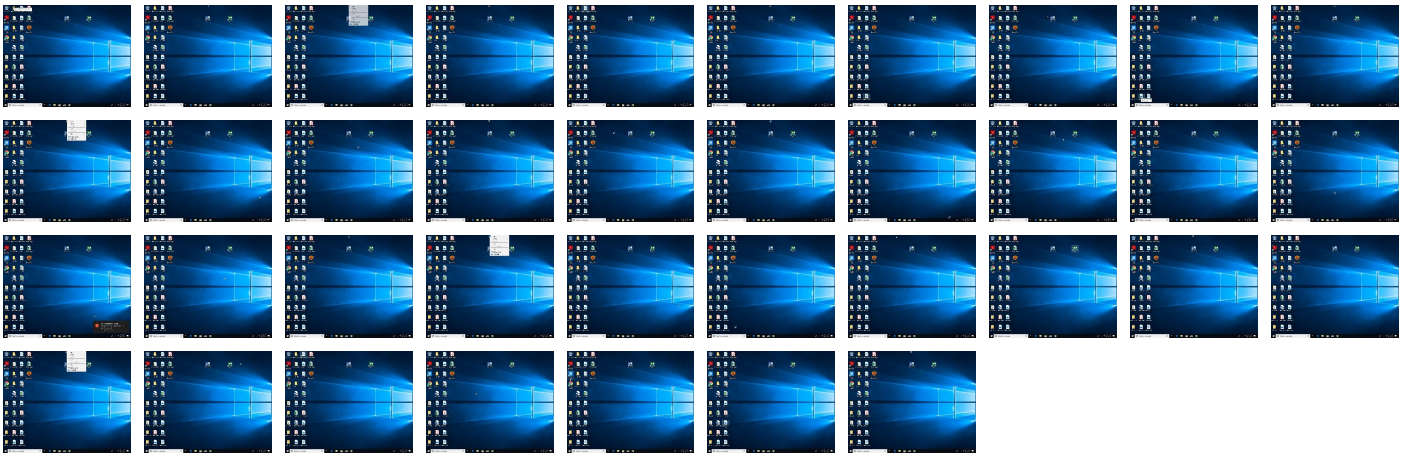
Behavior Graph



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

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
30.2.xwizard.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen		Download File
13.2.important invoice presentation nov 2021.exe.1cf00000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
14.2.xwizard.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen		Download File
1.2.important invoice presentation nov 2021.exe.1c8f0000.1.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoPublicCodeSigningCAR36.crl0y	0%	URL Reputation	safe	
http://crl.sectigo.com/SectigoPublicCodeSigningRootR46.crl0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://www.yandex.comsocks=	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0D	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoPublicCodeSigningCAR36.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoPublicCodeSigningRootR46.p7c0#	0%	URL Reputation	safe	
calibare5454.pro:3360	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
calibare5454.pro	51.195.57.233	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
calibare5454.pro:3360	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
51.195.57.233	calibare5454.pro	France		16276	OVHFR	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal

Analysis ID:	523630
Start date:	17.11.2021
Start time:	14:31:45
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	important invoice presentation nov 2021.pif (renamed file extension from pif 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:	35
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:	mal84.troj.spyw.evad.winEXE@26/2@1/1
EGA Information:	• Successful, ratio: 66.7%
HDC Information:	• Successful, ratio: 91.9% (good quality ratio 46%) • Quality average: 39.4% • Quality standard deviation: 44%
HCA Information:	• Successful, ratio: 94% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Override analysis time to 240s for sample files taking high CPU consumption
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
14:33:51	Task Scheduler	Run new task: Security path: C:\Program s>Files (x86)\Security\important invoice presentation nov 2021.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
51.195.57.233	4opi0b3gZn.exe	Get hash	malicious	Browse	
	fGh96VozUi.exe	Get hash	malicious	Browse	
	cTpmz8G3Ob.exe	Get hash	malicious	Browse	
	DigiCertUtil.exe	Get hash	malicious	Browse	
	FireFoxExtension.exe	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
OVHFR	XE7c64PfoP.exe	Get hash	malicious	Browse	• 91.134.150.150
	3AgSx1cQFE.exe	Get hash	malicious	Browse	• 51.81.139.72
	982tSWUdff.dll	Get hash	malicious	Browse	• 158.69.222.101
	ji2TXozBAl.dll	Get hash	malicious	Browse	• 158.69.222.101
	N6CyMVFTbm.dll	Get hash	malicious	Browse	• 158.69.222.101
	ji2TXozBAl.dll	Get hash	malicious	Browse	• 158.69.222.101
	index.dll	Get hash	malicious	Browse	• 51.68.175.8
	lUynlGo56B9U3mQG.dll	Get hash	malicious	Browse	• 51.178.61.60
	Ttj0AuTKHQ.dll	Get hash	malicious	Browse	• 51.178.61.60
	KgtyOfJo2W.dll	Get hash	malicious	Browse	• 51.178.61.60
	h5ZcTHDXbJ.dll	Get hash	malicious	Browse	• 51.178.61.60
	SCygJvetwW.dll	Get hash	malicious	Browse	• 51.68.175.8
	a5uyawQx9G.dll	Get hash	malicious	Browse	• 158.69.222.101
	bymJNhzejq.dll	Get hash	malicious	Browse	• 158.69.222.101
	DOC_1003394276473336675207.docm	Get hash	malicious	Browse	• 158.69.222.101
	Pending Invoice 38129337.exe	Get hash	malicious	Browse	• 54.38.220.85
	File#BOL.exe	Get hash	malicious	Browse	• 51.83.52.225
	60039DF63E861FBDABF05185173E4A6937A8813A9C499.exe	Get hash	malicious	Browse	• 66.70.218.54
	Report.docm	Get hash	malicious	Browse	• 158.69.222.101
	CyNu4YFki4.dll	Get hash	malicious	Browse	• 158.69.222.101

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Program Files (x86)\Security\important invoice presentation nov 2021.exe

Process:	C:\Windows\SysWOW64\xcopy.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	3391296
Entropy (8bit):	6.764334303023271
Encrypted:	false
SSDEEP:	98304:s1zCQ5fFa1BJLhjtX5yI3FwzLhYsJLIy38X79Tg:s1zCesBPny2y38X79T
MD5:	1364844E0BFB349272C5050FB0E677E3
SHA1:	FFC57AD66C9A3764A88A2B2C3EC1F0F19042C77A
SHA-256:	004F011B37E4446FA04B76AAE537CC00F6588C0705839152AE2D8A837EF2B730
SHA-512:	82AD807D0AE5D34D49A9DE38F02BA5096BF4B80DF8A58F1E9F2FF9FA53AE04B3B58C584CD19E62B996D63FE4E3FE1B1FDCC6C5C7433FBA7A07D19D4103EE8D3
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....2..v..v..v..b..j..b..W..b.....e.....o.....b..t..b..S..v..~....~.....w....w..Richv.....PE..L....q.a.....".....N.....".....@.....4.....3...@.....).|.....+..O.....3.@)....1. ....'.....'.....'.@.....".h.....text...."....."..... ..`.rdata..8K...".L...".....@..@.data.....0*..2...*.....@....rsrc....O....+..P...N+.....@..@.reloc.. .....1.....0.....@..B.....

C:\Program Files (x86)\Security\important invoice presentation nov 2021.exe:Zone.Identifier

Process:	C:\Windows\SysWOW64\xcopy.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64

C:\Program Files (x86)\Security\important invoice presentation nov 2021.exe:Zone.Identifier	
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.764334303023271
TrID:	• Win32 Executable (generic) a (10002005/4) 98.81% • Windows ActiveX control (116523/4) 1.15% • 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:	important invoice presentation nov 2021.exe
File size:	3391296
MD5:	1364844e0bfb349272c5050fb0e677e3
SHA1:	ffc57ad66c9a3764a88a2b2c3ec1f0f19042c77a
SHA256:	004f011b37e4446fa04b76aae537cc00f6588c0705839152ae2d8a837ef2b730
SHA512:	82ad807d0ae5d34d49a9de38f02ba5096bf4b80df8a58f1e9f2ff9fa53ae04b3b58c584cd19e62b996d63fe4e3fe1b1fdcc6c5c7433fba7a07d19d4103ee82d3
SSDEEP:	98304:s1zCQ5fFa1BJLhjtX5yI3FwzLhYsJLly38X79Tg:s1zCesBPny2y38X79T
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....2...v...v.....v...b...j...b...W...b.....e.....o.....b...t...b...S...v...~.....~.....w.....w...Richv.....

File Icon

Icon Hash:	69ab96a6a6dc6891

Static PE Info

General

Entrypoint:	0x5c944e
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x61907180 [Sun Nov 14 02:16:32 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	6
OS Version Minor:	0
File Version Major:	6
File Version Minor:	0
Subsystem Version Major:	6
Subsystem Version Minor:	0
Import Hash:	928ca23958b7b89682da5497b37038ac

Authenticode Signature

Signature Valid:	**true**

Signature Issuer:	CN=Sectigo Public Code Signing CA R36, O=Sectigo Limited, C=GB
Signature Validation Error:	**The operation completed successfully**
Error Number:	0
Not Before, Not After	• 11/11/2021 4:00:00 PM 11/12/2022 3:59:59 PM
Subject Chain	• CN=ULTRA ACADEMY LTD, O=ULTRA ACADEMY LTD, S=London, C=GB
Version:	3
Thumbprint MD5:	BCAF7BE878249CC7571201AE00B95303
Thumbprint SHA-1:	E94AD249747FD4B88750B2CD6D8D65AD33D3566D
Thumbprint SHA-256:	0D358ADC3623D52FBF1EC26ACAEBBEE7AFC73082276B60DE1FE51F59E4B4AEBC
Serial:	387EEB89B8BF626BBF4C7C9F5B998B40

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x22cac9	0x22cc00	unknown	unknown	unknown	unknown	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x22e000	0x74b38	0x74c00	False	0.342708612152	data	5.50911370588	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x2a3000	0x17f0c	0x13200	False	0.680695976307	data	7.16739114428	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rsrc	0x2bb000	0x54fdc	0x55000	False	0.794674862132	data	7.15845808893	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x310000	0x2f620	0x2f800	False	0.469078947368	data	6.58652778609	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, 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

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 17, 2021 14:34:01.496373892 CET	192.168.2.6	8.8.8.8	0xa048	Standard query (0)	calibare5454.pro	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 17, 2021 14:34:01.583832026 CET	8.8.8.8	192.168.2.6	0xa048	No error (0)	calibare54 54.pro		51.195.57.233	A (IP address)	IN (0x0001)
Nov 17, 2021 14:37:19.377098083 CET	8.8.8.8	192.168.2.6	0xdb66	No error (0)	prda.aadg. msidentity.com	www.tm.a.prd.aadg.trafficmanager.net		CNAME (Canonical name)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: important invoice presentation nov 2021.exe PID: 6968 Parent PID: 4240

General

Start time:	14:32:39
Start date:	17/11/2021
Path:	C:\Users\user\Desktop\important invoice presentation nov 2021.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\important invoice presentation nov 2021.exe"
Imagebase:	0x1250000
File size:	3391296 bytes
MD5 hash:	1364844E0BFB349272C5050FB0E677E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_NetWire_1, Description: Yara detected NetWire RAT, Source: 00000001.00000002.507835553.000000001C8F0000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: cmd.exe PID: 3576 Parent PID: 6968

General

Start time:	14:33:44
Start date:	17/11/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /c xcopy "C:\Users\user\Desktop\important invoice presentation nov 2021.exe" "%ProgramFiles%\Security\" /y /i /c /q
Imagebase:	0x2a0000
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: 5272 Parent PID: 3576

General

Start time:	14:33:45
Start date:	17/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: xcopy.exe PID: 6100 Parent PID: 3576

General

Start time:	14:33:46
Start date:	17/11/2021
Path:	C:\Windows\SysWOW64\xcopy.exe
Wow64 process (32bit):	true
Commandline:	xcopy "C:\Users\user\Desktop\important invoice presentation nov 2021.exe" "C:\Program Files (x86)\Security\" /y /i /c /q
Imagebase:	0x12c0000
File size:	44544 bytes
MD5 hash:	9F3712DDC0D7FE3D75B8A06C6EE8E68C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: cmd.exe PID: 5536 Parent PID: 6968

General

Start time:	14:33:49
Start date:	17/11/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /c schtasks /create /sc ONLOGON /tn "Security" /tr "%ProgramFiles%\Security\important invoice presentation nov 2021.exe" /it /f
Imagebase:	0x2a0000
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: 3168 Parent PID: 5536

General

Start time:	14:33:50
Start date:	17/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: schtasks.exe PID: 5660 Parent PID: 5536

General

Start time:	14:33:50
Start date:	17/11/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks /create /sc ONLOGON /tn "Security" /tr "C:\Program Files (x86)\Security\important invoice presentation nov 2021.exe" /it /f
Imagebase:	0xa10000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: important invoice presentation nov 2021.exe PID: 2872 Parent PID: 936

General

Start time:	14:33:51
Start date:	17/11/2021
Path:	C:\Program Files (x86)\Security\important invoice presentation nov 2021.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\Security\important invoice presentation nov 2021.exe
Imagebase:	0xb90000
File size:	3391296 bytes
MD5 hash:	1364844E0BFB349272C5050FB0E677E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_NetWire_1, Description: Yara detected NetWire RAT, Source: 0000000D.00000002.683551594.000000001CF00000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

Analysis Process: xwizard.exe PID: 5612 Parent PID: 6968

General

Start time:	14:33:51
Start date:	17/11/2021
Path:	C:\Windows\SysWOW64\xwizard.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\xwizard.exe
Imagebase:	0x11e0000
File size:	55808 bytes
MD5 hash:	17059CA3DDD41B52DE4140705B38AE53
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_NetWire_1, Description: Yara detected NetWire RAT, Source: 0000000E.00000002.863773731.0000000000422000.00000004.00020000.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: cmd.exe PID: 5704 Parent PID: 2872

General

Start time:	14:35:08
Start date:	17/11/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /c xcopy "C:\Program Files (x86)\Security\important invoice presentation nov 2021.exe" "%ProgramFiles%\Security\" /y /i /c /q
Imagebase:	0x2a0000
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: 3132 Parent PID: 5704

General

Start time:	14:35:09

Start date:	17/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: xcopy.exe PID: 4920 Parent PID: 5704

General

Start time:	14:35:10
Start date:	17/11/2021
Path:	C:\Windows\SysWOW64\xcopy.exe
Wow64 process (32bit):	true
Commandline:	xcopy "C:\Program Files (x86)\Security\important invoice presentation nov 2021.exe" "C:\Program Files (x86)\Security\" /y /i /c /q
Imagebase:	0x7ff7e33a0000
File size:	44544 bytes
MD5 hash:	9F3712DDC0D7FE3D75B8A06C6EE8E68C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 3032 Parent PID: 2872

General

Start time:	14:35:11
Start date:	17/11/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	cmd /c schtasks /create /sc ONLOGON /tn "Security" /tr "%ProgramFiles%\Security\important invoice presentation nov 2021.exe" /it /f
Imagebase:	0x2a0000
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: 4388 Parent PID: 3032

General

Start time:	14:35:12
Start date:	17/11/2021

Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: schtasks.exe PID: 2032 Parent PID: 3032

General

Start time:	14:35:12
Start date:	17/11/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	schtasks /create /sc ONLOGON /tn "Security" /tr "C:\Program Files (x86)\Security\important invoice presentation nov 2021.exe" /it /f
Imagebase:	0xa10000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities

Show Windows behavior

Analysis Process: xwizard.exe PID: 2040 Parent PID: 2872

General

Start time:	14:35:13
Start date:	17/11/2021
Path:	C:\Windows\SysWOW64\xwizard.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\xwizard.exe
Imagebase:	0x11e0000
File size:	55808 bytes
MD5 hash:	17059CA3DDD41B52DE4140705B38AE53
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_NetWire_1, Description: Yara detected NetWire RAT, Source: 0000001E.00000002.688394318.0000000000422000.00000004.00020000.sdmp, Author: Joe Security • Rule: netwire, Description: detect netwire in memory, Source: 0000001E.00000002.688394318.0000000000422000.00000004.00020000.sdmp, Author: JPCERT/CC Incident Response Group

Disassembly

Code Analysis