ID: 501991
Sample Name: iAuPyHuUkk
Cookbook: default.jbs
Time: 13:36:28
Date: 13/10/2021
Version: 33.0.0 White Diamond

Table of Contents

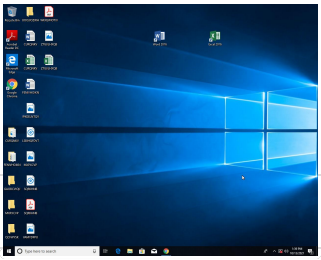
Windows Analysis Report iAuPyHuUkk

Overview

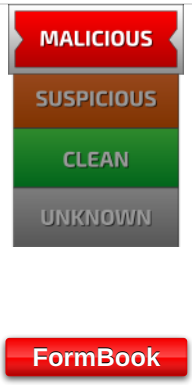
General Information

Sample Name:	iAuPyHuUkk (renamed file extension from none to exe)
Analysis ID:	501991
MD5:	6040407905ea1a..
SHA1:	96ecf27fd10a666..
SHA256:	2f2831bdecd1f92..
Tags:	32 exe trojan
Infos:	

Most interesting Screenshot:



Detection



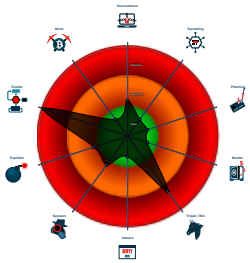
FormBook

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 …
- Yara detected AntiVM3
- 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 detect sandboxes and other…
- Self deletion via cmd delete

Classification



Process Tree

- **System is w10x64**
- iAuPyHuUkk.exe (PID: 476 cmdline: 'C:\Users\user\Desktop\iAuPyHuUkk.exe' MD5: 6040407905EA1AA24DD58DC8BEFA4255)
  - iAuPyHuUkk.exe (PID: 6968 cmdline: C:\Users\user\Desktop\iAuPyHuUkk.exe MD5: 6040407905EA1AA24DD58DC8BEFA4255)
    - explorer.exe (PID: 3440 cmdline: C:\Windows\Explorer.EXE MD5: AD5296B280E8F522A8A897C96BAB0E1D)
      - autofmt.exe (PID: 5980 cmdline: C:\Windows\SysWOW64\autofmt.exe MD5: 7FC345F685C2A58283872D851316ACC4)
      - control.exe (PID: 3540 cmdline: C:\Windows\SysWOW64\control.exe MD5: 40FBA3FBFD5E33E0DE1BA45472FDA66F)
        - cmd.exe (PID: 4432 cmdline: /c del 'C:\Users\user\Desktop\iAuPyHuUkk.exe' MD5: F3BDBE3BB6F734E357235F4D5898582D)
          - conhost.exe (PID: 5900 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.aliexpress-br.com/mexq/"
  ],
  "decoy": [
    "cyebang.com",
    "hcswwsz.com",
    "50003008.com",
    "yfly624.xyz",
    "trungtamhohap.xyz",
    "sotlbb.com",
    "bizhan69.com",
    "brandmty.net",
    "fucibou.xyz",
    "orderinformantmailer.store",
    "nobleminers.com",
    "divinevoid.com",
    "quickappraisal.net",
    "adventuretravelsworld.com",
    "ashainitiativemp.com",
    "ikkbs-a02.com",
    "rd26x.com",
    "goraeda.com",
    "abbastanza.info",
    "andypartridge.photography",
    "xn--aprendes-espaol-brb.com",
    "jrceleste.com",
    "bestwarsawhotels.com",
    "fospine.online",
    "rayofdesign.online",
    "hablamarca.com",
    "nichellejonesrealtor.com",
    "zamarasystem.com",
    "thepropertygoat.com",
    "fightfigures.com",
    "mxconglomerate.com",
    "elecoder.com",
    "mabnapakhsh.com",
    "girlspiter.club",
    "xn--lcka2cufqed6765c4ef1x1g.xyz",
    "cancleaningpros.com",
    "galestorm.net",
    "besrbee.com",
    "sjmdesignstudio.com",
    "kickonlines.com",
    "generateyourart.com",
    "promiseface.com",
    "searchingspacespot.com",
    "jovemmilionario.com",
    "paomovar.com",
    "dogiadunggiare.online",
    "uniqued.net",
    "glassrootsstudio.com",
    "rabenteec.com",
    "asistente-ti.com",
    "xn--l6qw76agwi5rjeuzk9q.com",
    "azapsolutions.com",
    "wmh3gk2fzw2m.biz",
    "districonio.com",
    "dapekdelivery.com",
    "vintagepaseo.com",
    "od0aew1pox.com",
    "iphone13promax.design",
    "texttheruffleddaisy.com",
    "umdasch-lagertechnik.com",
    "growthabove.com",
    "eltacorancherofoodtruck.com",
    "gafoodstamps.com",
    "mzalluom.com"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000D.00000002.619163959.0000000002FE0000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
0000000D.00000002.619163959.0000000002FE0000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
0000000D.00000002.619163959.0000000002FE0000.00000040.00020000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ae9:$sqlite3step: 68 34 1C 7B E1 • 0x16bfc:$sqlite3step: 68 34 1C 7B E1 • 0x16b18:$sqlite3text: 68 38 2A 90 C5 • 0x16c3d:$sqlite3text: 68 38 2A 90 C5 • 0x16b2b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c53:$sqlite3blob: 68 53 D8 7F 8C
00000003.00000002.455602320.0000000001930000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000003.00000002.455602320.0000000001930000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 25 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
3.2.iAuPyHuUkk.exe.400000.0.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
3.2.iAuPyHuUkk.exe.400000.0.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8618:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89b2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146c5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141b1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147c7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1493f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ca:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1342c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa142:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19bb7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
3.2.iAuPyHuUkk.exe.400000.0.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ae9:$sqlite3step: 68 34 1C 7B E1 • 0x16bfc:$sqlite3step: 68 34 1C 7B E1 • 0x16b18:$sqlite3text: 68 38 2A 90 C5 • 0x16c3d:$sqlite3text: 68 38 2A 90 C5 • 0x16b2b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c53:$sqlite3blob: 68 53 D8 7F 8C
0.2.iAuPyHuUkk.exe.33e3150.1.raw.unpack	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
3.2.iAuPyHuUkk.exe.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
Click to see the 6 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

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

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:

- .NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

- Self deletion via cmd delete

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
- Queues an APC in another process (thread injection)
- Modifies the context of a thread in another process (thread injection)

Stealing of Sensitive Information:

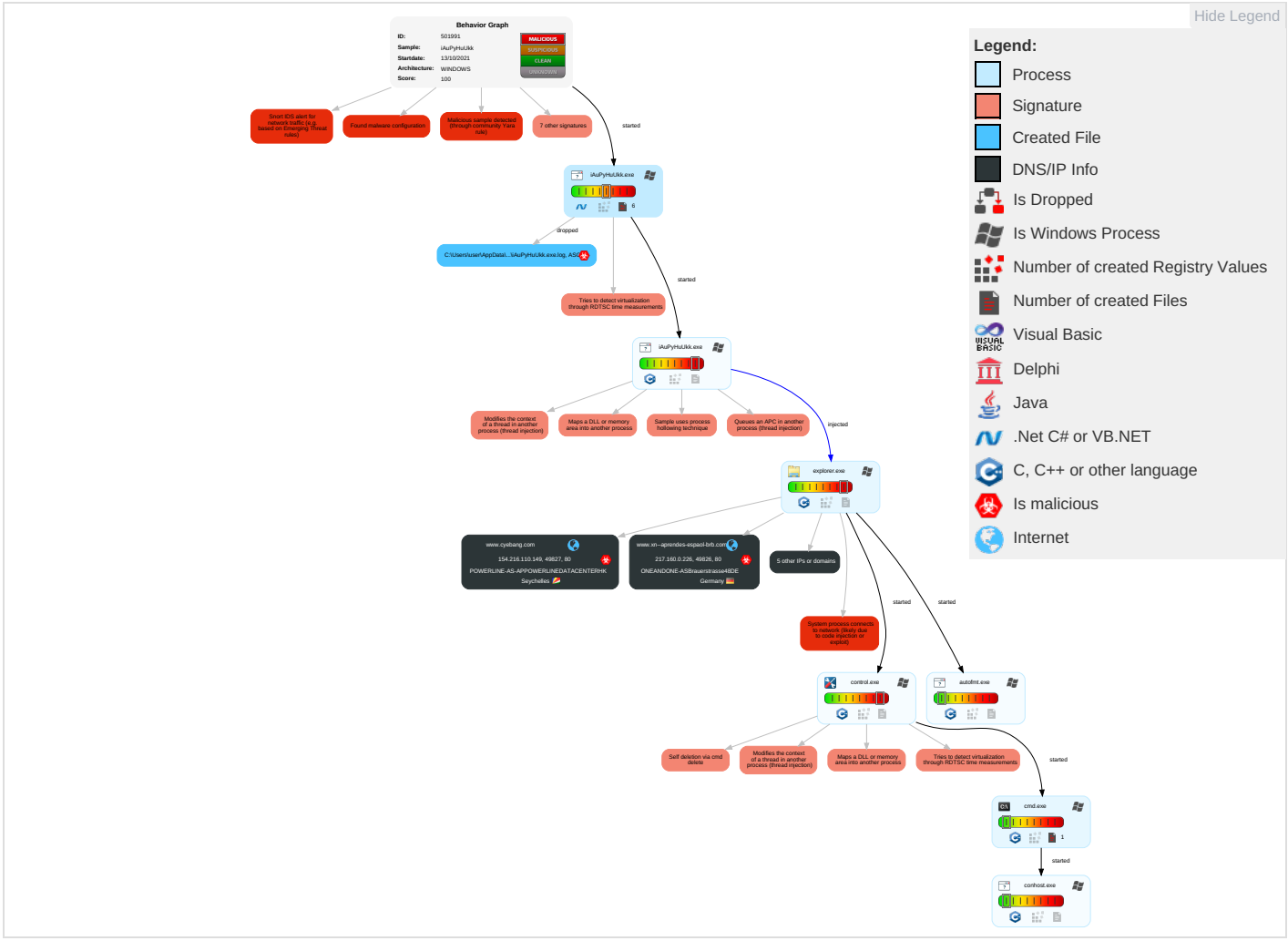
- Yara detected FormBook

Remote Access Functionality:

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 5 1 2	Masquerading 1	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	Process Discovery 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)	Virtualization/Sandbox Evasion 3 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	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 5 1 2	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 3	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 1 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

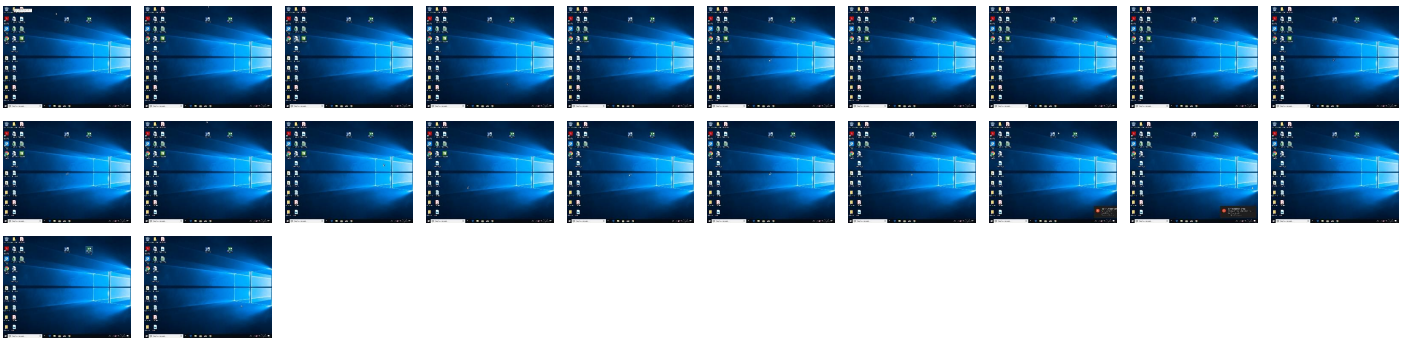
Behavior Graph



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
iAuPyHuUkk.exe	15%	ReversingLabs		

Dropped Files

No Antivirus matches

Unpacked PE Files

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

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://i4.cdn-image.com/__media__/pics/27586/searchbtn.png)	0%	Avira URL Cloud	safe	
http://i4.cdn-image.com/__media__/fonts/open-sans/open-sans.svg#open-sans	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://i4.cdn-image.com/__media__/fonts/open-sans/open-sans.woff	0%	Avira URL Cloud	safe	
http://www.vintagepaseo.com/display.cfm	0%	Avira URL Cloud	safe	
http://i4.cdn-image.com/__media__/pics/27587/Left.png)	0%	Avira URL Cloud	safe	
http://i4.cdn-image.com/__media__/fonts/open-sans/open-sans.eot	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp//e	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.cyebang.com/mexq/?e66HNDO=g6L0/Z2eA1jwRGo1l6rXBhzWGtzMcF3Ol1vrZIbNMV/6CHuR9YyStXwolwULrpYmw34wy4pkGQ==&6lux=TrTPmvux5	100%	Avira URL Cloud	malware	
http://i4.cdn-image.com/__media__/pics/27587/Right.png)	0%	Avira URL Cloud	safe	
http://www.collada.org/2005/11/COLLADASchema9Done	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.zhongyicts.com.cnava	0%	Avira URL Cloud	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://i4.cdn-image.com/__media__/fonts/open-sans-bold/open-sans-bold.woff2	0%	Avira URL Cloud	safe	
http://www.ascendercorp.com/typedesigners.html9	0%	Avira URL Cloud	safe	
http://i4.cdn-image.com/__media__/fonts/open-sans-bold/open-sans-bold.eot	0%	Avira URL Cloud	safe	
http://www.carterandcone.com8	0%	URL Reputation	safe	
http://i4.cdn-image.com/__media__/fonts/open-sans/open-sans.otf	0%	Avira URL Cloud	safe	
http://i4.cdn-image.com/__media__/pics/468/netsol-favicon-2020.jpg	0%	Avira URL Cloud	safe	
http://i4.cdn-image.com/__media__/fonts/open-sans-bold/open-sans-bold.otf	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.fontbureau.comgrito	0%	URL Reputation	safe	
http://i4.cdn-image.com/__media__/fonts/open-sans-bold/open-sans-bold.eot?#iefix	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://i4.cdn-image.com/__media__/pics/27587/BG_2.png)	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.vintagepaseo.com/All_Inclusive_Vacation_Packages.cfm?fp=DaDrTtodEbKG7H0GzLA3PtWLrM%2BdgeV	0%	Avira URL Cloud	safe	
http://i4.cdn-image.com/__media__/fonts/open-sans-bold/open-sans-bold.svg#open-sans-bold	0%	Avira URL Cloud	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.vintagepaseo.com/__media__/design/underconstructionnotice.php?d=vintagepaseo.com	0%	Avira URL Cloud	safe	
http://www.vintagepaseo.com/mexq/?e66HNDO=NdiAijP1TUDTbxv	0%	Avira URL Cloud	safe	
http://www.carterandcone.como.Z	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.carterandcone.como.N	0%	Avira URL Cloud	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.vintagepaseo.com/__media__/js/trademark.php?d=vintagepaseo.com&type=ns	0%	Avira URL Cloud	safe	
http://www.vintagepaseo.com/mexq/?e66HNDO=NdiAijP1TUDTbxv+UVf96WWBcfe2HF0RhGf6TXdRPwqQZT7SHaZsoP4NORlVjEEjxsHi13Lz5g==&6lux=TrTPmvux5	0%	Avira URL Cloud	safe	
http://www.vintagepaseo.com/Migraine_Pain_Relief.cfm?fp=DaDrTtodEbKG7H0GzLA3PtWLrM%2BdgeVzyxLURkW8zf	0%	Avira URL Cloud	safe	
http://i4.cdn-image.com/__media__/fonts/open-sans/open-sans.woff2	0%	Avira URL Cloud	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://www.vintagepaseo.com/Top_10_Luxury_Cars.cfm?fp=DaDrTtodEbKG7H0GzLA3PtWLrM%2BdgeVzyxLURkW8zfJI	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://i4.cdn-image.com/__media__/fonts/open-sans-bold/open-sans-bold.woff	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://i4.cdn-image.com/__media__/pics/10667/netsol-logos-2020-165-50.jpg	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn7	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/ico	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://i4.cdn-image.com/__media__/fonts/open-sans/open-sans.ttf	0%	Avira URL Cloud	safe	
http://i4.cdn-image.com/__media__/js/min.js?v2.3	0%	Avira URL Cloud	safe	
http://www.Vintagepaseo.com	0%	Avira URL Cloud	safe	

Source	Detection	Scanner	Label	Link
http://www.vintagepaseo.com/Work_from_Home.cfm?fp=DaDrTtodEbKG7H0GzLA3PtWLrM%2BdgeVzyxLURkW8zfJIpKi%	0%	Avira URL Cloud	safe	
http://i4.cdn-image.com/__media__/fonts/open-sans-bold/open-sans-bold.ttf	0%	Avira URL Cloud	safe	
http://www.tiro.comc	0%	URL Reputation	safe	
http://www.vintagepaseo.com/Credit_Card_Application.cfm?fp=DaDrTtodEbKG7H0GzLA3PtWLrM%2BdgeVzyxLURkW	0%	Avira URL Cloud	safe	
http://www.xn--aprendes-espaol-brb.com/mexq/?e66HNDO=aPMuX7G1Ot9XJXghMAabXwwkzBWzprGcmmQ5cfrgMP5E/C43hf1Uz5bqYekFv+cUss1JtU0p5g==&6lux=TrTPmvux5	0%	Avira URL Cloud	safe	
http://i4.cdn-image.com/__media__/fonts/open-sans/open-sans.eot?#iefix	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
www.vintagepaseo.com	208.91.197.27	true	true		unknown
windowsupdate.s.llnwi.net	178.79.242.0	true	false		unknown
www.cyebang.com	154.216.110.149	true	true		unknown
www.xn--aprendes-espaol-brb.com	217.160.0.226	true	true		unknown
www.brandmty.net	unknown	unknown	true		unknown
www.districonio.com	unknown	unknown	true		unknown
www.iphone13promax.design	unknown	unknown	true		unknown
www.umdasch-lagertechnik.com	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://www.cyebang.com/mexq/?e66HNDO=g6L0/Z2eA1jwRGo1l6rXBhzWGtzMcF3Ol1vrZIbNMV/6CHuR9YyStXwolwULrpYmw34wy4pkGQ==&6lux=TrTPmvux5	true	• Avira URL Cloud: malware	unknown
http://www.vintagepaseo.com/mexq/?e66HNDO=NdiAijP1TUDTbxv+UVf96WWBcfe2HF0RhGf6TXdRPwqQZT7SHaZsoP4NORlVjEEjxsHi13Lz5g==&6lux=TrTPmvux5	true	• Avira URL Cloud: safe	unknown
http://www.xn--aprendes-espaol-brb.com/mexq/?e66HNDO=aPMuX7G1Ot9XJXghMAabXwwkzBWzprGcmmQ5cfrgMP5E/C43hf1Uz5bqYekFv+cUss1JtU0p5g==&6lux=TrTPmvux5	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
217.160.0.226	www.xn--aprendes-espaol-brb.com	Germany		8560	ONEANDONE-ASBrauerstrasse48DE	true
154.216.110.149	www.cyebang.com	Seychelles		132839	POWERLINE-AS-APPOWERLINEDATACENTERHK	true
208.91.197.27	www.vintagepaseo.com	Virgin Islands (BRITISH)		40034	CONFLUENCE-NETWORK-INCVG	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	501991
Start date:	13.10.2021
Start time:	13:36:28
Joe Sandbox Product:	CloudBasic

Overall analysis duration:	0h 11m 9s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	iAuPyHuUkk (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@8/1@8/3
EGA Information:	Failed
HDC Information:	• Successful, ratio: 26.8% (good quality ratio 24.7%) • Quality average: 69.8% • Quality standard deviation: 31.6%
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

Simulations

Behavior and APIs

Time	Type	Description
13:37:36	API Interceptor	1x Sleep call for process: iAuPyHuUkk.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
217.160.0.226	vURlUPQLT0.exe	Get hash	malicious	Browse	• www.xn--aprendes-espaol-brb.com/mexq/?4h=0bnTL8qh9&h8yxlz-=aPMuX7G1Ot9XJXghMAabXwwkzBWzprGcmmQ5cfrgMP5E/C43hf1Uz5bqYeoF8uQX181f

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
208.91.197.27	wDzceoRPhB.exe	Get hash	malicious	Browse	• www.vaughnmethod.com/ed9s/?j6A=cMgc34DI6EHgRBPPCU1upM8r6W5gmyFdUZ6BCP+wlJ0AAQ+v0J4fB8uzS/jKj/yu2Uo5&2d64u=GZS0ntMXED7DC
	etiyrflKft.exe	Get hash	malicious	Browse	• www.weprepareamerica-world.com/n092/?h0Gdj4dh=7QNXrpC+0zTYuDSJvYtcqWvwaJpzyS75Y6CJpFMcqskYdcMJUPnJbkzMB91F/535v440&1bkX=KN9l7
	INVPRF2100114_pdf.exe	Get hash	malicious	Browse	• www.youroutcs.com/euzn/?vPAl-=CR-TLLc&5j=Jq5AABYnwO9dbv77N4nPQwsgHB5GKQbjMYkkdBpcGmLbEHlDRj4+NcKZLwDv+32oOSRS
	PkF9Fg2Tnc.exe	Get hash	malicious	Browse	• www.thymoscorp.com/n092/?Cptd5=T476+wLEZakNnatpzDgnd+i8GD3CeHIKKZKbWkLuO1H4v0vGZa8Ua7CXK/8Rlqil4H1a&y4=7n3dvv
	2WK7SGkGVZ.exe	Get hash	malicious	Browse	• www.andrewfjohnston.com/b2c0/?1bV=j6ATrf&7nlpd=nPJDWeDX3x/7yoIb4Y8ACYvoKxwYoowpnQPys4jm4E2BXf8WUJ1hnsC1S/FzrgAx/9vb
	NEW ORDER INQUIRY_Q091421.PDF.exe	Get hash	malicious	Browse	• www.barrier-to-entry.com/h5jc/?8pW=UAgdrLYBEBHnZD6vumMuWShxuTvQQAMT+4FDgagiYMIIlUmoqNFKWavZLlig6d0hZcfT&1bE8p=8p04q8mHnH
	ugsuHxq7Ey.exe	Get hash	malicious	Browse	• www.weprepareamerica-world.com/n092/?UL=7QNXrpC+0zTYuDSJvYtcqWvwaJpzyS75Y6CJpFMcqskYdcMJUPnJbkzMB91vgJH5r6w0&rP=4hOh3

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	DHL_Online_Receipt.doc	Get hash	malicious	Browse	• www.getrichadams.com/c3hy/?yfL8-tq0=+C97xekWOCtRqspsnKWJgGOuAPiwQzy0YYswFyxb/tYUxnF7+gywk2v6MOtw6eF1FCkoSQ==&f6A8=dxo0srcx
	m2F8C6rz9J.exe	Get hash	malicious	Browse	• www.yesterdaystomorrownow.com/zizv/?FL0lxhs=tq18rE4QkgIvfNIpkqEMdP/7PcSlbVRZ9TDCQpLEuCwXiE5u+3jx/eVPwHHQIFKJLFE+&1bT8s=1bbhp0_P
	AWB.doc	Get hash	malicious	Browse	• www.shans-online.com/fzsg/?i2M8mbL8=wYA5+ODQw7YIFkSefVPDQdsb1XpS7kW79pgoTMk5mjoxU7vP2T6by19X6tBJuHEX3lcOtQ==&X6A=bTMtXz7XNfKd
	SOA.exe	Get hash	malicious	Browse	• www.andrewfjohnston.com/b2c0/?3ff=y6AT2b&m4C=nPJDWeDSq27+w4JhkI8ACYvoKxwYoowpnQPys4jm4E2BXf8WUJ1hnsC1S8FsokkK/+Kf
	HBW PAYMENT LIST FOR 2021,20212009.xlsx	Get hash	malicious	Browse	• www.hivizpeople.com/n092/?ixl0i0t=uaY0THpty5EvCloUtnm06lpodfUxh6yq2Ukbc245yKA9WepW8xtBavSpPmKwlutgZVJfqg==&kb=-Z4LWJsPDRiPHr
	77dsREO8Me.exe	Get hash	malicious	Browse	• www.youroutcs.com/euzn/?6lDh4=Jq5AABYnwO9dbv77N4nPQwsgHB5GKQbjMYkkdBpcGmLbEHlDRj4+NcKZLwDFhHGoKQZS&Ph-PB=1bpljFA
	Sales _DEG212004755711421641.pdf.exe	Get hash	malicious	Browse	• www.traveladvisorsuccess.net/gs2m/?8pHX=5jhxgd&h4=R9Myd3XtH8UfpLcxkW7UMZG2K+ZHkiBKmQ+KXW7xNpgHOl826W3TGb5gliCaUB40A9/Y

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	3xzHrbPdZ7.exe	Get hash	malicious	Browse	• vpn.premrera.com:443/viewpre.asp?cstring=wcxbaa-1753643374&tom=255&id=6003031
	VINASHIP STAR.xlsx	Get hash	malicious	Browse	• www.cpb.site/nthe/?xtxh=21tMkqEIUZBUKU+ck7CVVp3eTiqf/+4cN27Pgp5ejfxv1jbsXk06Rfkh8MQLsUSEnTHARw==&U2=mv-t_rDPAPsD6l
	MV TAICHUNG.xlsx	Get hash	malicious	Browse	• www.cpb.site/nthe/?7nMt=21tMkqEIUZBUKU+ck7CVVp3eTiqf/+4cN27Pgp5ejfxv1jbsXk06Rfkh8MQLsUSEnTHARw==&gDHho=b2JPovgHUt
	BIN.exe	Get hash	malicious	Browse	• www.jwpropertiestn.com/n8ba/?I6El7rEX=iMNnVuY+gvXz0j53tPU+imZoGlggyOcz8e4ohSepbhwGfYAQxyq22Rg/4FGnobgDSPq5&yBZ02=2df8xb-H6hatkZkp
	OrdGreece89244.exe	Get hash	malicious	Browse	• www.carstoriesusa.net/rvoe/?q6pHq=L4-hsduP_n0dm&5jn=fAOs8VWxDgCcN/b38ZjPEpzSltT9i6eUIfWB05FDSs6jml76oEIdxB/bsn2NMp244tD1hAXsWQ==
	REMMITANCE COPY.exe	Get hash	malicious	Browse	• www.lovefromnewyork.com/kmb0/?H6JHLVy=kV+lEXg8yEf0RijPwLmsZpVBvRfnl4wggG07Ng5Cei2p8cSyeu82h3Ryg2Q6rnDNHAltvCyP6Q==&r48XKx=9rAHYr10f

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
www.xn--aprendes-espaol-brb.com	XaTgTJhfol.exe	Get hash	malicious	Browse	• 217.160.0.226
	vURlUPQLT0.exe	Get hash	malicious	Browse	• 217.160.0.226
windowsupdate.s.llnwi.net	ORDER CONFIRMATION.exe	Get hash	malicious	Browse	• 178.79.242.128
	HqiJ8HpbxU.exe	Get hash	malicious	Browse	• 178.79.242.0
	PEKv5PX7Wq.exe	Get hash	malicious	Browse	• 178.79.242.0
	R6QyqCNJgljVTjY.exe	Get hash	malicious	Browse	• 178.79.242.0
	SsbgfSoVLC.exe	Get hash	malicious	Browse	• 178.79.242.0
	pvHBhNUyIm.exe	Get hash	malicious	Browse	• 178.79.242.0

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Request For New Qoute - Ist Order.exe	Get hash	malicious	Browse	• 178.79.242.0
	569vj51Zrs.exe	Get hash	malicious	Browse	• 178.79.242.0
	correction HAWB.exe	Get hash	malicious	Browse	• 178.79.242.0
	correction HAWB.exe	Get hash	malicious	Browse	• 178.79.242.0
	Statement of Account.exe	Get hash	malicious	Browse	• 178.79.242.128
	Statement of Account.exe	Get hash	malicious	Browse	• 178.79.242.128
	jh6KzwrXQp.exe	Get hash	malicious	Browse	• 178.79.242.0
	heX1kOkwqy.exe	Get hash	malicious	Browse	• 178.79.242.0
	mixsix_20211013-084409.exe	Get hash	malicious	Browse	• 178.79.242.0
	2rd Quater Order Quotation.zip.xls	Get hash	malicious	Browse	• 178.79.242.128
	DOC REC EIPT.html	Get hash	malicious	Browse	• 178.79.242.128
	Efe-8 GPP Project Steel Pipe Tender.exe	Get hash	malicious	Browse	• 178.79.242.128
	emil.franchi@global.com #Ud83d#Udce0 VGX47BBSBJ44838.HTM	Get hash	malicious	Browse	• 178.79.242.128
	DHL Lieferschein,pdf.exe	Get hash	malicious	Browse	• 178.79.242.128

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
POWERLINE-AS-APPOWERLINEDATACENTERHK	x86	Get hash	malicious	Browse	• 154.92.66.213
	4SkZvkMy6J	Get hash	malicious	Browse	• 45.205.161.234
	jIIPdrw41a	Get hash	malicious	Browse	• 156.242.206.51
	Lv9eznkydx.exe	Get hash	malicious	Browse	• 156.242.193.106
	yir8ieZzXL	Get hash	malicious	Browse	• 156.242.206.31
	UpsxN0u4wi	Get hash	malicious	Browse	• 156.243.213.52
	7ylx6ZIBpI	Get hash	malicious	Browse	• 154.203.73.118
	4uSa8tiph0	Get hash	malicious	Browse	• 45.205.161.238
	D_13567899.exe	Get hash	malicious	Browse	• 156.250.197.5
	Y76514IzYh	Get hash	malicious	Browse	• 160.124.153.91
	RZo4KTtZbb	Get hash	malicious	Browse	• 156.251.7.181
	Oq1I3DGMP8	Get hash	malicious	Browse	• 156.242.159.6
	46gV91KJhQ	Get hash	malicious	Browse	• 156.244.234.135
	RaVPWTArgG	Get hash	malicious	Browse	• 156.242.159.3
	ZFb3RmLJzo	Get hash	malicious	Browse	• 156.244.234.133
	vHLDOsbYKA	Get hash	malicious	Browse	• 156.242.206.52
	T5BjNBDzJa	Get hash	malicious	Browse	• 156.252.64.214
	hnBBQPVGVR	Get hash	malicious	Browse	• 154.209.59.237
	55bUuUSd6j	Get hash	malicious	Browse	• 156.242.30.39
	tI0W00k1vt	Get hash	malicious	Browse	• 156.251.3.6
ONEANDONE-ASBrauerstrasse48DE	vbc.exe	Get hash	malicious	Browse	• 217.160.0.17
	justificante de la transfer.exe	Get hash	malicious	Browse	• 212.227.15.158
	vURlUPQLT0.exe	Get hash	malicious	Browse	• 74.208.236.170
	82051082.exe	Get hash	malicious	Browse	• 213.171.195.105
	8205108.exe	Get hash	malicious	Browse	• 74.208.236.156
	Lv9eznkydx.exe	Get hash	malicious	Browse	• 217.160.0.238
	c9.dll	Get hash	malicious	Browse	• 87.106.18.141
	2e.dll	Get hash	malicious	Browse	• 87.106.18.141
	a3.exe	Get hash	malicious	Browse	• 87.106.18.141
	a04.dll	Get hash	malicious	Browse	• 87.106.18.141
	50.dll	Get hash	malicious	Browse	• 87.106.18.141
	Quote -0071021.exe	Get hash	malicious	Browse	• 217.160.0.7
	DHL SHIPMENT.HTML	Get hash	malicious	Browse	• 217.160.0.196
	hwIILTIn0n.exe	Get hash	malicious	Browse	• 217.160.0.17
	just.exe	Get hash	malicious	Browse	• 212.227.15.158
	2WK7SGkGVZ.exe	Get hash	malicious	Browse	• 74.208.236.156
	0n1pEFuGKC.exe	Get hash	malicious	Browse	• 74.208.236.145
	VmbABLKNbD.exe	Get hash	malicious	Browse	• 74.208.236.108
	Update-KB250-x86.exe	Get hash	malicious	Browse	• 74.208.5.20
	Update-KB2984-x86.exe	Get hash	malicious	Browse	• 74.208.5.20

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\iAuPyHuUkk.exe.log	
Process:	C:\Users\user\Desktop\iAuPyHuUkk.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1308
Entropy (8bit):	5.348115897127242
Encrypted:	false
SSDEEP:	24:MLUE4KJXE4qpE4Ks2E1qE4qpAE4Kzr7RKDE4KhK3VZ9pKhPKIE4oKFKHKorE4x88:MIHKtH2HKXE1qHmAHKzvRYHKhQnoPtH2
MD5:	832D6A22CE7798D72609B9C21B4AF152
SHA1:	B086DE927BFEE6039F5555CE53C397D1E59B4CA4
SHA-256:	9E5EE72EF293C66406AF155572BF3B0CF9DA09CC1F60ED6524AAFD65553CE551
SHA-512:	A1A70F76B98C2478830AE737B4F12507D859365F046C5A415E1EBE3D87FFD2B64663A31E1E5142F7C3A7FE9A6A9CB8C143C2E16E94C3DD6041D1CCABEDDD2C21
Malicious:	**true**
Reputation:	low
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..2,"System.Deployment, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21e8e2b95c\System.Xml.ni.dll",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.507453805098472
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:	iAuPyHuUkk.exe
File size:	698880
MD5:	6040407905ea1aa24dd58dc8befa4255
SHA1:	96ecf27fd10a6663cbfaadb7643abeaf4061ea77
SHA256:	2f2831bdecd1f925134fd944fc57f84b76ffe872e01c66f3662f1f9194a4b362
SHA512:	d16e31ae6f510ab9f2f2474c064781c15e666f871a969f394f3e6590c7c1dabf19a98c62866e0342d4e6ec9cb40ab2f036c0d687c92f34df7527c340dae923f2
SSDEEP:	12288:hSBIB+gqzVl16yDr67jAkWoDq5jAyWb3PnB5JRU/V18H:sBVVmEJaqdAtj/RRGV
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....fa.....0..... ... .@.. .....@.....

File Icon

Icon Hash:	d6e0ececc8e8f4cc

Static PE Info

General

Entrypoint:	0x481a8a
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:	0x61668406 [Wed Oct 13 07:00:22 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	0x7fa90	0x7fc00	False	0.915104039261	data	7.86255981519	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x82000	0x2a838	0x2aa00	False	0.18847369868	data	5.44795610818	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xae000	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

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
10/13/21-13:39:27.811719	ICMP	402	ICMP Destination Unreachable Port Unreachable			192.168.2.6	8.8.8.8
10/13/21-13:39:28.079722	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49827	80	192.168.2.6	154.216.110.149
10/13/21-13:39:28.079722	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49827	80	192.168.2.6	154.216.110.149
10/13/21-13:39:28.079722	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49827	80	192.168.2.6	154.216.110.149

Network Port Distribution

TCP Packets

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 13, 2021 13:39:00.196365118 CEST	192.168.2.6	8.8.8.8	0x6a87	Standard query (0)	www.iphone 13promax.design	A (IP address)	IN (0x0001)
Oct 13, 2021 13:39:05.286163092 CEST	192.168.2.6	8.8.8.8	0x69e9	Standard query (0)	www.vintag epaseo.com	A (IP address)	IN (0x0001)
Oct 13, 2021 13:39:11.041781902 CEST	192.168.2.6	8.8.8.8	0x9cd5	Standard query (0)	www.brandm ty.net	A (IP address)	IN (0x0001)
Oct 13, 2021 13:39:16.125418901 CEST	192.168.2.6	8.8.8.8	0xda7	Standard query (0)	www.xn--ap rendes-espaol-brb.com	A (IP address)	IN (0x0001)
Oct 13, 2021 13:39:21.413523912 CEST	192.168.2.6	8.8.8.8	0x1561	Standard query (0)	www.distri conio.com	A (IP address)	IN (0x0001)
Oct 13, 2021 13:39:26.461357117 CEST	192.168.2.6	8.8.8.8	0x9ea6	Standard query (0)	www.cyeban g.com	A (IP address)	IN (0x0001)
Oct 13, 2021 13:39:27.473282099 CEST	192.168.2.6	8.8.8.8	0x9ea6	Standard query (0)	www.cyeban g.com	A (IP address)	IN (0x0001)
Oct 13, 2021 13:39:33.414989948 CEST	192.168.2.6	8.8.8.8	0x18ce	Standard query (0)	www.umdasch-lagertechnik.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 13, 2021 13:38:13.648951054 CEST	8.8.8.8	192.168.2.6	0x17ae	No error (0)	windowsupd ate.s.llnwi.net		178.79.242.0	A (IP address)	IN (0x0001)
Oct 13, 2021 13:39:00.275882006 CEST	8.8.8.8	192.168.2.6	0x6a87	Server failure (2)	www.iphone 13promax.design	none	none	A (IP address)	IN (0x0001)
Oct 13, 2021 13:39:05.422707081 CEST	8.8.8.8	192.168.2.6	0x69e9	No error (0)	www.vintag epaseo.com		208.91.197.27	A (IP address)	IN (0x0001)
Oct 13, 2021 13:39:11.082210064 CEST	8.8.8.8	192.168.2.6	0x9cd5	Name error (3)	www.brandm ty.net	none	none	A (IP address)	IN (0x0001)
Oct 13, 2021 13:39:16.155879974 CEST	8.8.8.8	192.168.2.6	0xda7	No error (0)	www.xn--ap rendes-espaol-brb.com		217.160.0.226	A (IP address)	IN (0x0001)
Oct 13, 2021 13:39:21.450542927 CEST	8.8.8.8	192.168.2.6	0x1561	Name error (3)	www.distri conio.com	none	none	A (IP address)	IN (0x0001)
Oct 13, 2021 13:39:27.798012018 CEST	8.8.8.8	192.168.2.6	0x9ea6	No error (0)	www.cyeban g.com		154.216.110.149	A (IP address)	IN (0x0001)
Oct 13, 2021 13:39:27.811642885 CEST	8.8.8.8	192.168.2.6	0x9ea6	No error (0)	www.cyeban g.com		154.216.110.149	A (IP address)	IN (0x0001)
Oct 13, 2021 13:39:33.463068962 CEST	8.8.8.8	192.168.2.6	0x18ce	Name error (3)	www.umdasch-lagertechnik.com	none	none	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.vintagepaseo.com
- www.xn--aprendes-espaol-brb.com
- www.cyebang.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.6	49805	208.91.197.27	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2021 13:39:05.577222109 CEST	6005	OUT	GET /mexq/?e66HNDO=NdiAijP1TUDTbxv+UVf96WWBcfe2HF0RhGf6TXdRPwqQZT7SHaZsoP4NORlVjEEjxsHi13Lz5g==&6lux=TrTPmvux5 HTTP/1.1 Host: www.vintagepaseo.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Oct 13, 2021 13:39:05.854733944 CEST	6006	IN	HTTP/1.1 200 OK Date: Wed, 13 Oct 2021 11:39:05 GMT Server: Apache Set-Cookie: vsid=917vr3816707456615690; expires=Mon, 12-Oct-2026 11:39:05 GMT; Max-Age=157680000; path=/; domain=www.vintagepaseo.com; HttpOnly X-Adblock-Key: MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAKX74ixpzVyXbJprcLfbH4psP4+L2entqri0lzh6pkAaXLPIcclv6DQBeJJjGFWrBIF6QMyFwXT5CCRyjS2penECAwEAAQ==_BvmoE1YFCm+tBN52SitLTqdTVO+b/MNnOMS6bzT4FdAriOe/RlkeAXaeSbohmAblVkfZ8kWSX7V6WunDyRriUQ== Keep-Alive: timeout=5, max=125 Connection: Keep-Alive Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Data Raw: 34 66 39 31 0d 0a 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 20 50 55 42 4c 49 43 20 22 2d 2f 2f 57 33 43 2f 2f 44 54 44 20 48 54 4d 4c 20 34 2e 30 31 2f 2f 45 4e 22 20 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 54 52 2f 68 74 6d 6c 34 2f 73 74 72 69 63 74 2e 64 74 64 22 3e 0d 0a 3c 68 74 6d 6c 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 77 33 2e 6f 72 67 2f 31 39 39 2f 78 68 74 6d 6c 22 20 64 61 74 61 2d 61 64 62 6c 6f 63 6b 6b 65 79 3d 22 4d 46 77 77 44 51 59 4a 4b 6f 5a 49 68 76 63 4e 41 51 45 42 42 51 41 44 53 77 41 77 53 41 4a 42 41 4b 58 37 34 69 78 70 7a 56 79 58 62 4a 70 72 63 4c 66 62 48 34 70 73 50 34 2b 4c 32 65 6e 74 71 72 69 30 6c 7a 68 36 70 6b 41 61 58 4c 50 49 63 63 6c 76 36 44 51 42 65 4a 4a 6a 47 46 57 72 42 49 46 36 51 4d 79 46 77 58 54 35 43 43 52 79 6a 53 32 70 65 6e 45 43 41 77 45 41 41 51 3d 3d 5f 42 76 6d 6f 45 31 59 46 43 6d 2b 74 42 4e 35 32 53 69 74 4c 54 64 54 56 4f 2b 62 2f 4d 4e 6e 4f 4d 53 36 62 7a 54 34 46 64 41 72 69 4f 65 2f 52 6c 6b 65 41 58 61 65 53 62 6f 68 6d 41 62 6c 56 6b 66 5a 38 6b 57 53 58 37 56 36 57 75 6e 44 79 52 72 69 55 51 3d 3d 22 3e 0d 0a 3c 68 65 61 64 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 76 61 72 20 61 62 70 3b 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 76 69 6e 74 61 67 65 70 61 73 65 6f 2e 63 6f 6d 2f 70 78 2e 6a 73 3f 63 68 3d 31 22 3e 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 68 74 74 70 3a 2f 2f 77 77 77 2e 76 69 6e 74 61 67 65 70 61 73 65 6f 2e 63 6f 6d 2f 70 78 2e 6a 73 3f 63 68 3d 32 22 3e 3c 2f 73 63 72 69 70 74 3e 3c 73 63 72 69 70 74 20 74 79 70 65 3d 22 74 65 78 74 2f 6a 61 76 61 73 63 72 69 70 74 22 3e 66 75 6e 63 74 69 6f 6e 20 68 61 6e 64 6c 65 41 42 50 44 65 74 65 63 74 28 29 7b 74 72 79 7b 69 66 28 21 61 62 70 29 20 72 65 74 75 72 6e 3b 76 61 72 20 69 6d 67 6c 6f 67 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 69 6d 67 22 29 3b 69 6d 67 6c 6f 67 2e 73 74 79 6c 65 2e 68 65 69 67 68 74 3d 22 30 70 78 22 3b 69 6d 67 6c 6f Data Ascii: 4f91<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01//EN" "http://www.w3.org/TR/html4/strict.dtd"><html xmlns="http://www.w3.org/1999/xhtml" data-adblockkey="MFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAKX74ixpzVyXbJprcLfbH4psP4+L2entqri0lzh6pkAaXLPIcclv6DQBeJJjGFWrBIF6QMyFwXT5CCRyjS2penECAwEAAQ==_BvmoE1YFCm+tBN52SitLTqdTVO+b/MNnOMS6bzT4FdAriOe/RlkeAXaeSbohmAblVkfZ8kWSX7V6WunDyRriUQ==><head><script type="text/javascript">var abp;</script><script type="text/javascript" src="http://www.vintagepaseo.com/px.js?ch=1"></script><script type="text/javascript" src="http://www.vintagepaseo.com/px.js?ch=2"></script><script type="text/javascript">function handleABPDetect(){try{if(!abp) return;var imglog = document.createElement("img");imglog.style.height="0px";imglo

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.6	49826	217.160.0.226	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2021 13:39:16.181458950 CEST	6077	OUT	GET /mexq/?e66HNDO=aPMuX7G1Ot9XJXghMAabXwwkzBWzprGcmmQ5cfrgMP5E/C43hf1Uz5bqYekFv+cUss1JtU0p5g==&6lux=TrTPmvux5 HTTP/1.1 Host: www.xn--aprendes-espaol-brb.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
Oct 13, 2021 13:39:16.395705938 CEST	6078	IN	HTTP/1.1 301 Moved Permanently Content-Type: text/html; charset=UTF-8 Transfer-Encoding: chunked Connection: close Date: Wed, 13 Oct 2021 11:39:16 GMT Server: Apache X-Powered-By: PHP/7.4.24 Expires: Wed, 11 Jan 1984 05:00:00 GMT Cache-Control: no-cache, must-revalidate, max-age=0 X-Redirect-By: WordPress Location: http://xn--aprendes-espaol-brb.com/mexq/?e66HNDO=aPMuX7G1Ot9XJXghMAabXwwkzBWzprGcmmQ5cfrgMP5E/C43hf1Uz5bqYekFv+cUss1JtU0p5g==&6lux=TrTPmvux5 Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

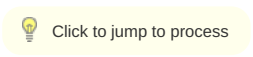
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.6	49827	154.216.110.149	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Oct 13, 2021 13:39:28.079721928 CEST	6079	OUT	GET /mexq/?e66HNDO=g6L0/Z2eA1jwRGo1l6rXBhzWGtzMcF3Ol1vrZIbNMV/6CHuR9YyStXwolwULrpYmw34wy4pkGQ==&6lux=TrTPmvux5 HTTP/1.1 Host: www.cyebang.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Oct 13, 2021 13:39:28.372508049 CEST	6081	IN	HTTP/1.1 200 OK Content-Type: text/html; charset=UTF-8 Server: Microsoft-IIS/8.5 X-Powered-By: PHP/5.6.40 X-Powered-By: ASP.NET Date: Wed, 13 Oct 2021 11:39:24 GMT Connection: close Content-Length: 1245 Data Raw: 0d 0a 0d 0a 0d 0a 0d 0a 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 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0d 0a 3c 6c 69 6e 6b 20 72 65 6c 3d 22 69 63 6f 6e 22 20 68 72 65 66 3d 22 2f 66 61 76 69 63 6f 6e 2e 69 63 6f 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 2f 3e 0d 0a 3c 74 69 74 6c 65 3e e4 b9 9d e6 b8 b8 e4 bc 9a e5 a4 87 e7 94 a8 e7 bd 91 e5 9d 80 5f e9 a6 96 e9 a1 b5 3c 2f 74 69 74 6c 65 3e 0d 0a 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 6b 65 79 77 6f 72 64 73 22 20 63 6f 6e 74 65 6e 74 3d 22 e4 b9 9d e6 b8 b8 e4 bc 9a e5 a4 87 e7 94 a8 e7 bd 91 e5 9d 80 5f e9 a6 96 e9 a1 b5 22 3e 0d 0a 20 20 20 20 3c 6d 65 74 61 20 6e 61 6d 65 3d 22 64 65 73 63 72 69 70 74 69 6f 6e 22 63 6f 6e 74 65 6e 74 3d 22 e4 b9 9d e6 b8 b8 e4 bc 9a e5 a4 87 e7 94 a8 e7 bd 91 e5 9d 80 5f e9 a6 96 e9 a1 b5 22 3e 0d 0a 3c 6d 65 74 61 20 69 64 3d 22 76 69 65 77 70 6f 72 74 22 20 6e 61 6d 65 3d 22 76 69 65 77 70 6f 72 74 22 20 63 6f 6e 74 65 6e 74 3d 22 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 2c 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 6e 6f 22 3e 0d 0a 3c 73 63 72 69 70 74 3e 0d 0a 76 61 72 20 5f 68 6d 74 20 3d 20 5f 68 6d 74 20 7c 7c 20 5b 5d 3b 0d 0a 28 66 75 6e 63 74 69 6f 6e 28 29 20 7b 0d 0a 20 20 76 61 72 20 68 6d 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 22 73 63 72 69 70 74 22 29 3b 0d 0a 20 20 68 6d 2e 73 72 63 20 3d 20 22 68 74 74 70 73 3a 2f 2f 68 6d 2e 62 61 69 64 75 2e 63 6f 6d 2f 68 6d 2e 6a 73 3f 38 35 31 38 36 36 39 66 30 64 33 31 65 34 31 35 30 38 62 65 30 62 61 62 66 35 61 38 66 63 32 38 22 3b 0d 0a 20 20 76 61 72 20 73 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 73 42 79 54 61 67 4e 61 6d 65 28 22 73 63 72 69 70 74 22 29 5b 30 5d 3b 20 0d 0a 20 20 73 2e 70 61 72 65 6e 74 4e 6f 64 65 2e 69 6e 73 65 72 74 42 65 66 6f 72 65 28 68 6d 2c 20 73 29 3b 0d 0a 7d 29 28 29 3b 0d 0a 3c 2f 73 63 72 69 70 74 3e 0d 0a 20 20 3c 73 63 72 69 70 74 3e 0d 0a 28 66 75 6e 63 74 69 6f 6e 28 29 7b 0d 0a 20 20 20 20 76 61 72 20 62 70 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 63 72 65 61 74 65 45 6c 65 6d 65 6e 74 28 27 73 63 72 69 70 74 27 29 3b 0d 0a 20 20 20 20 76 61 72 20 63 75 72 50 72 6f 74 6f 63 6f 6c 20 3d 20 77 69 6e 64 6f 77 2e 6c 6f 63 61 74 69 6f 6e 2e 70 72 6f 74 6f 63 6f 6c 2e 73 70 6c 69 74 28 27 3a 27 29 5b 30 5d 3b 0d 0a 20 20 20 20 69 66 20 28 63 75 72 50 72 6f 74 6f 63 6f 6c 20 3d 3d 3d 20 27 68 74 74 70 73 27 29 20 7b 0d 0a 20 20 20 20 20 20 20 20 62 70 2e 73 72 63 20 3d 20 27 68 74 74 70 73 3a 2f 2f 7a 7a 2e 62 64 73 74 61 74 69 63 2e 63 6f 6d 2f 6c 69 6e 6b 73 75 62 6d 69 74 2f 70 75 73 68 2e 6a 73 27 3b 0d 0a 20 20 20 20 7d 0d 0a 20 20 20 20 65 6c 73 65 20 7b 0d 0a 20 20 20 20 20 20 20 20 62 70 2e 73 72 63 20 3d 20 27 68 74 74 70 3a 2f 2f 70 75 73 68 2e 7a 68 61 6e 7a 68 61 6e 67 2e 62 61 69 64 75 2e 63 6f 6d 2f 70 75 73 68 2e 6a 73 27 3b 0d 0a 20 20 20 20 7d 0d 0a 20 20 20 20 76 61 72 20 73 20 3d 20 64 6f 63 75 6d 65 6e 74 2e 67 65 74 45 6c 65 6d 65 6e 74 73 42 79 54 61 67 4e 61 6d 65 28 22 73 63 72 69 70 74 22 29 5b 30 5d 3b 0d 0a 20 20 20 20 73 2e 70 61 72 65 6e 74 4e 6f 64 65 2e 69 6e 73 65 72 74 42 65 66 6f 72 65 28 62 70 2c 20 73 29 3b 0d 0a Data Ascii: <!DOCTYPE html><html><head><meta charset="utf-8"><link rel="icon" href="/favicon.ico" type="image/x-icon"/><title>_</title><meta name="keywords" content="_"> <meta name="description"content="_"><meta id="viewport" name="viewport" content="width=device-width,minimum-scale=1.0,maximum-scale=1.0,user-scalable=no"><script>var _hmt = _hmt || [];(function() { var hm = document.createElement("script"); hm.src = "https://hm.baidu.com/hm.js?8518669f0d31e41508be0babf5a8fc28"; var s = document.getElementsByTagName("script")[0]; s.parentNode.insertBefore(hm, s);})();</script> <script>(function(){ var bp = document.createElement('script'); var curProtocol = window.location.protocol.split(':')[0]; if (curProtocol === 'https') { bp.src = 'https://zz.bdstatic.com/linksubmit/push.js'; } else { bp.src = 'http://push.zhanzhang.baidu.com/push.js'; } var s = document.getElementsByTagName("script")[0]; s.parentNode.insertBefore(bp, s);

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: iAuPyHuUkk.exe PID: 476 Parent PID: 6508

General

Start time:	13:37:28
Start date:	13/10/2021
Path:	C:\Users\user\Desktop\iAuPyHuUkk.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\iAuPyHuUkk.exe'
Imagebase:	0xf00000
File size:	698880 bytes
MD5 hash:	6040407905EA1AA24DD58DC8BEFA4255
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: 00000000.00000002.371245810.00000000043C9000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.371245810.00000000043C9000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.371245810.00000000043C9000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.370703013.00000000033F7000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.370638895.00000000033C1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: iAuPyHuUkk.exe PID: 6968 Parent PID: 476

General

Start time:	13:37:37
Start date:	13/10/2021
Path:	C:\Users\user\Desktop\iAuPyHuUkk.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\iAuPyHuUkk.exe
Imagebase:	0xbc0000
File size:	698880 bytes
MD5 hash:	6040407905EA1AA24DD58DC8BEFA4255
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: 00000003.00000002.455602320.0000000001930000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.455602320.0000000001930000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.455602320.0000000001930000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.454131267.00000000015D0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.454131267.00000000015D0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.454131267.00000000015D0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000003.00000002.453689507.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000003.00000002.453689507.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000003.00000002.453689507.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: explorer.exe PID: 3440 Parent PID: 6968

General

Start time:	13:37:38
Start date:	13/10/2021
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: 00000005.00000000.400507122.00000000075B9000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.400507122.00000000075B9000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.400507122.00000000075B9000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000005.00000000.421546178.00000000075B9000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000005.00000000.421546178.00000000075B9000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000005.00000000.421546178.00000000075B9000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities Show Windows behavior

Analysis Process: autofmt.exe PID: 5980 Parent PID: 3440

General

Start time:	13:38:07
Start date:	13/10/2021
Path:	C:\Windows\SysWOW64\autofmt.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\SysWOW64\autofmt.exe
Imagebase:	0x12e0000
File size:	831488 bytes
MD5 hash:	7FC345F685C2A58283872D851316ACC4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: control.exe PID: 3540 Parent PID: 3440

General

Start time:	13:38:14
Start date:	13/10/2021
Path:	C:\Windows\SysWOW64\control.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\control.exe
Imagebase:	0xd20000
File size:	114688 bytes
MD5 hash:	40FBA3FBFD5E33E0DE1BA45472FDA66F
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: 0000000D.00000002.619163959.0000000002FE0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.619163959.0000000002FE0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.619163959.0000000002FE0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.619272890.0000000003010000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.619272890.0000000003010000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.619272890.0000000003010000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000D.00000002.617454019.00000000009B0000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000D.00000002.617454019.00000000009B0000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000D.00000002.617454019.00000000009B0000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

Show Windows behavior

File Read

Analysis Process: cmd.exe PID: 4432 Parent PID: 3540

General

Start time:	13:38:18
Start date:	13/10/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Users\user\Desktop\iAuPyHuUkk.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

Analysis Process: conhost.exe PID: 5900 Parent PID: 4432

General

Start time:	13:38:19
Start date:	13/10/2021
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