

ID: 745091
Sample Name:
PO0000001552.xls
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 19:26:14
Date: 13/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report PO0000001552.xls 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Threatname: Emotet 4
Yara Signatures 5
Initial Sample 5
Memory Dumps 5
Unpacked PEs 6
Sigma Signatures 6
Snort Signatures 6
Joe Sandbox Signatures 7
AV Detection 7
Software Vulnerabilities 7
Networking 7
E-Banking Fraud 7
System Summary 8
Boot Survival 8
Hooking and other Techniques for Hiding and Protection 8
HIPS / PFW / Operating System Protection Evasion 8
Stealing of Sensitive Information 8
Mitre Att&ck Matrix 8
Behavior Graph 9
Screenshots 9
Thumbnails 9
Antivirus, Machine Learning and Genetic Malware Detection 10
Initial Sample 10
Dropped Files 10
Unpacked PE Files 10
Domains 10
URLs 11
Domains and IPs 11
Contacted Domains 11
Contacted URLs 11
URLs from Memory and Binaries 12
World Map of Contacted IPs 14
Public IPs 15
Private 16
General Information 16
Warnings 17
Simulations 17
Behavior and APIs 17
Joe Sandbox View / Context 17
IPs 17
Domains 17
ASNs 18
JA3 Fingerprints 18
Dropped Files 18
Created / dropped Files 18
C:\Users\user\AppData\Local\Microsoft\FontCache\4\Catalog\ListAll.Json 18
C:\Users\user\AppData\Local\Microsoft\FontCache\4\PreviewFont\flat_officeFontsPreview.ttf 18
C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\E9097BEB-F41B-41FA-A529-2854DCDBD67E 18
C:\Users\user\AppData\Local\Microsoft\Office\16.0\excel.exe_Rules.xml 19
C:\Users\user\AppData\Local\Microsoft\TokenBroker\Cache\089d66ba04a8cec4bdc5267f42f39cf84278bb67.tbres 19
C:\Users\user\AppData\Local\Microsoft\TokenBroker\Cache\5475cb191e478c39370a215b2da98a37e9dc813d.tbres 19
C:\Users\user\AppData\Local\Microsoft\TokenBroker\Cache\9aad439831564ef9f88438a70a63c87e26ef3852.tbres 20
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\98S549LJ\o0oHPECmC0WPIXcvQPJOXzFOO7w00z7mkDO[1].dll 20
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CE8D676K\EvvmhfKiKFhKrSuHfBq[1].dll 20
C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\PO0000001552.LNK 21
C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat 21
C:\Users\user\elv2.ooocccxxx 21
C:\Users\user\elv3.ooocccxxx 22
C:\Windows\System32\GanZhs\FrugrCuQjdEr.dll (copy) 22
C:\Windows\System32\XEzXl\JZazaZgAOY.dll (copy) 22

Copyright Joe Security LLC 2022

Static File Info 23
General 23
File Icon 23
Static OLE Info 23
General 23
OLE File "PO0000001552.xls" 23
Indicators 23
Summary 23
Document Summary 23
Streams 24
Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096 24
General 24
Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096 24
General 24
Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 82874 24
General 24
Network Behavior 24
Snort IDS Alerts 24
Network Port Distribution 25
TCP Packets 25
UDP Packets 27
DNS Queries 27
DNS Answers 27
HTTP Request Dependency Graph 27
Statistics 28
Behavior 28
System Behavior 28
Analysis Process: EXCEL.EXEPID: 4380, Parent PID: 3800 28
General 28
File Activities 28
Registry Activities 28
Analysis Process: regsvr32.exePID: 6588, Parent PID: 4380 29
General 29
Analysis Process: regsvr32.exePID: 6608, Parent PID: 4380 29
General 29
File Activities 29
Analysis Process: regsvr32.exePID: 6676, Parent PID: 6608 30
General 30
Registry Activities 30
Key Value Created 30
Analysis Process: regsvr32.exePID: 6756, Parent PID: 4380 30
General 30
File Activities 30
Analysis Process: regsvr32.exePID: 6792, Parent PID: 6756 30
General 30
Registry Activities 31
Key Value Created 31
Disassembly 31

Copyright Joe Security LLC 2022

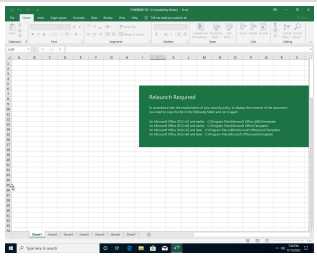
Windows Analysis Report

PO0000001552.xls

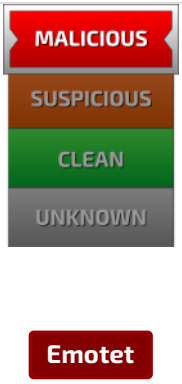
Overview

General Information

Sample Name:	PO0000001552.xls
Analysis ID:	745091
MD5:	ecdc3f1e9afd2ce..
SHA1:	0121ba555dfe0b..
SHA256:	1e494fd9ec670e..
Infos:	



Detection



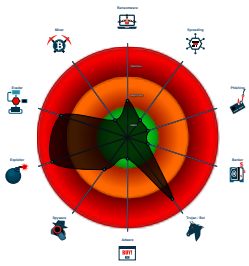
Emotet

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

Signatures

- Multi AV Scanner detection for subm…
- Document exploit detected (drops P…
- Malicious sample detected (through…
- Yara detected Emotet
- System process connects to networ…
- Document exploit detected (creates…
- Antivirus detection for URL or domain
- Multi AV Scanner detection for dom…
- Snort IDS alert for network traffic
- Creates an autostart registry key po…
- Creates multiple autostart registry k…
- Office process drops PE file

Classification



Process Tree

- **System is w10x64_ra**
- EXCEL.EXE (PID: 4380 cmdline: C:\Program Files\Microsoft Office\Root\Office16\EXCEL.EXE" "C:\Users\user\Desktop\PO0000001552.xls MD5: 23CAD504B3E04BB54CD636AD2874041A)
  - regsvr32.exe (PID: 6588 cmdline: C:\Windows\System32\regsvr32.exe /S ..\elv1.ooocccxxx MD5: 578BAB56836A3FE455FFC7883041825B)
  - regsvr32.exe (PID: 6608 cmdline: C:\Windows\System32\regsvr32.exe /S ..\elv2.ooocccxxx MD5: 578BAB56836A3FE455FFC7883041825B)
    - regsvr32.exe (PID: 6676 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\XEzXl\JZazaZgAOY.dll" MD5: 578BAB56836A3FE455FFC7883041825B)
  - regsvr32.exe (PID: 6756 cmdline: C:\Windows\System32\regsvr32.exe /S ..\elv3.ooocccxxx MD5: 578BAB56836A3FE455FFC7883041825B)
    - regsvr32.exe (PID: 6792 cmdline: C:\Windows\system32\regsvr32.exe "C:\Windows\system32\GanZhs\FrugrCuQjdEr.dll" MD5: 578BAB56836A3FE455FFC7883041825B)
- **cleanup**

Malware Configuration

Threatname: Emotet

Copyright Joe Security LLC 2022

```
{
  "C2 list": [
    "173.255.211.88:443",
    "45.63.99.23:7080",
    "182.162.143.56:443",
    "91.187.140.35:8080",
    "212.24.98.99:8080",
    "119.59.103.152:8080",
    "45.235.8.30:8080",
    "172.104.251.154:8080",
    "72.15.201.15:8080",
    "169.57.156.166:8080",
    "103.75.201.2:443",
    "213.239.212.5:443",
    "164.90.222.65:443",
    "201.94.166.162:443",
    "94.23.45.86:4143",
    "183.111.227.137:8080",
    "186.194.240.217:443",
    "107.170.39.149:8080",
    "147.139.166.154:8080",
    "5.135.159.50:443",
    "206.189.28.199:8080",
    "104.168.155.143:8080",
    "129.232.188.93:443",
    "82.223.21.224:8080",
    "103.43.75.120:443",
    "103.132.242.26:8080",
    "139.59.56.73:8080",
    "164.68.99.3:8080",
    "202.129.205.3:8080",
    "167.172.199.165:8080",
    "110.232.117.186:8080",
    "209.97.163.214:443",
    "167.172.253.162:8080",
    "1.234.2.232:8080",
    "159.65.88.10:8080",
    "95.217.221.146:8080",
    "153.92.5.27:8080",
    "91.207.28.33:8080",
    "188.44.20.25:443",
    "153.126.146.25:7080",
    "163.44.196.120:8080",
    "172.105.226.75:8080",
    "115.68.227.76:8080",
    "159.65.140.115:443",
    "139.59.126.41:443",
    "197.242.150.244:8080",
    "45.176.232.124:443",
    "45.118.115.99:8080",
    "149.56.131.28:8080",
    "79.137.35.198:8080",
    "173.212.193.249:8080",
    "160.16.142.56:8080",
    "159.89.202.34:443",
    "185.4.135.165:8080"
  ],
  "Public Key": [
    "RUNTMSAAAABAX3S2xNjcDD0fBno33Ln5t71eii+mofIPoXkNFOX1MeiwCh48iz97kB0mJjGGZXwardnDXKxI8GCHGNl0PFj5kCHHpgAjAJA=",
    "RUNLMSAAAADzozW1Di4r9DVWzQpMKT588RDdy7BPILP6AiDOTLYMHkSWvrQO5slbmr1OvZ2Pz+AQWzRMggQmAtO6rPH7nyx2ayEIpgAYAJA="
  ]
}
```


Yara Signatures

Initial Sample

Source	Rule	Description	Author	Strings
PO0000001552.xls	SUSP_Excel4Macro_AutoOpen	Detects Excel4 macro use with auto open / close	John Lambert @JohnLaTwC	• 0x0:$header_docf: D0 CF 11 E0 • 0x146aa:$s1: Excel • 0x1573f:$s1: Excel • 0x35d0:$Auto_Open: 18 00 17 00 20 00 00 01 07 00 00 00 00 00 00 00 00 01 3A

Memory Dumps

Source	Rule	Description	Author	Strings
0000000C.00000002.2414304563.00000000009BB000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Emotet_3	Yara detected Emotet	Joe Security	
0000000A.00000002.2414500170.0000000000BBB000.00000004.00000020.00020000.00000000.sdmp	JoeSecurity_Emotet_3	Yara detected Emotet	Joe Security	
00000008.00000002.1291594477.0000000180001000.00000020.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
00000008.00000002.1291594477.0000000180001000.00000020.00001000.00020000.00000000.sdmp	Windows_Trojan_Emotet_db7d33fa	unknown	unknown	• 0x171c2:$chunk_0: 4C 8D 9C 24 80 00 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0x2a90c:$chunk_0: 4C 8D 9C 24 80 00 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0x24ac0:$chunk_1: 8B C7 41 0F B7 4C 45 00 41 8B 1C 8C 48 03 DD 48 3B DE 72 1B • 0x1b568:$chunk_2: 48 8B C4 48 89 48 08 48 89 50 10 4C 89 40 18 4C 89 48 20 C3 • 0x216e4:$chunk_4: 48 39 3B 4C 8D 9C 24 80 00 00 00 49 8B 5B 10 49 8B 73 18 40 0F 95 C7 8B C7 49 8B 7B 20 49 8B E3 5D C3 • 0x2ae01:$chunk_4: 48 39 3B 4C 8D 9C 24 80 00 00 00 49 8B 5B 10 49 8B 73 20 40 0F 95 C7 8B C7 49 8B 7B 28 49 8B E3 5D C3 • 0x24ad4:$chunk_6: 43 8B 84 FE 8C 00 00 00 48 03 C6 48 3B D8 73 0B
00000008.00000002.1290019980.0000000000980000.00000040.00001000.00020000.00000000.sdmp	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
Click to see the 1 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
8.2.regsvr32.exe.980000.0.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
8.2.regsvr32.exe.980000.0.unpack	Windows_Trojan_Emotet_db7d33fa	unknown	unknown	• 0x169c2:$chunk_0: 4C 8D 9C 24 80 00 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0x2a10c:$chunk_0: 4C 8D 9C 24 80 00 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0x242c0:$chunk_1: 8B C7 41 0F B7 4C 45 00 41 8B 1C 8C 48 03 DD 48 3B DE 72 1B • 0x1ad68:$chunk_2: 48 8B C4 48 89 48 08 48 89 50 10 4C 89 40 18 4C 89 48 20 C3 • 0x20ee4:$chunk_4: 48 39 3B 4C 8D 9C 24 80 00 00 00 49 8B 5B 10 49 8B 73 18 40 0F 95 C7 8B C7 49 8B 7B 20 49 8B E3 5D C3 • 0x2a601:$chunk_4: 48 39 3B 4C 8D 9C 24 80 00 00 00 49 8B 5B 10 49 8B 73 20 40 0F 95 C7 8B C7 49 8B 7B 28 49 8B E3 5D C3 • 0x242d4:$chunk_6: 43 8B 84 FE 8C 00 00 00 48 03 C6 48 3B D8 73 0B
8.2.regsvr32.exe.980000.0.raw.unpack	JoeSecurity_Emotet_1	Yara detected Emotet	Joe Security	
8.2.regsvr32.exe.980000.0.raw.unpack	Windows_Trojan_Emotet_db7d33fa	unknown	unknown	• 0x175c2:$chunk_0: 4C 8D 9C 24 80 00 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0x2ad0c:$chunk_0: 4C 8D 9C 24 80 00 00 00 8B C3 49 8B 5B 10 49 8B 73 18 49 8B 7B 20 49 8B E3 5D C3 • 0x24ec0:$chunk_1: 8B C7 41 0F B7 4C 45 00 41 8B 1C 8C 48 03 DD 48 3B DE 72 1B • 0x1b968:$chunk_2: 48 8B C4 48 89 48 08 48 89 50 10 4C 89 40 18 4C 89 48 20 C3 • 0x21ae4:$chunk_4: 48 39 3B 4C 8D 9C 24 80 00 00 00 49 8B 5B 10 49 8B 73 18 40 0F 95 C7 8B C7 49 8B 7B 20 49 8B E3 5D C3 • 0x2b201:$chunk_4: 48 39 3B 4C 8D 9C 24 80 00 00 00 49 8B 5B 10 49 8B 73 20 40 0F 95 C7 8B C7 49 8B 7B 28 49 8B E3 5D C3 • 0x24ed4:$chunk_6: 43 8B 84 FE 8C 00 00 00 48 03 C6 48 3B D8 73 0B

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET CNC Feodo Tracker Reported CnC Server TCP group 9 - Source IP: 192.168.2.3 - Destination IP: 182.162.143.56	
Timestamp:	192.168.2.3182.162.143.56497124432404316 11/13/22-19:28:07.391953
SID:	2404316
Source Port:	49712
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET CNC Feodo Tracker Reported CnC Server TCP group 18 - Source IP: 192.168.2.3 - Destination IP: 45.63.99.23	
Timestamp:	192.168.2.345.63.99.234970970802404334 11/13/22-19:27:51.342965
SID:	2404334
Source Port:	49709
Destination Port:	7080
Protocol:	TCP
Classtype:	A Network Trojan was detected

ET DNS Query to a *.top domain - Likely Hostile - Source IP: 192.168.2.3 - Destination IP: 1.1.1.1	
Timestamp:	192.168.2.31.1.1.1631775320238883 11/13/22-19:27:02.730666
SID:	2023883
Source Port:	63177
Destination Port:	53
Protocol:	UDP
Classtype:	Potentially Bad Traffic

ET CNC Feodo Tracker Reported CnC Server TCP group 8 - Source IP: 192.168.2.3 - Destination IP: 173.255.211.88	
Timestamp:	192.168.2.3173.255.211.88497054432404314 11/13/22-19:27:33.992872
SID:	2404314
Source Port:	49705
Destination Port:	443
Protocol:	TCP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

AV Detection



Multi AV Scanner detection for submitted file

Antivirus detection for URL or domain

Multi AV Scanner detection for domain / URL

Software Vulnerabilities



Document exploit detected (drops PE files)

Document exploit detected (creates forbidden files)

Document exploit detected (process start blacklist hit)

Document exploit detected (UrlDownloadToFile)

Networking



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

Snort IDS alert for network traffic

C2 URLs / IPs found in malware configuration

E-Banking Fraud



Copyright Joe Security LLC 2022

Yara detected Emotet

System Summary



Malicious sample detected (through community Yara rule)

Office process drops PE file

Boot Survival



Creates an autostart registry key pointing to binary in C:\Windows

Creates multiple autostart registry keys

Drops PE files to the user root directory

Hooking and other Techniques for Hiding and Protection



Hides that the sample has been downloaded from the Internet (zone.identifier)

HIPS / PFW / Operating System Protection Evasion



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

Stealing of Sensitive Information



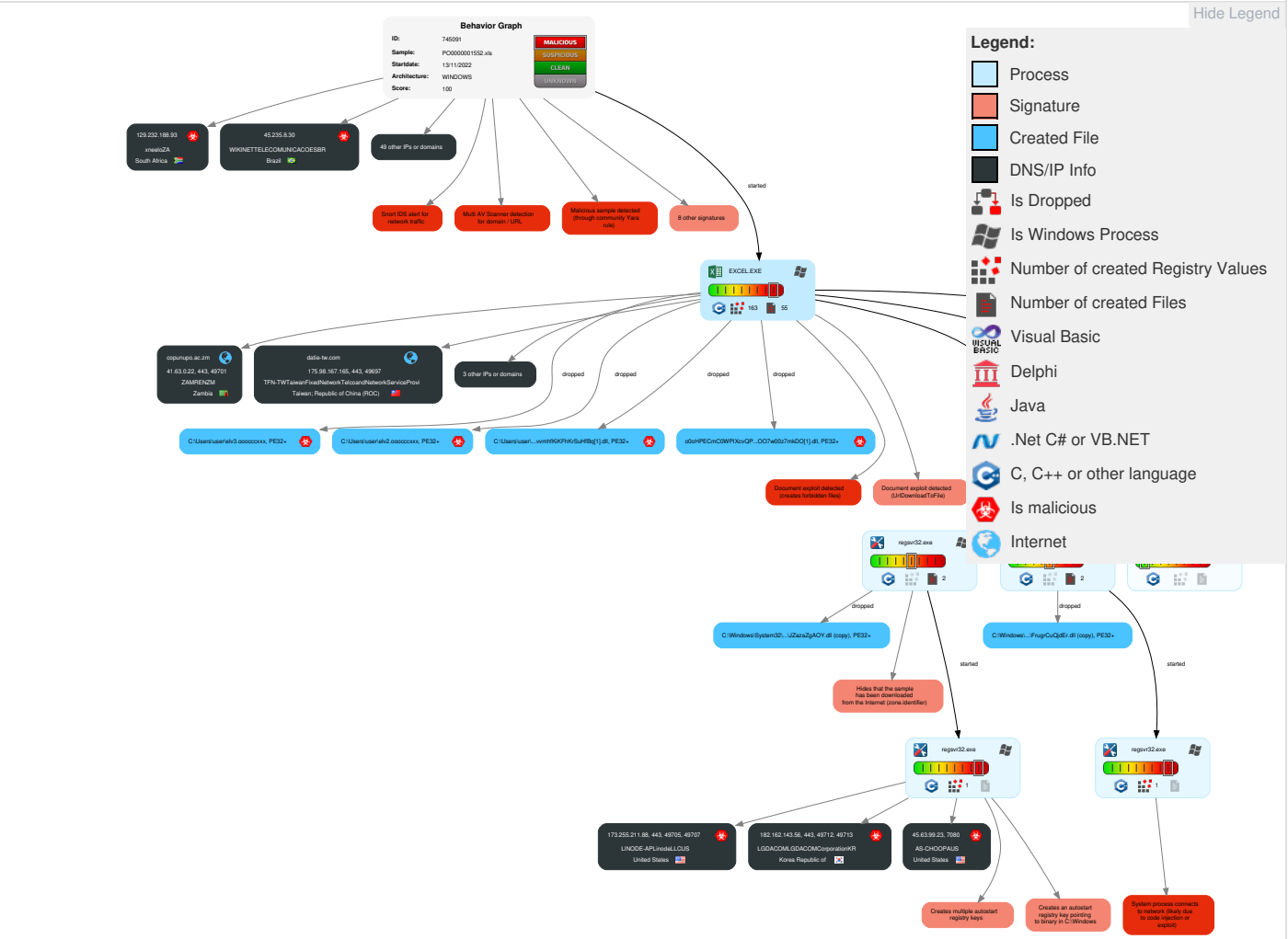
Yara detected Emotet

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Native API	2 1 Registry Run Keys / Startup Folder	1 1 Process Injection	1 4 1 Masquerading	OS Credential Dumping	1 System Time Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 1 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	4 3 Exploitation for Client Execution	1 DLL Side-Loading	2 1 Registry Run Keys / Startup Folder	1 Virtualization/Sandbox Evasion	LSASS Memory	1 1 Security Software Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Non-Standard Port	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout
Domain Accounts	At (Linux)	Logon Script (Windows)	1 DLL Side-Loading	1 1 Process Injection	Security Account Manager	1 Virtualization/Sandbox Evasion	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 3 Ingress Tool Transfer	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Hidden Files and Directories	NTDS	2 Process Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	4 Non-Application Layer Protocol	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 Obfuscated Files or Information	LSA Secrets	1 File and Directory Discovery	SSH	Keylogging	Data Transfer Size Limits	1 2 5 Application Layer Protocol	Manipulate Device Communication		Manipulate App Store Rankings or Ratings
Replication Through Removable Media	Launchd	Rc.common	Rc.common	1 Regsvr32	Cached Domain Credentials	2 6 System Information Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service		Abuse Accessibility Features
External Remote Services	Scheduled Task	Startup Items	Startup Items	1 DLL Side-Loading	DCSync	Network Sniffing	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Wi-Fi Access Points		Data Encrypted for Impact

Copyright Joe Security LLC 2022

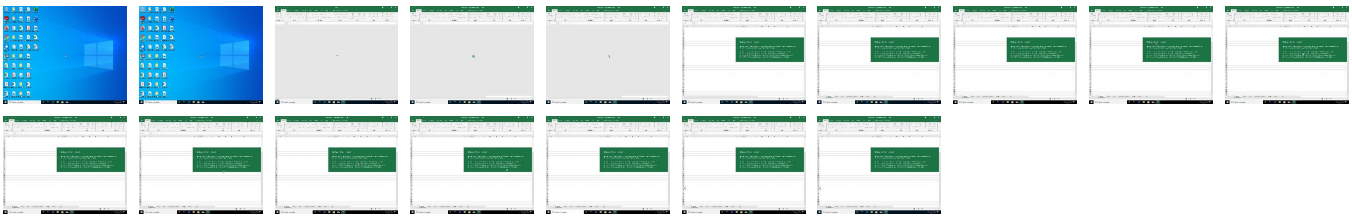
Behavior Graph

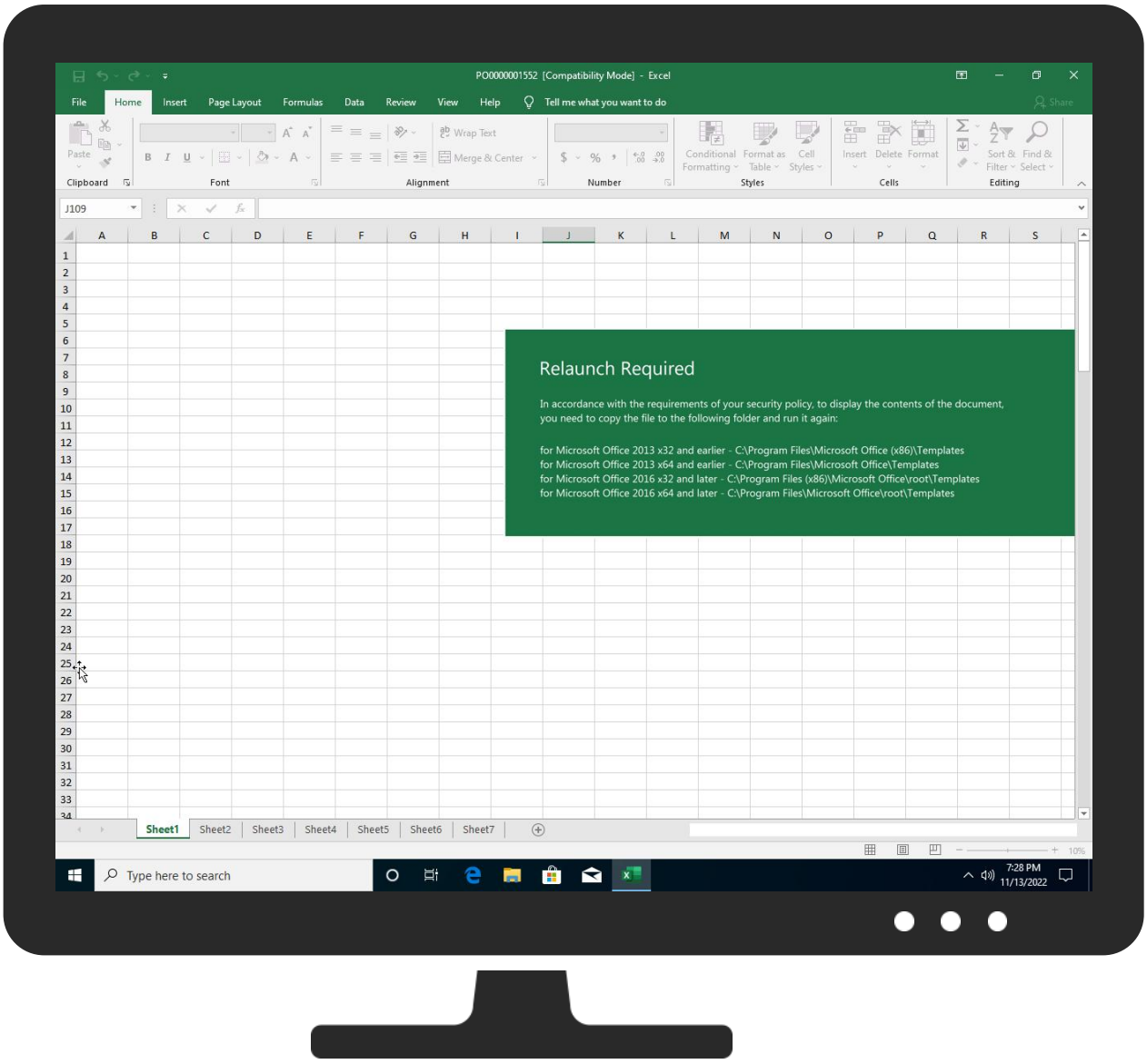


Screenshots

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
PO0000001552.xls	66%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
8.2.regsvr32.exe.980000.0.unpack	100%	Avira	HEUR/AGEN.1215461		Download File

Domains

Source	Detection	Scanner	Label	Link
sbm.xinmoshiwang.com	13%	Virustotal		Browse
datie-tw.com	10%	Virustotal		Browse
copunupo.ac.zm	18%	Virustotal		Browse
ly.yjlianyi.top	13%	Virustotal		Browse

Copyright Joe Security LLC 2022

URLs

Source	Detection	Scanner	Label	Link
http://https://roaming.edog.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://api.aadrm.com	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://api.addins.store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://prod-global-autodetect.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	URL Reputation	safe	
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	0%	Avira URL Cloud	safe	
http://https://182.162.143.56/qqvehgyxm/bitss/ktcpnaio/F	100%	Avira URL Cloud	malware	
http://https://182.162.143.56/qqvehgyxm/bitss/ktcpnaio/	100%	Avira URL Cloud	malware	
http://https://45.63.99.23:7080/qqvehgyxm/bitss/ktcpnaio/	0%	Avira URL Cloud	safe	
http://ly.yjlianyi.top/wp-admin/4cChao/	100%	Avira URL Cloud	malware	
http://https://45.63.99.23:7080/tkafmhcgcid/	0%	Avira URL Cloud	safe	
http://sbm.xinmoshiwang.com/upload/VaOfWEb3pW76UO/	100%	Avira URL Cloud	malware	
http://https://45.63.99.23:7080/b	0%	Avira URL Cloud	safe	
http://https://my.microsoftpersonalcontent.com	0%	Avira URL Cloud	safe	
http://https://api.scheduler.	0%	Avira URL Cloud	safe	
http://https://45.63.99.23:7080/tkafmhcgcid/8eM	0%	Avira URL Cloud	safe	
http://https://182.162.143.56/tkafmhcgcid/	100%	Avira URL Cloud	malware	
http://https://182.162.143.56/	100%	Avira URL Cloud	malware	
http://https://45.63.99.23:7080/2	0%	Avira URL Cloud	safe	
http://https://45.63.99.23:7080/qqvehgyxm/bitss/ktcpnaio/%	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
sbm.xinmoshiwang.com	47.92.35.35	true	false	• 13%, Virustotal, Browse	unknown
datie-tw.com	175.98.167.165	true	false	• 10%, Virustotal, Browse	unknown
copunupo.ac.zm	41.63.0.22	true	false	• 18%, Virustotal, Browse	unknown
ly.yjlianyi.top	81.68.152.197	true	false	• 13%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://ly.yjlianyi.top/wp-admin/4cChao/	false	• Avira URL Cloud: malware	unknown
http://https://182.162.143.56/qqvehgyxm/bitss/ktcpnaio/	true	• Avira URL Cloud: malware	unknown
http://sbm.xinmoshiwang.com/upload/VaOfWEb3pW76UO/	true	• Avira URL Cloud: malware	unknown
http://https://182.162.143.56/tkafmhcgcid/	true	• Avira URL Cloud: malware	unknown

Copyright Joe Security LLC 2022

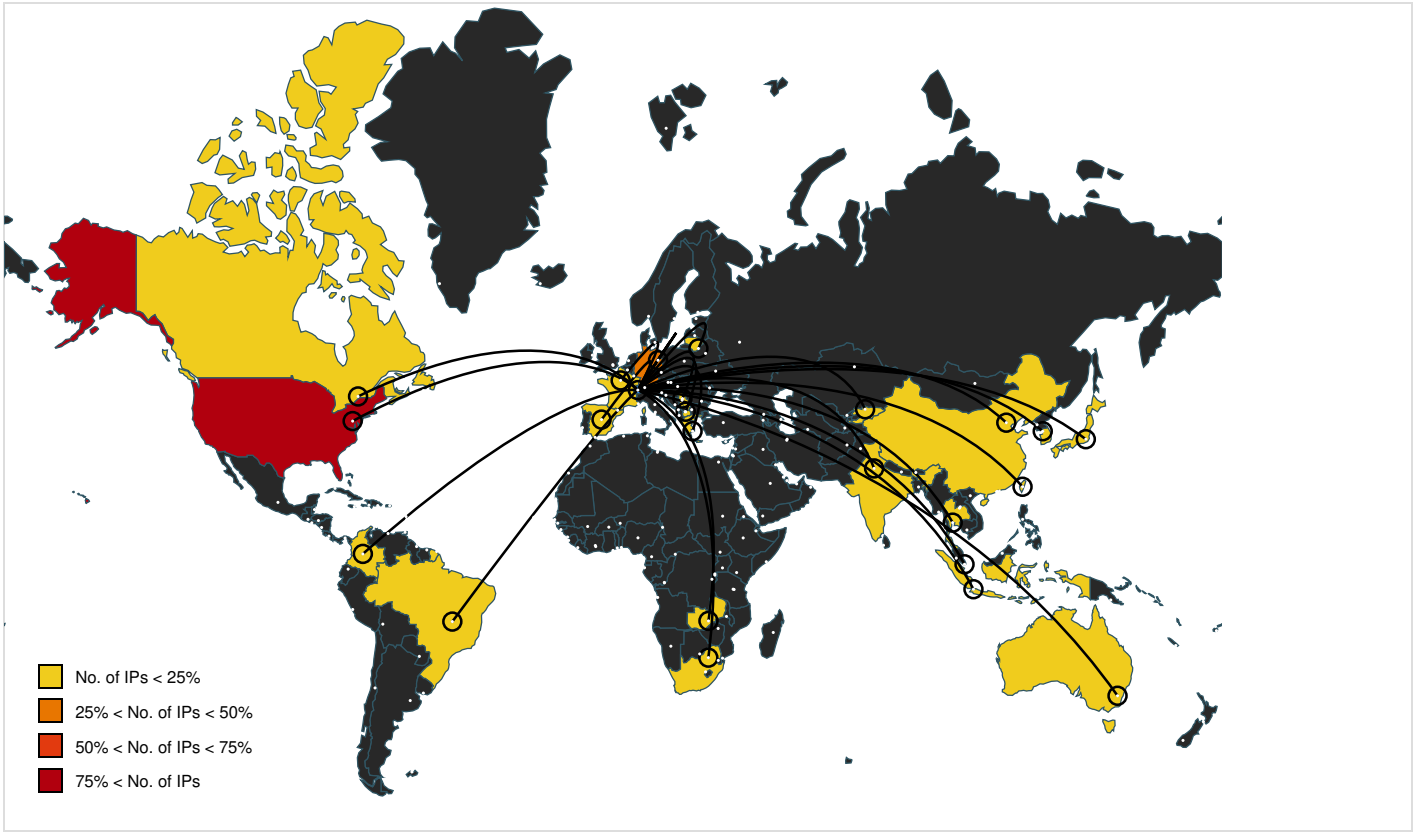
URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://api.diagnosticssdf.office.com	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://login.microsoftonline.com/	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://shell.suite.office.com:1443	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://login.windows.net/72f988bf-86f1-41af-91ab-2d7cd011db47/oauth2/authorize	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://autodiscover-s.outlook.com/	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://roaming.edog.	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false	• URL Reputation: safe	unknown
http://https://insertmedia.bing.office.net/images/officeonlinecontent/browse?cp=Flickr	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://cdn.entity.	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false	• URL Reputation: safe	unknown
http://https://api.addins.omex.office.net/appinfo/query	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/tenantassociationkey	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://dev.virtualearth.net/REST/V1/GeospatialEndpoint/	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://powerlift.acompli.net	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false	• URL Reputation: safe	unknown
http://https://rpsticket.partnerservices.getmicrosoftkey.com	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false	• URL Reputation: safe	unknown
http://https://lookup.onenote.com/lookup/geolocation/v1	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://cortana.ai	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false	• URL Reputation: safe	unknown
http://https://apc.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/imports	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://cloudfiles.onenote.com/upload.aspx	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://syncservice.protection.outlook.com/PolicySync/PolicySync.svc/SyncFile	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://entitlement.diagnosticssdf.office.com	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://na01.oscs.protection.outlook.com/api/SafeLinksApi/GetPolicy	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://182.162.143.56/qqvehgyxm/bitss/ktcpnaio/F	regsvr32.exe, 0000000C.00000003.20667070 11.0000000000A43000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 000C.00000002.2416113424.0000000000A4600 0.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://api.aadrm.com/	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false	• URL Reputation: safe	unknown
http://https://ofcrecsvcapi-int.azurewebsites.net/	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false	• URL Reputation: safe	unknown
http://https://dataservice.protection.outlook.com/PsorWebService/v1/ClientSyncFile/MipPolicies	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://api.microsoftstream.com/api/	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://insertmedia.bing.office.net/images/hosted?host=office&adlt=strict&hostType=Immersive	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://cr.office.com	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://augloop.office.com;https://augloop-int.officeppe.com;https://augloop-dogfood.officeppe.com;h	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false	• Avira URL Cloud: safe	low
http://https://portal.office.com/account/?ref=ClientMeControl	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://45.63.99.23:7080/qqvehgyxm/bitss/ktcpnaio/	regsvr32.exe, 0000000C.00000003.20048567 29.0000000000A34000.00000004.00000020.00 020000.00000000.sdmp, regsvr32.exe, 0000 000C.00000003.2004490975.0000000000A0D00 0.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://graph.ppe.windows.net	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://res.getmicrosoftkey.com/api/redemptionevents	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false	• URL Reputation: safe	unknown
http://https://powerlift-frontdesk.acompli.net	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false	• URL Reputation: safe	unknown
http://https://tasks.office.com	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://officeci.azurewebsites.net/api/	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false	• URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://45.63.99.23:7080/tkafmhcgcid/	regsvr32.exe, 0000000A.00000003.19272573 89.0000000000C31000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://sr.outlook.office.net/ws/speech/recognize/assistant/work	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://api.scheduler.	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://my.microsoftpersonalcontent.com	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false	• Avira URL Cloud: safe	unknown
http://https://store.office.cn/addinstemplate	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false	• URL Reputation: safe	unknown
http://https://api.aadrm.com	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office.com/autosuggest/api/v1/init?cvid=	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://globaldisco.crm.dynamics.com	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://messaging.engagement.office.com/	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://nam.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://dev0-api.acompli.net/autodetect	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false	• URL Reputation: safe	unknown
http://https://www.odwebp.svc.ms	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false	• URL Reputation: safe	unknown
http://https://api.diagnosticssdf.office.com/v2/feedback	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://api.powerbi.com/v1.0/myorg/groups	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://web.microsoftstream.com/video/	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://api.addins.store.officeppe.com/addinstemplate	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false	• URL Reputation: safe	unknown
http://https://45.63.99.23:7080/b	regsvr32.exe, 0000000C.00000003.20048567 29.0000000000A34000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://graph.windows.net	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://dataservice.o365filtering.com/	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false	• URL Reputation: safe	unknown
http://https://officesetup.getmicrosoftkey.com	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false	• URL Reputation: safe	unknown
http://https://analysis.windows.net/powerbi/api	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://prod-global-autodetect.acompli.net/autodetect	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false	• URL Reputation: safe	unknown
http://https://outlook.office365.com/autodiscover/autodiscover.json	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://powerpoint.uservoice.com/forums/288952-powerpoint-for-ipad-iphone-ios	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://consent.config.office.com/consentcheckin/v1.0/consents	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://eur.learningtools.onenote.com/learningtoolsapi/v2.0/getfreeformspeech	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://learningtools.onenote.com/learningtoolsapi/v2.0/Getvoices	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/System.ShortCircuitProfile.json	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://ncus.contentsync.	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false	• URL Reputation: safe	unknown
http://https://onedrive.live.com/about/download/?windows10SyncClientInstalled=false	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://45.63.99.23:7080/tkafmhcgcid/8eM	regsvr32.exe, 0000000A.00000003.19276931 96.0000000000C0C000.00000004.00000020.00 020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://webdir.online.lync.com/autodiscover/autodiscoverservice.svc/root/	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://weather.service.msn.com/data.aspx	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://apis.live.net/v5.0/	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false	• URL Reputation: safe	unknown
http://https://officemobile.uservoice.com/forums/929800-office-app-ios-and-ipad-asks	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://word.uservoice.com/forums/304948-word-for-ipad-iphone-ios	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://messaging.lifecycle.office.com/	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://autodiscover-s.outlook.com/autodiscover/autodiscover.xml	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://management.azure.com	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://outlook.office365.com	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://wus2.contentsync.	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false	• URL Reputation: safe	unknown
http://https://incidents.diagnostics.office.com	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://clients.config.office.net/user/v1.0/ios	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://182.162.143.56/	regsvr32.exe, 0000000A.00000003.2012380786.0000000000C4A000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000A.00000002.2416327091.0000000000C4D000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000A.00000003.2012998285.0000000000C4D000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000C.00000003.2066707011.0000000000A43000.00000004.00000020.00020000.00000000.sdmp, regsvr32.exe, 0000000C.00000002.2416113424.0000000000A46000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: malware	unknown
http://https://45.63.99.23:7080/2	regsvr32.exe, 0000000A.00000003.1927414494.0000000000C41000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://insertmedia.bing.office.net/odc/insertmedia	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://o365auditrealtimeingestion.manage.office.com	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://outlook.office365.com/api/v1.0/me/Activities	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://api.office.net	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://incidents.diagnosticssdf.office.com	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://asgsmsproxyapi.azurewebsites.net/	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false	• URL Reputation: safe	unknown
http://https://clients.config.office.net/user/v1.0/android/policies	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://45.63.99.23:7080/qqvehgyxm/bitss/ktcpnaio/%	regsvr32.exe, 0000000C.00000003.2004490975.0000000000A0D000.00000004.00000020.00020000.00000000.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://entitlement.diagnostics.office.com	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://pf.directory.live.com/profile/mine/WLX.Profiles.IC.json	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://substrate.office.com/search/api/v2/init	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://outlook.office.com/	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://storage.live.com/clientlogs/uploadlocation	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://outlook.office365.com/	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high
http://https://webshell.suite.office.com	E9097BEB-F41B-41FA-A529-2854DCDBD67E.0.dr	false		high

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
110.232.117.186	unknown	Australia		56038	RACKCORP-APRackCorpAU	true
103.132.242.26	unknown	India		45117	INPL-IN-APIshansNetworkIN	true
104.168.155.143	unknown	United States		54290	HOSTWINDSUS	true
79.137.35.198	unknown	France		16276	OVHFR	true
45.118.115.99	unknown	Indonesia		131717	IDNIC-CIFO-AS-IDPTCitraJelajahInformatikaID	true
172.104.251.154	unknown	United States		63949	LINODE-APLinodeLLCUS	true
115.68.227.76	unknown	Korea Republic of		38700	SMILESERV-AS-KRSMILESERVKR	true
81.68.152.197	ly.yjlianyi.top	China		45090	CNNIC-TENCENT-NET-APShenzhenTencentComputerSystemsCompa	false
163.44.196.120	unknown	Singapore		135161	GMO-Z-COM-THGMO-ZcomNetDesignHoldingsCoLtdSG	true
206.189.28.199	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
45.63.99.23	unknown	United States		20473	AS-CHOOPAUS	true
107.170.39.149	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
197.242.150.244	unknown	South Africa		37611	AfrihostZA	true
185.4.135.165	unknown	Greece		199246	TOPHOSTGR	true
183.111.227.137	unknown	Korea Republic of		4766	KIXS-AS-KRKoreaTelecomKR	true
45.176.232.124	unknown	Colombia		267869	CABLEYTELECOMUNICACIONESDECOLOMBIASAS CABLETELCOC	true
139.59.56.73	unknown	Singapore		14061	DIGITALOCEAN-ASNUS	true
169.57.156.166	unknown	United States		36351	SOFTLAYERUS	true
175.98.167.165	datie-tw.com	Taiwan; Republic of China (ROC)		9924	TFN-TWTaiwanFixedNetworkTelcoandNetworkServiceProvi	false
164.68.99.3	unknown	Germany		51167	CONTABODE	true
139.59.126.41	unknown	Singapore		14061	DIGITALOCEAN-ASNUS	true
167.172.253.162	unknown	United States		14061	DIGITALOCEAN-ASNUS	true

Copyright Joe Security LLC 2022

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
147.139.166.154	unknown	United States		45102	CNNIC-ALIBABA-US-NET-APAlibabaUSTechnologyCoLtdC	true
202.129.205.3	unknown	Thailand		45328	NIPA-AS-THNIPATECHNOLOGYCOLTDTH	true
167.172.199.165	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
153.92.5.27	unknown	Germany		47583	AS-HOSTINGERLT	true
159.65.140.115	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
159.65.88.10	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
172.105.226.75	unknown	United States		63949	LINODE-APLinodeLLCUS	true
164.90.222.65	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
213.239.212.5	unknown	Germany		24940	HETZNER-ASDE	true
5.135.159.50	unknown	France		16276	OVHFR	true
173.255.211.88	unknown	United States		63949	LINODE-APLinodeLLCUS	true
212.24.98.99	unknown	Lithuania		62282	RACKRAYUABRakrejusLT	true
186.194.240.217	unknown	Brazil		262733	NetceteraTelecomunicacoesLtdaBR	true
91.187.140.35	unknown	Serbia		13092	UB-ASRS	true
119.59.103.152	unknown	Thailand		56067	METRABYTE-TH453LadplacoutJorakhaebuaTH	true
159.89.202.34	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
201.94.166.162	unknown	Brazil		28573	CLAROSABR	true
160.16.142.56	unknown	Japan		9370	SAKURA-BSAKURAInternetIncJP	true
103.75.201.2	unknown	Thailand		133496	CDNPLUSCOLTD-AS-APCDNPLUSCOLTDTH	true
91.207.28.33	unknown	Kyrgyzstan		39819	PROHOSTKG	true
103.43.75.120	unknown	Japan		20473	AS-CHOOPAUS	true
188.44.20.25	unknown	Macedonia		57374	GIV-ASMK	true
45.235.8.30	unknown	Brazil		267405	WIKINETTELECOMUNICACOESBR	true
153.126.146.25	unknown	Japan		7684	SAKURA-ASAKURAInternetIncJP	true
72.15.201.15	unknown	United States		13649	ASN-VINSUS	true
82.223.21.224	unknown	Spain		8560	ONEANDONE-ASBrauerstrasse48DE	true
173.212.193.249	unknown	Germany		51167	CONTABODE	true
47.92.35.35	sbm.xinmoshiwang.com	China		37963	CNNIC-ALIBABA-CN-NET-APHangzhouAlibabaAdvertisingCoLtd	false
95.217.221.146	unknown	Germany		24940	HETZNER-ASDE	true
41.63.0.22	copunupo.ac.zm	Zambia		37532	ZAMRENZM	false
149.56.131.28	unknown	Canada		16276	OVHFR	true
209.97.163.214	unknown	United States		14061	DIGITALOCEAN-ASNUS	true
182.162.143.56	unknown	Korea Republic of		3786	LGDACOMLGDACOMCorporationKR	true
1.234.2.232	unknown	Korea Republic of		9318	SKB-ASSKBroadbandCoLtdKR	true
129.232.188.93	unknown	South Africa		37153	xneeloZA	true
94.23.45.86	unknown	France		16276	OVHFR	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	745091
Start date and time:	2022-11-13 19:26:14 +01:00

Copyright Joe Security LLC 2022

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 5m 26s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PO0000001552.xls
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Analysis system description:	Windows 10 64 bit version 1909 (MS Office 2019, IE 11, Chrome 104, Firefox 88, Adobe Reader DC 21, Java 8 u291, 7-Zip)
Number of analysed new started processes analysed:	19
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.expl.evad.winXLS@11/15@4/59
EGA Information:	• Successful, ratio: 50%
HDC Information:	• Successful, ratio: 67.7% (good quality ratio 58.8%) • Quality average: 65.2% • Quality standard deviation: 35.3%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .xls

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, RuntimeBroker.exe, SIHClient.exe, backgroundTaskHost.exe, SgrmBroker.exe, usocoreworker.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded IPs from analysis (whitelisted): 52.109.76.141, 52.109.77.0, 52.113.194.132, 52.109.89.14, 88.221.168.226, 13.69.239.73
- Excluded domains from analysis (whitelisted): slscr.update.microsoft.com, eur.roaming1.live.com.akadns.net, fs-wildcard.microsoft.com.edgekey.net, fs-wildcard.microsoft.com.edgekey.net.globalredir.akadns.net, ecs-office.s-0005.s-msedge.net, roaming.officeapps.live.com, login.live.com, e16604.g.akamaiedge.net, onedscolprdneu03.northeurope.cloudapp.azure.com, officeclient.microsoft.com, prod.fs.microsoft.com.akadns.net, ecs.office.com, self-events-data.trafficmanager.net, client.wns.windows.com, fs.microsoft.com, prod.configsvc1.live.com.akadns.net, self.events.data.microsoft.com, ctldl.windowsupdate.com, prod.roaming1.live.com.akadns.net, s-0005-office.config.skype.com, prod.nexusrules.live.com.akadns.net, s-0005.s-msedge.net, config.officeapps.live.com, ecs.office.trafficmanager.net, nexusrules.officeapps.live.com, europe.configsvc1.live.com.akadns.net
- Report size getting too big, too many NtCreateFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryAttributesFile calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
19:27:45	API Interceptor	6x Sleep call for process: regsvr32.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\FontCache\4\Catalog\ListAll.Json

Process:	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE
File Type:	JSON data
Category:	dropped
Size (bytes):	379722
Entropy (8bit):	4.9088149211082355
Encrypted:	false
SSDEEP:	1536:MApDpphudnceJZezca9uRszBEmj6QkjfoJ5Jj7DMnDAYRbLSm5rYOLdHKmC9:IDThumeGzcTRszB7DkjfaJj76RbNbLW9
MD5:	E9FB5A0DF105C6F7F80E8B650DF56AAB
SHA1:	0B7F6ADA05673F2535E61267C3CB428489ECEB55
SHA-256:	A24470762A1F9F5F069C0F70EF53D693D08B7C99797935800FF294BD3B2566F3
SHA-512:	65C83135CE550981ED88CB4A83127CB3C94D5C616F26B05185FCC129E5201A88EB0A1351D144E1511B50ADB388071BFCC60388FDD613EBBA5B202FFC76F7D42B
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	{"MajorVersion":4,"MinorVersion":17,"Expiration":14,"Fonts":[{"a":[4294966911],"f":"Abadi","fam":[],"sf":[{"c":[1,0],"dn":"Abadi","fs":32696,"ful":[{"lcp":983040,"lsc":"Latn","ltx":"Abadi"}],"gn":"Abadi","id":"23643452060","p":[2,11,6,4,2,1,4,2,2,4],"sub":[],"t":"ttf","u":[2147483651,0,0,0],"v":197263,"w":26215680},{"c":[1,0],"dn":"Abadi Extra Light","fs":22180,"ful":[{"lcp":983041,"lsc":"Latn","ltx":"Abadi Extra Light"}],"gn":"Abadi Extra Light","id":"17656736728","p":[2,11,2,4,2,1,4,2,2,4],"sub":[],"t":"ttf","u":[2147483651,0,0,0],"v":197263,"w":13108480}]},{"a":[4294966911],"f":"Agency FB","fam":[],"sf":[{"c":[536870913,0],"dn":"Agency FB Bold","fs":54372,"ful":[{"lcp":983042,"lsc":"Latn","ltx":"Agency FB"}],"gn":"Agency FB","id":"31150835240","p":[2,11,8,4,2,2,2,2,2,4],"sub":[],"t":"ttf","u":[3,0,0,0],"v":67502,"w":45875968},{"c":[536870913,0],"dn":"Agency FB","fs":52680,"ful":[{"lcp":983042,"lsc":"Latn","ltx":"Agency FB"}],"gn":"Agency FB","id":"29260917085","p":[2,11,5,3,2,2,2,2,

C:\Users\user\AppData\Local\Microsoft\FontCache\4\PreviewFont\flat_officeFontsPreview.ttf

Process:	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE
File Type:	TrueType Font data, 10 tables, 1st "OS/2", 7 names, Microsoft, language 0x409, \251 2018 Microsoft Corporation. All Rights Reserved.msofp_4_17RegularVersion 4.17;O365
Category:	dropped
Size (bytes):	672416
Entropy (8bit):	6.566110770587873
Encrypted:	false
SSDEEP:	12288:/3zUbLds556T1BEFGHtASk3+/KLQ/zp1km/WJ1ov0mPqxXE/RoVZPE9Ob:/Qfds5opwSL1kovT92
MD5:	4DFB7AADD4771ADDF1BA168C12DEDBF3
SHA1:	B379DC0E19FE0F51E77305BE0A7F3421B80E8A0F
SHA-256:	DB9B46CC2132D76EF90CA9A59AF03CB478BB91EA2CDA3E8E42DD0801873416E2
SHA-512:	1C5AE2C794017A81A4232A2EF43725A0DA30F9672123940D85D34A4A77744D2D7ECA5FFE9A91E2FEDDBDBADE4EEAD6AB80E565C1F8FBB813C5A2BC25F7F0A359
Malicious:	false
Preview:	..... OS/29.P...(...`cmap.s.....pglyf..e.....0.head-@;;.....6hheaE.@B.....$hmtx.....ploca..@....h...tmaxp..... name.T+...A\|....post...<..B.... .....Me.._.<.....<.....Aa.x.....Q....Aa....Aa.....~.....j.....3.....MS .@.....(...Q..... .....d.....0...J.....8...>.....+a..#...,.....K.....z.....N.....*...!...-...+....z.....h..%^..3...&j..+...+%..".....l.....$A...,.....g...&...=.....X..&.....*.....&...(B.....#.....j.....+...P...5.@...).....#.....*...N...7.....<...;>.....].....5.....#....s.....$.....$.....^.....H.....%...7.....6.....O...V.....K.....c.....!.....$...&...*p..+<..+...-....q.....O.....F..(....5..0K..$...0V...k..*e...o.....S...*...0..0...*M.....9...

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\E9097BEB-F41B-41FA-A529-2854DCDBD67E

Process:	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE

File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	150846
Entropy (8bit):	5.357322582686688
Encrypted:	false
SSDEEP:	1536:h+C7/gd3B4BQguw//Q9DQe+zQVk4F77nXmvidOXRsEwrNz6S:BHQ9DQe+zbXza
MD5:	322904D0B0020748A8ABC41788D78D9F
SHA1:	4CD879E03CEA5D5FEAEAB7BD9614BD392BADD8D1
SHA-256:	BF4C38ADA89E2623EC0AE27071BA770C6B7AE2966C93717F05B109E2FEDD38E4
SHA-512:	B90C3082BCFB5DC3F0A4D5E653DAA94950B3D7CFF1B14864291DBBC0775DEB5081F81033C916EA78C6E3A36F3CCCC22C612B0D158769E6C6A7FDA891CE33C C5
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2022-11-13T18:26:46">.. Build: 16.0.15905.30525-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:u rl>https://rr.office.microsoft.com/research/query.asmx</o:url>.. </o:service>.. <o:service o:name="ORedir">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ORedirSSL">.. <o:url>https://o15.officeredir.microsoft.com/r</o:url>.. </o:service>.. <o:service o:name="ClViewClientHelpId" o:au thentication="1">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. <o:ticket o:policy="MBI_SSL_SHORT" o:idprovider="1" o:target="[MAX.AuthHost]" o:h eaderValue="Passport1.4 from-PP='{}&p=''" />.. <o:ticket o:idprovider="3" o:headerValue="Bearer {}" o:resourceId="[MAX.ResourceId]" o:authorityUrl="[ADALAu thorityU

C:\Users\user\AppData\Local\Microsoft\Office\16.0\excel.exe_Rules.xml

Process:	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE
File Type:	XML 1.0 document, ASCII text, with very long lines (65536), with no line terminators
Category:	dropped
Size (bytes):	338423
Entropy (8bit):	5.1629516010869905
Encrypted:	false
SSDEEP:	1536:42/zodZJr6KP+1u6uSivsUQK75IthK8nF2XuN:VOr6KP+1u6uSivsUQK75IthYXU
MD5:	4FF54C343D309A7F69BD16B392F8C3A3
SHA1:	AC4012E403854396974652804E46E5406B23E492
SHA-256:	DBD62290F655ACCC6686A46A62909475980AA09102B3A0D7BAF2278B4DBA56AC
SHA-512:	0268D2B5D833AECB6AD08619F8C08254958978C66CEE156B61A52FE442AB5DB0F9BD12FF9D3CFC1C2E2A2858A8D8D32D2AE361DF3D9610E135A97A12664E0E 9B
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?><Rules xmlns="urn:Rules"><R Id="1000" V="5" DC="ESM" EN="Office.Telemetry.RuleErrorsAggregated" ATT="f998cc5ba4d 448d6a1e8e913ff18be94-dd122e0a-fcf8-4dc5-9dbb-6afac5325183-7405" SP="CriticalBusinessImpact" S="70" DL="A" DCa="PSP PSU" xmlns=""><S><Etw T="1" E="159 " G="{02fd33df-f746-4a10-93a0-2bc6273bc8e4}" /><F T="2"><O T="AND"><L><O T="NE"><L><S T="1" F="Warning" /></L><R><V V="37" T="U32" /></R></O></L> <R><O T="NE"><L><S T="1" F="Warning" /></L><R><V V="29" T="U32" /></R></O></R></O></F><TI T="3" I="10min" /><A T="4" E="TelemetrySuspend" /><A T="5" E="TelemetryShutdown" /></S><G I="true" R="TriggerOldest"><S T="2"><F N="RuleID" /><F N="RuleVersion" /><F N="Warning" /><F N="Info" /></S></G><C T="U32" I="0" O="false" N="ErrorCount"><C><S T="2" /></C></C><C T="U32" I="1" O="false" N="ErrorRuleId"><S T="2" F="RuleID" /></C><C T="U16" I="2" O="false" N=" ErrorRuleVersion"><S T="2" F="RuleVersion" /></C><C T="U8" I="3" O="false" N="WarningInfo"><S T="2"

C:\Users\user\AppData\Local\Microsoft\TokenBroker\Cache\089d66ba04a8cec4bdc5267f42f39cf84278bb67.tbres

Process:	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	2278
Entropy (8bit):	3.8418307979091164
Encrypted:	false
SSDEEP:	48:uiTrlKxsxxHxl9ll8utFJfX3b5y2R1eN66LY0d1rc:vTYrFJfX4iQYz
MD5:	3AE033F53B76D362C4A93629A0419482
SHA1:	14ED84431F31521E6327C666D1D2EC766E392016
SHA-256:	8C47A04565A320D35B265549BC11BED0BDCB001BCC28028638B4C8330324A270
SHA-512:	140863AA0784A3A57F4E0F9C0020A895E5D3FAE80ADF5F01EF80CA346B5C8CE4293FD788C0C43B685E3BD1BFD953A8155DF1E4AA647D3CCEA8C39F49AAD10 E26
Malicious:	false
Preview:	{.".T.B.D.a.t.a.S.t.o.r.e.O.b.j.e.c.t.".:.{.".H.e.a.d.e.r.".:.{.".O.b.j.e.c.t.T.y.p.e.".:.".T.o.k.e.n.R.e.s.p.o.n.s.e.".,.".S.c.h.e.m.a.V.e.r.s.i.o.n.M.a.j.o.r.".:.2.,.".S.c.h.e.m.a.V.e.r.s. i.o.n.M.i.n.o.r.".:.1.},.,".O.b.j.e.c.t.D.a.t.a.".:.{.".S.y.s.t.e.m.D.e.f.i.n.e.d.P.r.o.p.e.r.t.i.e.s.".:.{.".R.e.q.u.e.s.t.I.n.d.e.x.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c. t.e.d.".:.f.a.l.s.e.,.".V.a.l.u.e.".:.".C.J.1.m.u.g.S.o.z.s.S.9.x.S.Z./.Q.v.O.c.+.E.J.4.u.2.c.=.".},.,".E.x.p.i.r.a.t.i.o.n.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:. f.a.l.s.e.,.".V.a.l.u.e.".:.".g.O.I.i.4.J.X.3.2.A.E.=.".},.,".S.t.a.t.u.s.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.f.a.l.s.e.,.".V.a.l.u.e.".:.".A.A.A.A.A.A.=.=.".}. ,.".R.e.s.p.o.n.s.e.B.y.t.e.s.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.t.r.u.e.,.".V.a.l.u.e.".:.".A.Q.A.A.A.N.C.M.n.d.8.B.F.d.E.R.j.H.o.A.w.E./.C.l.+.s.B. A.A.A.A.B.4.7.F.9.z.

C:\Users\user\AppData\Local\Microsoft\TokenBroker\Cache\5475cb191e478c39370a215b2da98a37e9dc813d.tbres

Process:	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE

File Type:	data
Category:	dropped
Size (bytes):	2684
Entropy (8bit):	3.907754828884943
Encrypted:	false
SSDEEP:	48:uiTrlKxJx+xl9Il8uaz7HYRtKu9pEV2EpNYn549Ymca2d/vc:vYMPHQGV2EpNaYnT
MD5:	25F51D45674CF9EC3EEEFA2D89F736B0
SHA1:	50A2C33FE720343EDFFC4DCBA09F832901FD819A
SHA-256:	46DC8D20C16586691C4ED93B0B45AE530C67837B927BD79314D4EA62FD1C4FDE
SHA-512:	D8D4709354EC7D3A66CB79CA0C3DF507B67CEF3B4AD63344694DAA5FB03C99F8A88A81659E1B53F949167B929AF0B5DD7A9C94044D460F21C1757466065CA5D
Malicious:	false
Preview:	{.".T.B.D.a.t.a.S.t.o.r.e.O.b.j.e.c.t.".:.{.".H.e.a.d.e.r.".:.{.".O.b.j.e.c.t.T.y.p.e.".:.".T.o.k.e.n.R.e.s.p.o.n.s.e.".,.".S.c.h.e.m.a.V.e.r.s.i.o.n.M.a.j.o.r.".:.2.,.".S.c.h.e.m.a.V.e.r.s.i.o.n.M.i.n.o.r.".:.1.},.,".O.b.j.e.c.t.D.a.t.a.".:.{.".S.y.s.t.e.m.D.e.f.i.n.e.d.P.r.o.p.e.r.t.i.e.s.".:.{.".R.e.q.u.e.s.t.I.n.d.e.x.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.f.a.l.s.e.,.".V.a.l.u.e.".:.".V.H.X.L.G.R.5.H.j.D.k.3.C.i.F.b.L.a.m.K.N.+.n.c.g.T.0.=.".},.".E.x.p.i.r.a.t.i.o.n.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.f.a.l.s.e.,.".V.a.l.u.e.".:.".F.+.R.0.9.1.4.W.2.g.E.=.".},.,".S.t.a.t.u.s.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.f.a.l.s.e.,.".V.a.l.u.e.".:.".A.A.A.A.A.A.=.=.".},.,".R.e.s.p.o.n.s.e.B.y.t.e.s.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.t.r.u.e.,.".V.a.l.u.e.".:.".A.Q.A.A.A.N.C.M.n.d.8.B.F.d.E.R.j.H.o.A.w.E./.C.I.+.s.B.A.A.A.A.B.4.7.F.9.z.

C:\Users\user\AppData\Local\Microsoft\TokenBroker\Cache\9aad439831564ef9f88438a70a63c87e26ef3852.tbres

Process:	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	3902
Entropy (8bit):	3.9837858181337045
Encrypted:	false
SSDEEP:	96:GzYVH0Ed0sgxZ/xv8uyIefnFVIaBy5LgVtNKrkqq:6pEerxhxvxyIGVyFgVt8Lq
MD5:	B14B26190EE6FABE32EAB2F9EE926454
SHA1:	84F8AE7E2451837C856F2ABF6AC98CD24B0B4EE9
SHA-256:	071A156E540064BA81D051C98C3F2317E0ECE6440D2C76E6E5A40F17959B9983
SHA-512:	E437437F20A6B6D8CE7FB1BDB73E5001F1B85D7A678202A98DB56D282C17FE712159BD276AE307E5130F546B1CB0D7CA820398E561B059FDBC63DFB2C9EE38ED
Malicious:	false
Preview:	{.".T.B.D.a.t.a.S.t.o.r.e.O.b.j.e.c.t.".:.{.".H.e.a.d.e.r.".:.{.".O.b.j.e.c.t.T.y.p.e.".:.".T.o.k.e.n.R.e.s.p.o.n.s.e.".,.".S.c.h.e.m.a.V.e.r.s.i.o.n.M.a.j.o.r.".:.2.,.".S.c.h.e.m.a.V.e.r.s.i.o.n.M.i.n.o.r.".:.1.},.,".O.b.j.e.c.t.D.a.t.a.".:.{.".S.y.s.t.e.m.D.e.f.i.n.e.d.P.r.o.p.e.r.t.i.e.s.".:.{.".R.e.q.u.e.s.t.I.n.d.e.x.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.f.a.l.s.e.,.".V.a.l.u.e.".:.".m.q.1.D.m.D.F.W.T.v.n.4.h.D.i.n.C.m.P.I.f.i.b.v.O.F.I.=.".},.".E.x.p.i.r.a.t.i.o.n.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.f.a.l.s.e.,.".V.a.l.u.e.".:.".z.I.W.6.x.Y.3.3.2.A.E.=.".},.,".S.t.a.t.u.s.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.f.a.l.s.e.,.".V.a.l.u.e.".:.".A.w.A.A.A.A.=.=.".},.,".R.e.s.p.o.n.s.e.B.y.t.e.s.".:.{.".T.y.p.e.".:.".I.n.l.i.n.e.B.y.t.e.s.".,.".I.s.P.r.o.t.e.c.t.e.d.".:.t.r.u.e.,.".V.a.l.u.e.".:.".A.Q.A.A.A.N.C.M.n.d.8.B.F.d.E.R.j.H.o.A.w.E./.C.I.+.s.B.A.A.A.A.B.4.7.F.9.z.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\98S549LJ\o0oHPECmC0WPIXcvQPJOXzFOO7w00z7mkDO[1].dll

Process:	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	433152
Entropy (8bit):	6.773063357716462
Encrypted:	false
SSDEEP:	6144:PZUCuTJlyIOziaTGy+IeIt1xJh5eWhv/w62LcuPv8cD4mRKqdONyAzDxkMwp2/uw:Py7EzZ4+HvY62LxHJ4KTGDIT
MD5:	DD7105E9748A29B5BD61EA57214D57E3
SHA1:	827B323BDA769BA7FB838A231AA4160209266B14
SHA-256:	C987AD0CC79B598BDEE9EC7DA96B07E82A04CADD73CB3CAF85B799731DEEF9A1
SHA-512:	BECA102422697E4CD50B81289BDC5097935F11C0C5ACC86B7A69893FB819A3CD225E4B2594A2BB40163FBD68D7AC281B0FF260F30B55CF188112445EB26986B
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....?...I...I...I...I...I...I../...I..2I...I.."I...I...I...I...I...I..*I...I..+I...I...I...IRich..I.....PE..d....)mc....." .....[.....@.....pg..W....\..d.....T..... ..8.....text..... ..`.rdata...G... ...H.....@..@.data..../...p.....N.....@....pdata.....j.....@..@text.....@.. .rsrc...T.....@..@.reloc.....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\CE8D676K\EvvmhfKiKFhKrSuHfBq[1].dll

Process:	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	433152

Entropy (8bit):	6.7730613530277655
Encrypted:	false
SSDEEP:	6144:PZUCuTJlyIOziaTGy+IeIt1xJh5eWhv/w62LcuPv8cD4mRKqdONyAzDxkMwp2/uz:Py7EzZ4+HvY62LxHJ4KTGDIT
MD5:	3929B889987F447CB837ED326860AFC6
SHA1:	9BB1A7622F2BC5A6A51487434A77F395DE5E50D7
SHA-256:	B2AA99DEF35F913B42B882122C8DD5F72CEEAB82F6747F1B659C8632CD6EB902
SHA-512:	EF4DB4F06EE1F85AB96AA70FC5DD05A062DA6A5D13F9A643AFE471F6FDC9FEA62FF39F3C951286B7A865C66C53E0E73FD84E2E5030E1843F24FE014CE7BA9715
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....?...I..I..I..I..I..I..I../I..I..2I...I.."I..I..I..I..I..I..*I..I..+I..I..I...IRich.. .I.....PE..d....)mc....." .....[.....@.....pg..W....\..d.....T..... ..8.....text..... ..`.rdata...G... ...H.....@..@.data..../...p.....N.....@....pdata.....j.....@..@text.....@.. .rsrc...T.....@..@.reloc.....@..B..... .....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\PO0000001552.LNK

Process:	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Tue Aug 30 12:46:13 2022, mtime=Sun Nov 13 17:26:48 2022, atime=Sun Nov 13 17:26:48 2022, length=93184, window=hide
Category:	dropped
Size (bytes):	527
Entropy (8bit):	4.687349495162638
Encrypted:	false
SSDEEP:	6:4xtQl37wc4esXsbxSXzK9wm2PholjAlpYelsgFUiILlaWUdPFmJXSZXASzZXyav8:87c4xsbx4zK9wm2SjA0Jaldi3Fm2
MD5:	732950BB2A1CFEF84B6969CFFE0ABDE7
SHA1:	D674D7EFF59B48E8A8749F8D5C2801B6E3CE87DA
SHA-256:	6FDB0C9FA6FC38384EE7B77C0D481EBF5F9D771C29739A7DAF62E54626568E28
SHA-512:	290B32795635A528AD9CF40553B7ABFB6D44CD2558C4DF37F92E30B585562982D4E60253F7CE6F55F95BE5F8C6AC4ABEC0C1ABE45148FCB66C9D6BD9BE40A4CB
Malicious:	false
Preview:	L.....F.... ....:..v...(.!~.....R.~.....I.....p.n.2..I..mUU. .PO0000~1.XLS..R.....U.mmUU.....^.....q...P.O.0.0.0.0.0.0.1.5.5.2...x.l.s.....X.....-.... ...W.....;S.....C:\Users\user\Desktop\PO0000001552.xls..'.....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.P.O.0.0.0.0.0.0.1.5.5.2...x.l.s.`.....X.....134349.....N...n..O...}R.....i(... .....N...n..O...}R.....i(.....E.....9...1SPS..mD..pH.H@..=x.....h....H....F.5./EG.gM.U.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat

Process:	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE
File Type:	Generic INItialization configuration [xls]
Category:	dropped
Size (bytes):	75
Entropy (8bit):	4.363995491825093
Encrypted:	false
SSDEEP:	3:bDuMJltOvCpulmMYdvCpulv:bCmOaEYdac
MD5:	F9CBF4D309E73196DBCB3C5F14717F77
SHA1:	26353BE9CD1B9EBDCE83B69267B48D80472BC7A6
SHA-256:	7CB5B3C956A55B3E4A70A8DA7615CAF7D7960B89BFE00C0EC8553680BF87150F
SHA-512:	47D359B978738F514DD3735DF520D1ACF9A55EAAF49C9A30D902342F345D74CCA24D323ABD0CC75CE7C2AAB3CA0FBACD2E62F07624AF55501CA39355E8EB52B
Malicious:	false
Preview:	[folders]..Templates.LNK=0..PO0000001552.LNK=0..[xls]..PO0000001552.LNK=0..

C:\Users\user\elv2.ooocccxxx

Process:	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	433152
Entropy (8bit):	6.7730613530277655
Encrypted:	false
SSDEEP:	6144:PZUCuTJlyIOziaTGy+IeIt1xJh5eWhv/w62LcuPv8cD4mRKqdONyAzDxkMwp2/uz:Py7EzZ4+HvY62LxHJ4KTGDIT
MD5:	3929B889987F447CB837ED326860AFC6
SHA1:	9BB1A7622F2BC5A6A51487434A77F395DE5E50D7
SHA-256:	B2AA99DEF35F913B42B882122C8DD5F72CEEAB82F6747F1B659C8632CD6EB902

SHA-512:	EF4DB4F06EE1F85AB96AA70FC5DD05A062DA6A5D13F9A643AFE471F6FDC9FEA62FF39F3C951286B7A865C66C53E0E73FD84E2E5030E1843F24FE014CE7BA97 15
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....?...I...I...I...I...I...I../I...I..2I...I.."I...I...I...I...I...I..*I...I..+I...I...I...IRich.. .I.....PE..d....)mc....." .....[.....@.....pg..W....\..d.....T..... ..8.....text..... ..`.rdata...G... ...H.....@..@.data..../...p.....N.....@....pdata.....j.....@..@text.....@.. .rsrc...T.....@..@.reloc.....@..B..... .....

C:\Users\user\elv3.oooccсxxx

Process:	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	433152
Entropy (8bit):	6.773063357716462
Encrypted:	false
SSDEEP:	6144:PZUCuTJlyIOziaTGy+IeIt1xJh5eWhv/w62LcuPv8cD4mRKqdONyAzDxkMwp2/uw:Py7EzZ4+HvY62LxHJ4KTGDIT
MD5:	DD7105E9748A29B5BD61EA57214D57E3
SHA1:	827B323BDA769BA7FB838A231AA4160209266B14
SHA-256:	C987AD0CC79B598BDEE9EC7DA96B07E82A04CADD73CB3CAF85B799731DEEF9A1
SHA-512:	BECA102422697E4CD50B81289BDC5097935F11C0C5ACC86B7A69893FB819A3CD225E4B2594A2BB40163FBD68D7AC281B0FF260F30B55CF188112445EB26986B
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....?...I...I...I...I...I...I../I...I..2I...I.."I...I...I...I...I...I..*I...I..+I...I...I...IRich.. .I.....PE..d....)mc....." .....[.....@.....pg..W....\..d.....T..... ..8.....text..... ..`.rdata...G... ...H.....@..@.data..../...p.....N.....@....pdata.....j.....@..@text.....@.. .rsrc...T.....@..@.reloc.....@..B..... .....

C:\Windows\System32\GanZhs\FrugrCuQjdEr.dll (copy)

Process:	C:\Windows\System32\regsvr32.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	433152
Entropy (8bit):	6.773063357716462
Encrypted:	false
SSDEEP:	6144:PZUCuTJlyIOziaTGy+IeIt1xJh5eWhv/w62LcuPv8cD4mRKqdONyAzDxkMwp2/uw:Py7EzZ4+HvY62LxHJ4KTGDIT
MD5:	DD7105E9748A29B5BD61EA57214D57E3
SHA1:	827B323BDA769BA7FB838A231AA4160209266B14
SHA-256:	C987AD0CC79B598BDEE9EC7DA96B07E82A04CADD73CB3CAF85B799731DEEF9A1
SHA-512:	BECA102422697E4CD50B81289BDC5097935F11C0C5ACC86B7A69893FB819A3CD225E4B2594A2BB40163FBD68D7AC281B0FF260F30B55CF188112445EB26986B
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....?...I...I...I...I...I...I../I...I..2I...I.."I...I...I...I...I...I..*I...I..+I...I...I...IRich.. .I.....PE..d....)mc....." .....[.....@.....pg..W....\..d.....T..... ..8.....text..... ..`.rdata...G... ...H.....@..@.data..../...p.....N.....@....pdata.....j.....@..@text.....@.. .rsrc...T.....@..@.reloc.....@..B..... .....

C:\Windows\System32\XEzXl\JZazaZgAOY.dll (copy)

Process:	C:\Windows\System32\regsvr32.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	433152
Entropy (8bit):	6.7730613530277655
Encrypted:	false
SSDEEP:	6144:PZUCuTJlyIOziaTGy+IeIt1xJh5eWhv/w62LcuPv8cD4mRKqdONyAzDxkMwp2/uz:Py7EzZ4+HvY62LxHJ4KTGDIT
MD5:	3929B889987F447CB837ED326860AFC6
SHA1:	9BB1A7622F2BC5A6A51487434A77F395DE5E50D7
SHA-256:	B2AA99DEF35F913B42B882122C8DD5F72CEEAB82F6747F1B659C8632CD6EB902
SHA-512:	EF4DB4F06EE1F85AB96AA70FC5DD05A062DA6A5D13F9A643AFE471F6FDC9FEA62FF39F3C951286B7A865C66C53E0E73FD84E2E5030E1843F24FE014CE7BA97 15
Malicious:	false

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....?...I...I...I...I...I...I../...I..2I...I.."I...I...I...I...I...I..*I...I..+I...I...I...IRich.. .I.....PE..d....)mc....." .....[.....@.....pg..W....\..d.....T..... ..8.....text..... ..`.rdata...G... ...H.....@..@.data..../...p.....N.....@....pdata.....j.....@..@text.....@.. .rsrc...T.....@..@.reloc.....@..B.....

Static File Info

General

File type:	Composite Document File V2 Document, Little Endian, Os: Windows, Version 10.0, Code page: 1251, Author: Gydar, Last Saved By: Gydar, Name of Creating Application: Microsoft Excel, Create Time/Date: Fri Jun 5 19:19:34 2015, Last Saved Time/Date: Thu Nov 10 07:26:07 2022, Security: 0
Entropy (8bit):	5.506793373203057
TrID:	• Microsoft Excel sheet (30009/1) 78.94% • Generic OLE2 / Multistream Compound File (8008/1) 21.06%
File name:	PO0000001552.xls
File size:	93184
MD5:	ecdc3f1e9afd2ce212a12ba3a844f521
SHA1:	0121ba555dfe0b42834759d201cce505bd619f86
SHA256:	1e494fd9ec670e351dd80258489770ffa43ee6f4be3e14c797f7ce64ae8e9d43
SHA512:	0b3f8566d8e4c49a0698f398e1d1e95ba6f750ccc25f204b1e9526ff6ef6f81e3131f70779ee88365ad65851d21ddeaefd20dab203cdba39b24c1d1a920dec9e
SSDEEP:	1536:vKpb8rGYrMPe3q7Q0XV5xtezEsi8/dgHbCXuZH4gb4CEn9J4ZvX5:vKpb8rGYrMPe3q7Q0XV5xtezEsi8/dgF
TLSH:	3B933A86B2F9D89DEA19C734889B4390A762EC204B564BCB3244F3A67FB0D501F539D7
File Content Preview:	.....>.....

File Icon



Icon Hash:	74f4e4c2cec4c0d4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "PO0000001552.xls"

Indicators

Has Summary Info:	
Application Name:	Microsoft Excel
Encrypted Document:	False
Contains Word Document Stream:	False
Contains Workbook/Book Stream:	True
Contains PowerPoint Document Stream:	False
Contains Visio Document Stream:	False
Contains ObjectPool Stream:	False
Flash Objects Count:	0
Contains VBA Macros:	False

Summary

Code Page:	1251
Author:	
Last Saved By:	
Create Time:	2015-06-05 18:19:34
Last Saved Time:	2022-11-10 07:26:07
Creating Application:	
Security:	0

Document Summary

Document Code Page:	1251
Thumbnail Scaling Desired:	False
Company:	
Contains Dirty Links:	False
Shared Document:	False
Changed Hyperlinks:	False
Application Version:	1048576

Streams

Stream Path: \x5DocumentSummaryInformation, File Type: data, Stream Size: 4096

General	
Stream Path:	\x5DocumentSummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.3985130586395627
Base64 Encoded:	False
Data ASCII:	. . . . . + , 0 . . . $ . . . . . P . . . . . X . . . . . d . . . . . l . . . . . t . . . . . | . . . . . S h e e t 1 . . . . . S h e e t 2 . . . . . S h e e t 3 . . . . . S h e e t 4 . . . . . S h e e t 5 . . . . . S h e e t 6 . . . . . S h e
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 02 d5 cd d5 9c 2e 1b 10 93 97 08 00 2b 2c f9 ae 30 00 00 00 24 01 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 e1 00 00 00

Stream Path: \x5SummaryInformation, File Type: data, Stream Size: 4096

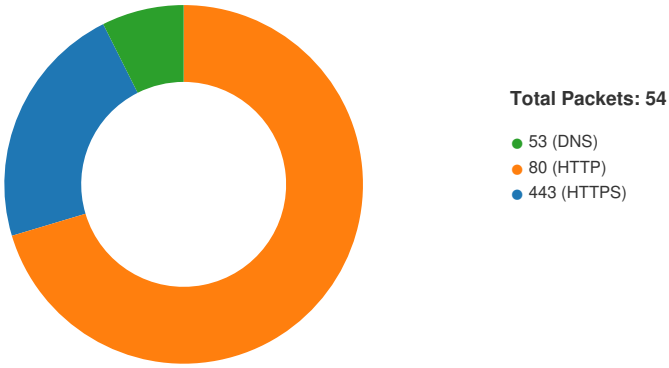
General	
Stream Path:	\x5SummaryInformation
File Type:	data
Stream Size:	4096
Entropy:	0.2784985381370367
Base64 Encoded:	False
Data ASCII:	. . . . . O h . . . + ' 0 . . . . . @ . . . . . H . . . . . X . . . . . h . . . . . G y d a r . . . . . G y d a r . . . . . M i c r o s o f t E x c e l . @ . . . . ? R , . @ . . . . .
Data Raw:	fe ff 00 00 0a 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00 e0 85 9f f2 f9 4f 68 10 ab 91 08 00 2b 27 b3 d9 30 00 00 00 a0 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 58 00 00 00 12 00 00 00 68 00 00 00 0c 00 00 00 80 00 00 00 0d 00 00 00 8c 00 00 00 13 00 00 00 98 00 00 00 02 00 00 00 e3 04 00 00 1e 00 00 00 08 00 00 00

Stream Path: Workbook, File Type: Applesoft BASIC program data, first line number 16, Stream Size: 82874

General	
Stream Path:	Workbook
File Type:	Applesoft BASIC program data, first line number 16
Stream Size:	82874
Entropy:	5.92856896968195
Base64 Encoded:	True
Data ASCII:	. . . . . Z O . . . . . \ \ . p . . . . G y d a r B . . . . a . . . . . = ... P . 8 . . . . . X . @ . . . . . " . . . . .
Data Raw:	09 08 10 00 00 06 05 00 5a 4f cd 07 c9 00 02 00 06 08 00 00 e1 00 02 00 b0 04 c1 00 02 00 00 00 e2 00 00 00 5c 00 70 00 05 00 00 47 79 64 61 72 20 20 20

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
192.168.2.31.1.1.1631775 32023883 11/13/22-19:27:02.730666	UDP	2023883	ET DNS Query to a *.top domain - Likely Hostile	63177	53	192.168.2.3	1.1.1.1
192.168.2.3173.255.211.88497054324043144 11/13/22-19:27:33.992872	TCP	2404314	ET CNC Feodo Tracker Reported CnC Server TCP group 8	49705	443	192.168.2.3	173.255.211.88

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 13, 2022 19:26:49.746951103 CET	49697	443	192.168.2.3	175.98.167.165
Nov 13, 2022 19:26:49.746999025 CET	443	49697	175.98.167.165	192.168.2.3
Nov 13, 2022 19:26:49.747102022 CET	49697	443	192.168.2.3	175.98.167.165
Nov 13, 2022 19:26:49.748613119 CET	49697	443	192.168.2.3	175.98.167.165
Nov 13, 2022 19:26:49.748639107 CET	443	49697	175.98.167.165	192.168.2.3
Nov 13, 2022 19:26:50.236835957 CET	443	49697	175.98.167.165	192.168.2.3
Nov 13, 2022 19:26:50.237086058 CET	49697	443	192.168.2.3	175.98.167.165
Nov 13, 2022 19:26:50.285685062 CET	49697	443	192.168.2.3	175.98.167.165
Nov 13, 2022 19:26:50.285739899 CET	443	49697	175.98.167.165	192.168.2.3
Nov 13, 2022 19:26:50.286483049 CET	443	49697	175.98.167.165	192.168.2.3
Nov 13, 2022 19:26:50.286737919 CET	49697	443	192.168.2.3	175.98.167.165
Nov 13, 2022 19:26:50.287277937 CET	49697	443	192.168.2.3	175.98.167.165
Nov 13, 2022 19:26:50.287300110 CET	443	49697	175.98.167.165	192.168.2.3
Nov 13, 2022 19:26:50.694597006 CET	443	49697	175.98.167.165	192.168.2.3
Nov 13, 2022 19:26:50.694730997 CET	443	49697	175.98.167.165	192.168.2.3
Nov 13, 2022 19:26:50.694792032 CET	49697	443	192.168.2.3	175.98.167.165
Nov 13, 2022 19:26:50.694830894 CET	49697	443	192.168.2.3	175.98.167.165
Nov 13, 2022 19:26:50.696415901 CET	49697	443	192.168.2.3	175.98.167.165
Nov 13, 2022 19:26:50.696441889 CET	443	49697	175.98.167.165	192.168.2.3
Nov 13, 2022 19:26:50.696466923 CET	49697	443	192.168.2.3	175.98.167.165
Nov 13, 2022 19:26:50.696533918 CET	49697	443	192.168.2.3	175.98.167.165
Nov 13, 2022 19:26:51.585938931 CET	49699	80	192.168.2.3	47.92.35.35
Nov 13, 2022 19:26:51.794390917 CET	80	49699	47.92.35.35	192.168.2.3
Nov 13, 2022 19:26:51.794640064 CET	49699	80	192.168.2.3	47.92.35.35
Nov 13, 2022 19:26:51.795133114 CET	49699	80	192.168.2.3	47.92.35.35
Nov 13, 2022 19:26:51.994139910 CET	80	49699	47.92.35.35	192.168.2.3
Nov 13, 2022 19:26:52.000014067 CET	80	49699	47.92.35.35	192.168.2.3
Nov 13, 2022 19:26:52.000138044 CET	80	49699	47.92.35.35	192.168.2.3
Nov 13, 2022 19:26:52.000183105 CET	49699	80	192.168.2.3	47.92.35.35
Nov 13, 2022 19:26:52.000225067 CET	80	49699	47.92.35.35	192.168.2.3
Nov 13, 2022 19:26:52.000261068 CET	49699	80	192.168.2.3	47.92.35.35

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 13, 2022 19:26:52.000277042 CET	49699	80	192.168.2.3	47.92.35.35
Nov 13, 2022 19:26:52.000313997 CET	80	49699	47.92.35.35	192.168.2.3
Nov 13, 2022 19:26:52.000363111 CET	49699	80	192.168.2.3	47.92.35.35
Nov 13, 2022 19:26:52.000385046 CET	80	49699	47.92.35.35	192.168.2.3
Nov 13, 2022 19:26:52.000435114 CET	49699	80	192.168.2.3	47.92.35.35
Nov 13, 2022 19:26:52.000454903 CET	80	49699	47.92.35.35	192.168.2.3
Nov 13, 2022 19:26:52.000504017 CET	49699	80	192.168.2.3	47.92.35.35
Nov 13, 2022 19:26:52.000525951 CET	80	49699	47.92.35.35	192.168.2.3
Nov 13, 2022 19:26:52.000581980 CET	80	49699	47.92.35.35	192.168.2.3
Nov 13, 2022 19:26:52.000592947 CET	49699	80	192.168.2.3	47.92.35.35
Nov 13, 2022 19:26:52.000633001 CET	49699	80	192.168.2.3	47.92.35.35
Nov 13, 2022 19:26:52.000658989 CET	80	49699	47.92.35.35	192.168.2.3
Nov 13, 2022 19:26:52.000716925 CET	80	49699	47.92.35.35	192.168.2.3
Nov 13, 2022 19:26:52.000727892 CET	49699	80	192.168.2.3	47.92.35.35
Nov 13, 2022 19:26:52.000770092 CET	49699	80	192.168.2.3	47.92.35.35
Nov 13, 2022 19:26:52.194159031 CET	80	49699	47.92.35.35	192.168.2.3
Nov 13, 2022 19:26:52.194242954 CET	80	49699	47.92.35.35	192.168.2.3
Nov 13, 2022 19:26:52.194303036 CET	80	49699	47.92.35.35	192.168.2.3
Nov 13, 2022 19:26:52.194353104 CET	80	49699	47.92.35.35	192.168.2.3
Nov 13, 2022 19:26:52.194401026 CET	80	49699	47.92.35.35	192.168.2.3
Nov 13, 2022 19:26:52.194463015 CET	80	49699	47.92.35.35	192.168.2.3
Nov 13, 2022 19:26:52.194478035 CET	49699	80	192.168.2.3	47.92.35.35
Nov 13, 2022 19:26:52.194503069 CET	49699	80	192.168.2.3	47.92.35.35
Nov 13, 2022 19:26:52.194545031 CET	80	49699	47.92.35.35	192.168.2.3
Nov 13, 2022 19:26:52.194587946 CET	49699	80	192.168.2.3	47.92.35.35
Nov 13, 2022 19:26:52.194613934 CET	80	49699	47.92.35.35	192.168.2.3
Nov 13, 2022 19:26:52.194658995 CET	49699	80	192.168.2.3	47.92.35.35
Nov 13, 2022 19:26:52.194681883 CET	80	49699	47.92.35.35	192.168.2.3
Nov 13, 2022 19:26:52.194709063 CET	49699	80	192.168.2.3	47.92.35.35
Nov 13, 2022 19:26:52.194742918 CET	80	49699	47.92.35.35	192.168.2.3
Nov 13, 2022 19:26:52.194761038 CET	49699	80	192.168.2.3	47.92.35.35
Nov 13, 2022 19:26:52.194802999 CET	49699	80	192.168.2.3	47.92.35.35
Nov 13, 2022 19:26:52.194828987 CET	80	49699	47.92.35.35	192.168.2.3
Nov 13, 2022 19:26:52.194880962 CET	80	49699	47.92.35.35	192.168.2.3
Nov 13, 2022 19:26:52.194896936 CET	49699	80	192.168.2.3	47.92.35.35
Nov 13, 2022 19:26:52.194942951 CET	49699	80	192.168.2.3	47.92.35.35
Nov 13, 2022 19:26:52.194962978 CET	80	49699	47.92.35.35	192.168.2.3
Nov 13, 2022 19:26:52.195020914 CET	80	49699	47.92.35.35	192.168.2.3
Nov 13, 2022 19:26:52.195030928 CET	49699	80	192.168.2.3	47.92.35.35
Nov 13, 2022 19:26:52.195075989 CET	49699	80	192.168.2.3	47.92.35.35
Nov 13, 2022 19:26:52.195101976 CET	80	49699	47.92.35.35	192.168.2.3
Nov 13, 2022 19:26:52.195158958 CET	80	49699	47.92.35.35	192.168.2.3
Nov 13, 2022 19:26:52.195168972 CET	49699	80	192.168.2.3	47.92.35.35
Nov 13, 2022 19:26:52.195214033 CET	49699	80	192.168.2.3	47.92.35.35
Nov 13, 2022 19:26:52.195231915 CET	80	49699	47.92.35.35	192.168.2.3
Nov 13, 2022 19:26:52.195291042 CET	80	49699	47.92.35.35	192.168.2.3
Nov 13, 2022 19:26:52.195302010 CET	49699	80	192.168.2.3	47.92.35.35
Nov 13, 2022 19:26:52.195353985 CET	80	49699	47.92.35.35	192.168.2.3
Nov 13, 2022 19:26:52.195364952 CET	49699	80	192.168.2.3	47.92.35.35
Nov 13, 2022 19:26:52.195410967 CET	49699	80	192.168.2.3	47.92.35.35
Nov 13, 2022 19:26:52.195431948 CET	80	49699	47.92.35.35	192.168.2.3
Nov 13, 2022 19:26:52.195487976 CET	49699	80	192.168.2.3	47.92.35.35
Nov 13, 2022 19:26:52.385291100 CET	80	49699	47.92.35.35	192.168.2.3
Nov 13, 2022 19:26:52.385369062 CET	80	49699	47.92.35.35	192.168.2.3
Nov 13, 2022 19:26:52.385411978 CET	80	49699	47.92.35.35	192.168.2.3
Nov 13, 2022 19:26:52.385436058 CET	49699	80	192.168.2.3	47.92.35.35
Nov 13, 2022 19:26:52.385490894 CET	49699	80	192.168.2.3	47.92.35.35
Nov 13, 2022 19:26:52.385512114 CET	80	49699	47.92.35.35	192.168.2.3
Nov 13, 2022 19:26:52.385562897 CET	80	49699	47.92.35.35	192.168.2.3

Copyright Joe Security LLC 2022

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 13, 2022 19:26:52.385580063 CET	49699	80	192.168.2.3	47.92.35.35
Nov 13, 2022 19:26:52.385627031 CET	49699	80	192.168.2.3	47.92.35.35
Nov 13, 2022 19:26:52.385651112 CET	80	49699	47.92.35.35	192.168.2.3
Nov 13, 2022 19:26:52.385713100 CET	80	49699	47.92.35.35	192.168.2.3
Nov 13, 2022 19:26:52.385724068 CET	49699	80	192.168.2.3	47.92.35.35
Nov 13, 2022 19:26:52.385766983 CET	49699	80	192.168.2.3	47.92.35.35
Nov 13, 2022 19:26:52.385795116 CET	80	49699	47.92.35.35	192.168.2.3
Nov 13, 2022 19:26:52.385854006 CET	80	49699	47.92.35.35	192.168.2.3
Nov 13, 2022 19:26:52.385864019 CET	49699	80	192.168.2.3	47.92.35.35
Nov 13, 2022 19:26:52.385907888 CET	49699	80	192.168.2.3	47.92.35.35

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 13, 2022 19:26:49.247679949 CET	55847	53	192.168.2.3	1.1.1.1
Nov 13, 2022 19:26:49.745223999 CET	53	55847	1.1.1.1	192.168.2.3
Nov 13, 2022 19:26:51.035073042 CET	64213	53	192.168.2.3	1.1.1.1
Nov 13, 2022 19:26:51.582151890 CET	53	64213	1.1.1.1	192.168.2.3
Nov 13, 2022 19:26:57.543345928 CET	52281	53	192.168.2.3	1.1.1.1
Nov 13, 2022 19:26:57.751965046 CET	53	52281	1.1.1.1	192.168.2.3
Nov 13, 2022 19:27:02.730665922 CET	63177	53	192.168.2.3	1.1.1.1
Nov 13, 2022 19:27:03.479362965 CET	53	63177	1.1.1.1	192.168.2.3

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class	DNS over HTTPS
Nov 13, 2022 19:26:49.247679949 CET	192.168.2.3	1.1.1.1	0xa733	Standard query (0)	datie-tw.com	A (IP address)	IN (0x0001)	false
Nov 13, 2022 19:26:51.035073042 CET	192.168.2.3	1.1.1.1	0xa2a2	Standard query (0)	sbm.xinmoshiwang.com	A (IP address)	IN (0x0001)	false
Nov 13, 2022 19:26:57.543345928 CET	192.168.2.3	1.1.1.1	0xa26	Standard query (0)	copunupo.ac.zm	A (IP address)	IN (0x0001)	false
Nov 13, 2022 19:27:02.730665922 CET	192.168.2.3	1.1.1.1	0x5c13	Standard query (0)	ly.yjlianyi.top	A (IP address)	IN (0x0001)	false

DNS Answers

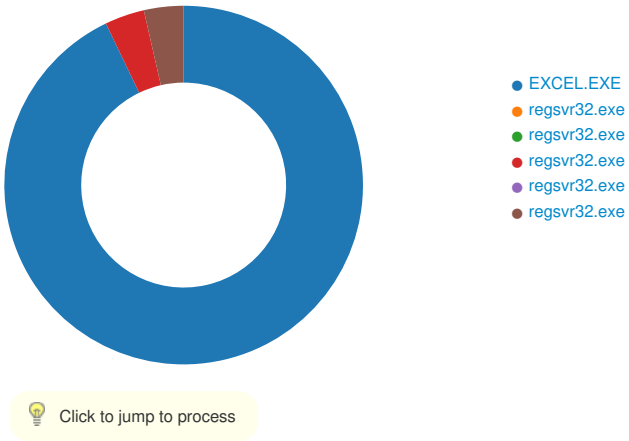
Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class	DNS over HTTPS
Nov 13, 2022 19:26:49.745223999 CET	1.1.1.1	192.168.2.3	0xa733	No error (0)	datie-tw.com		175.98.167.165	A (IP address)	IN (0x0001)	false
Nov 13, 2022 19:26:51.582151890 CET	1.1.1.1	192.168.2.3	0xa2a2	No error (0)	sbm.xinmoshiwang.com		47.92.35.35	A (IP address)	IN (0x0001)	false
Nov 13, 2022 19:26:57.751965046 CET	1.1.1.1	192.168.2.3	0xa26	No error (0)	copunupo.ac.zm		41.63.0.22	A (IP address)	IN (0x0001)	false
Nov 13, 2022 19:27:03.479362965 CET	1.1.1.1	192.168.2.3	0x5c13	No error (0)	ly.yjlianyi.top		81.68.152.197	A (IP address)	IN (0x0001)	false

HTTP Request Dependency Graph

- datie-tw.com
- copunupo.ac.zm
- 182.162.143.56
- sbm.xinmoshiwang.com
- ly.yjlianyi.top

Statistics

Behavior



System Behavior

Analysis Process: EXCEL.EXE PID: **4380**, Parent PID: **3800**

General

Target ID:	0
Start time:	19:26:43
Start date:	13/11/2022
Path:	C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	C:\Program Files\Microsoft Office\Root\Office16\EXCEL.EXE" "C:\Users\user\Desktop\PO0000001552.xls
Imagebase:	0x7ff62cde0000
File size:	64367408 bytes
MD5 hash:	23CAD504B3E04BB54CD636AD2874041A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Registry Activities

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

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: regsvr32.exe PID: **6588**, Parent PID: **4380**

General

Target ID:	7
Start time:	19:26:50
Start date:	13/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe /S ..\elv1.ooocccxxx
Imagebase:	0x7ff7208c0000
File size:	24064 bytes
MD5 hash:	578BAB56836A3FE455FFC7883041825B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: regsvr32.exe PID: **6608**, Parent PID: **4380**

General

Target ID:	8
Start time:	19:26:54
Start date:	13/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe /S ..\elv2.ooocccxxx
Imagebase:	0x7ff7208c0000
File size:	24064 bytes
MD5 hash:	578BAB56836A3FE455FFC7883041825B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.1291594477.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Emotet_db7d33fa, Description: unknown, Source: 00000008.00000002.1291594477.0000000180001000.00000020.00001000.00020000.00000000.sdmp, Author: unknown • Rule: JoeSecurity_Emotet_1, Description: Yara detected Emotet, Source: 00000008.00000002.1290019980.0000000000980000.00000040.00001000.00020000.00000000.sdmp, Author: Joe Security • Rule: Windows_Trojan_Emotet_db7d33fa, Description: unknown, Source: 00000008.00000002.1290019980.0000000000980000.00000040.00001000.00020000.00000000.sdmp, Author: unknown
Reputation:	moderate

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **6676**, Parent PID: **6608**

General

Target ID:	10
Start time:	19:26:57
Start date:	13/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\XEzXl\JZazaZgAOY.dll"
Imagebase:	0x7ff7208c0000
File size:	24064 bytes
MD5 hash:	578BAB56836A3FE455FFC7883041825B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_3, Description: Yara detected Emotet, Source: 0000000A.00000002.2414500170.0000000000BBB000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	JZazaZgAOY.dll	unicode	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\XEzXl\JZazaZgAOY.dll"	success or wait	1	180020877	RegSetValueExW

Analysis Process: regsvr32.exe PID: **6756**, Parent PID: **4380**

General

Target ID:	11
Start time:	19:27:00
Start date:	13/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\System32\regsvr32.exe /S ..\elv3.ooocccxxx
Imagebase:	0x7ff7208c0000
File size:	24064 bytes
MD5 hash:	578BAB56836A3FE455FFC7883041825B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

Old File Path	New File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: regsvr32.exe PID: **6792**, Parent PID: **6756**

General

Target ID:	12

Start time:	19:27:03
Start date:	13/11/2022
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\GanZhs\FrugrCuQjdEr.dll"
Imagebase:	0x7ff7208c0000
File size:	24064 bytes
MD5 hash:	578BAB56836A3FE455FFC7883041825B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_Emotet_3, Description: Yara detected Emotet, Source: 0000000C.00000002.2414304563.00000000009BB000.00000004.00000020.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

Registry Activities

Key Value Created

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	FrugrCuQjdEr.dll	unicode	C:\Windows\system32\regsvr32.exe "C:\Windows\system32\GanZhs\FrugrCuQjdEr.dll"	success or wait	1	180020877	RegSetValueExW

Disassembly

No disassembly