ID: 431937
Sample Name:
Documents_13134976_1377491379.xlsb
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 15:20:54
Date: 09/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

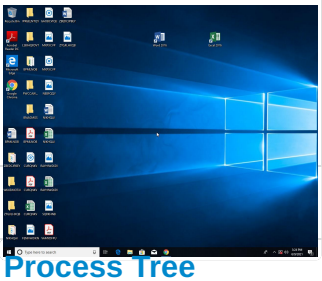
Analysis Report Documents_13134976_1377491379.xlsb

Overview

General Information

Sample Name:	Documents_13134976_1377491379.xlsb
Analysis ID:	431937
MD5:	276bf3db434b887.
SHA1:	eee2be9136f2c70.
SHA256:	27180043ebeb8f2.
Tags:	xlsb xlsx
Infos:	

Most interesting Screenshot:



Detection

MALICIOUS
SUSPICIOUS
CLEAN
UNKNOWN

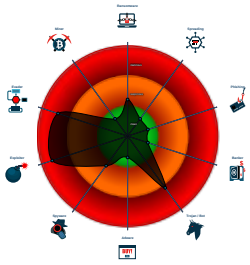
Hidden Macro 4.0

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

Signatures

- Document exploit detected (creates …
- Document exploit detected (drops P…
- Office document tries to convince vi…
- Sigma detected: BlueMashroom DLL…
- Snort IDS alert for network traffic (e.…
- System process connects to networ…
- Creates an autostart registry key po…
- Document exploit detected (UrlDown…
- Document exploit detected (process…
- Drops PE files to the user root direc…
- Found Excel 4.0 Macro with suspicio…
- Office process drops PE file

Classification



Process Tree

- **System is w10x64**
- EXCEL.EXE (PID: 6528 cmdline: 'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding MD5: 5D6638F2C8F8571C593999C58866007E)
  - regsvr32.exe (PID: 6796 cmdline: regsvr32 -s ..\iepfusn.dll MD5: 426E7499F6A7346F0410DEAD0805586B)
    - regsvr32.exe (PID: 6848 cmdline: -s ..\iepfusn.dll MD5: D78B75FC68247E8A63ACBA846182740E)
      - cmd.exe (PID: 6980 cmdline: cmd /c ping 8.8.7.7 -n 2 & start C:\Windows\system32\regsvr32.exe -s C:\Users\user\iepfusn.dll RV0KR MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
        - conhost.exe (PID: 6988 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
        - PING.EXE (PID: 7032 cmdline: ping 8.8.7.7 -n 2 MD5: 6A7389ECE70FB97BFE9A570DB4ACCC3B)
        - regsvr32.exe (PID: 5712 cmdline: C:\Windows\system32\regsvr32.exe -s C:\Users\user\iepfusn.dll RV0KR MD5: D78B75FC68247E8A63ACBA846182740E)
          - cmd.exe (PID: 1724 cmdline: cmd /c ping 8.8.7.7 -n 2 & start C:\Windows\system32\regsvr32.exe -s C:\Users\user\AppData\Local\Temp\L3YD7CE.dll N8DG MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
            - conhost.exe (PID: 1808 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
            - PING.EXE (PID: 6196 cmdline: ping 8.8.7.7 -n 2 MD5: 6A7389ECE70FB97BFE9A570DB4ACCC3B)
            - regsvr32.exe (PID: 6356 cmdline: C:\Windows\system32\regsvr32.exe -s C:\Users\user\AppData\Local\Temp\L3YD7CE.dll N8DG MD5: D78B75FC68247E8A63ACBA846182740E)
              - cmd.exe (PID: 6896 cmdline: cmd /c ping 8.8.7.7 -n 2 & start C:\Windows\system32\regsvr32.exe -s C:\Users\user\AppData\Local\Temp\L3YD7CE.dll VE50DB MD5: 4E2ACF4F8A396486AB4268C94A6A245F)
                - conhost.exe (PID: 5680 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
                - PING.EXE (PID: 6092 cmdline: ping 8.8.7.7 -n 2 MD5: 6A7389ECE70FB97BFE9A570DB4ACCC3B)
                - regsvr32.exe (PID: 6824 cmdline: C:\Windows\system32\regsvr32.exe -s C:\Users\user\AppData\Local\Temp\L3YD7CE.dll VE50DB MD5: D78B75FC68247E8A63ACBA846182740E)
- regsvr32.exe (PID: 6872 cmdline: 'C:\Windows\system32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\L3YD7CE.dll VE50DB MD5: D78B75FC68247E8A63ACBA846182740E)
- regsvr32.exe (PID: 400 cmdline: 'C:\Windows\system32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\L3YD7CE.dll VE50DB MD5: D78B75FC68247E8A63ACBA846182740E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Initial Sample

Source	Rule	Description	Author	Strings
app.xml	JoeSecurity_XlsWithMacro4	Yara detected Xls With Macro 4.0	Joe Security	

Sigma Overview

System Summary:

Sigma detected: BlueMashroom DLL Load

Sigma detected: Microsoft Office Product Spawning Windows Shell

Sigma detected: Regsvr32 Anomaly

Signature Overview

Click to jump to signature section

Software Vulnerabilities:

Document exploit detected (creates forbidden files)

Document exploit detected (drops PE files)

Document exploit detected (UrlDownloadToFile)

Document exploit detected (process start blacklist hit)

Networking:

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

Uses ping.exe to check the status of other devices and networks

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

Office process drops PE file

Boot Survival:

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

Drops PE files to the user root directory

Malware Analysis System Evasion:

Uses ping.exe to sleep

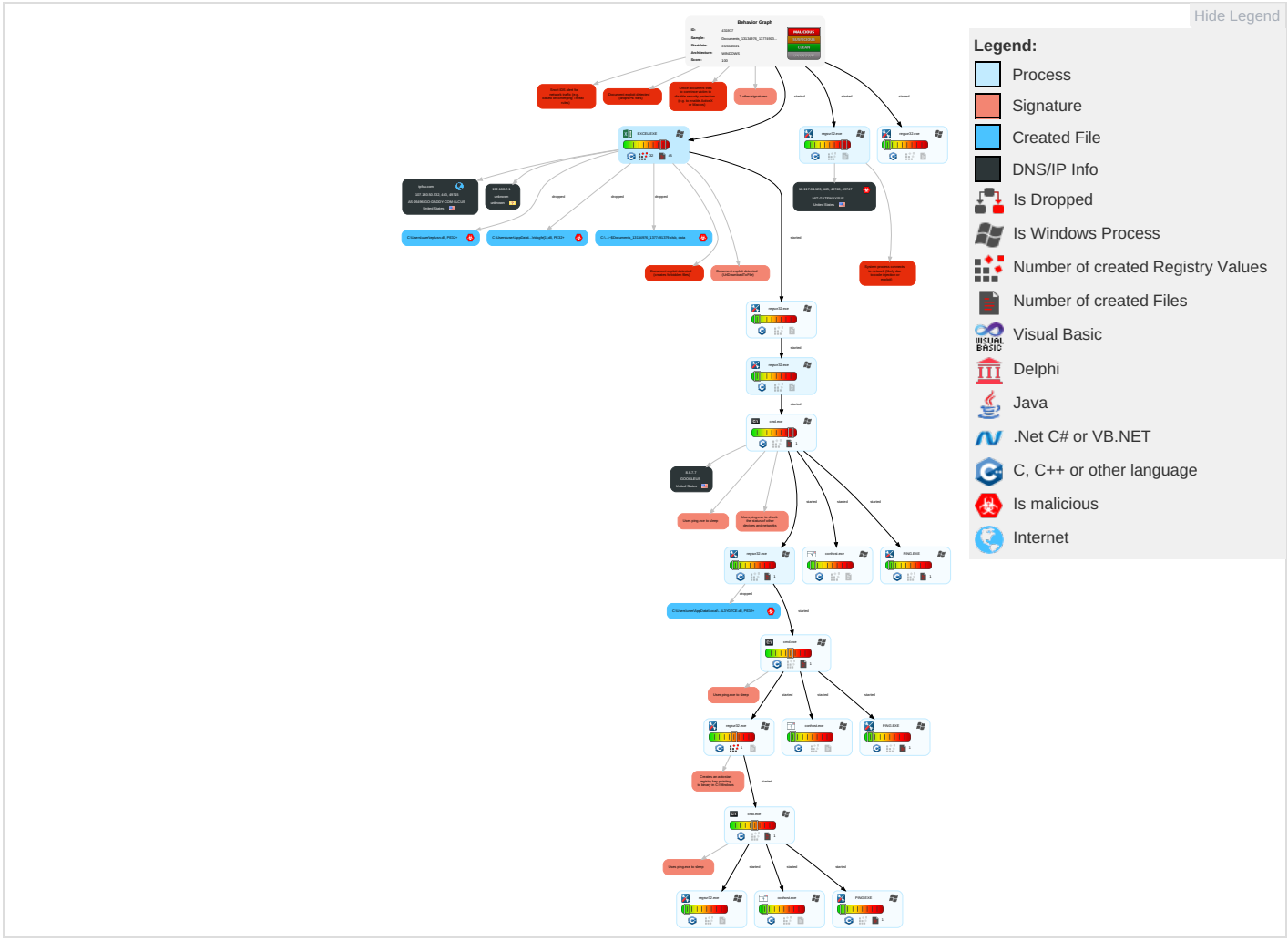
HIPS / PFW / Operating System Protection Evasion:

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

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Netwo Effect
Valid Accounts	Scripting 1	Registry Run Keys / Startup Folder 1 1	Process Injection 1 1 2	Masquerading 1 1 1	OS Credential Dumping	System Time Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1 2	Eaves Insecu Netwo Comm
Default Accounts	Exploitation for Client Execution 4 3	DLL Side-Loading 1	Registry Run Keys / Startup Folder 1 1	Disable or Modify Tools 1	LSASS Memory	Query Registry 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Non-Application Layer Protocol 1	Exploi Redire Calls/S
Domain Accounts	At (Linux)	Logon Script (Windows)	DLL Side-Loading 1	Virtualization/Sandbox Evasion 1 1	Security Account Manager	Security Software Discovery 2 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Application Layer Protocol 2	Exploi Track Locati
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Virtualization/Sandbox Evasion 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM C Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Scripting 1	LSA Secrets	Process Discovery 3	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manip Device Comm
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Regsvr32 1	Cached Domain Credentials	Remote System Discovery 1 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamm Denial Servic
External Remote Services	Scheduled Task	Startup Items	Startup Items	DLL Side-Loading 1	DCSync	System Network Configuration Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port	Rogue Acces
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	File and Directory Discovery 2	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol	Downg Insecu Protoc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Masquerading	/etc/passwd and /etc/shadow	System Information Discovery 2 4	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocols	Rogue Base S

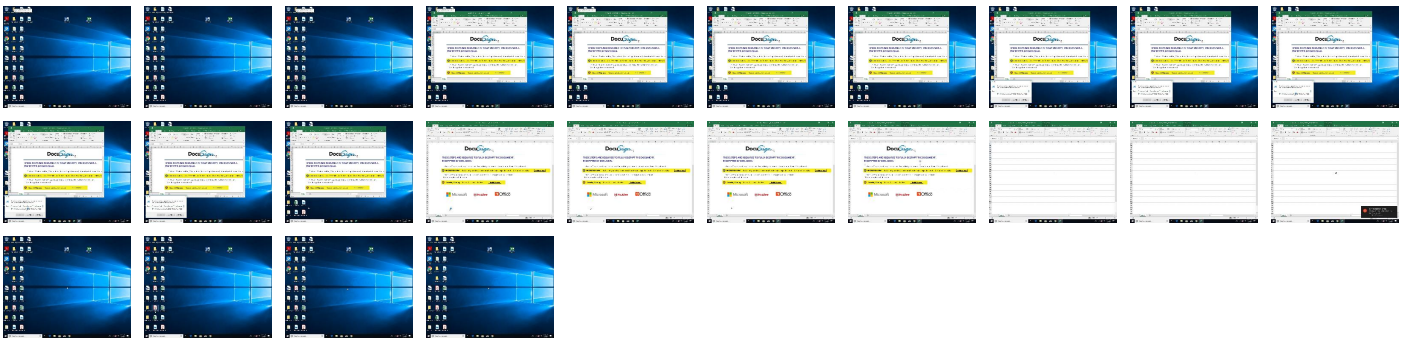
Behavior Graph



Screenshots

Thumbnails

This section contains all screenshots as thumbnails, including those not shown in the slideshow.



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Documents_13134976_1377491379.xlsb	2%	ReversingLabs		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\rtdsgfe[1].dll	6%	Metadefender		Browse
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\rtdsgfe[1].dll	4%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\L3YD7CE.dll	6%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\L3YD7CE.dll	4%	ReversingLabs		
C:\Users\user\iepfusn.dll	6%	Metadefender		Browse
C:\Users\user\iepfusn.dll	4%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://cdn.entity.	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	0%	URL Reputation	safe	
http://https://powerlift.acompli.net	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://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://rpsticket.partnerservices.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://cortana.ai	0%	URL Reputation	safe	
http://https://18.117.84.120/18.188.86.8/	0%	Avira URL Cloud	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://api.aadrm.com/	0%	URL Reputation	safe	
http://https://ofcrecsvcapi-int.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://18.117.84.120/#	0%	Avira URL Cloud	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	0%	URL Reputation	safe	
http://https://res.getmicrosoftkey.com/api/redemptionevents	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://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://powerlift-frontdesk.acompli.net	0%	URL Reputation	safe	
http://https://officeci.azurewebsites.net/api/	0%	Avira URL Cloud	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://store.office.cn/addinstemplate	0%	URL Reputation	safe	
http://https://18.188.86.8/kenichi/special21new/trailer2a5	0%	Avira URL Cloud	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://store.officeppe.com/addinstemplate	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	0%	URL Reputation	safe	
http://https://dev0-api.acompli.net/autodetect	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://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://www.odwebp.svc.ms	0%	URL Reputation	safe	
http://https://18.117.84.120/	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.com	0%	URL Reputation	safe	
http://https://officesetup.getmicrosoftkey.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://prod-global-autodetect.acompli.net/autodetect	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://ncus.contentsync.	0%	URL Reputation	safe	
http://https://ncus.contentsync.	0%	URL Reputation	safe	
http://https://18.117.84.120/kenichi/special21new/trailer2a5T0	0%	Avira URL Cloud	safe	
http://https://18.117.84.120/89b	0%	Avira URL Cloud	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://apis.live.net/v5.0/	0%	URL Reputation	safe	
http://https://18.188.86.8/Z	0%	Avira URL Cloud	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://wus2.contentsync.	0%	URL Reputation	safe	
http://https://18.117.84.120/kenichi/special21new/trailer2a5	0%	Avira URL Cloud	safe	
http://https://asgsmsproxyapi.azurewebsites.net/	0%	Avira URL Cloud	safe	
http://https://18.188.86.8:443/kenichi/special21new/trailer2a55	0%	Avira URL Cloud	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://dataservice.o365filtering.com/PolicySync/PolicySync.svc/SyncFile	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://ncus.pagecontentsync.	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	
http://https://skyapi.live.net/Activity/	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
tpfcu.com	107.180.50.232	true	false		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
8.8.7.7	unknown	United States		15169	GOOGLEUS	false
107.180.50.232	tpfcu.com	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	false
18.117.84.120	unknown	United States		3	MIT-GATEWAYSUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	431937
Start date:	09.06.2021
Start time:	15:20:54
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Documents_13134976_1377491379.xlsb
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	35
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.winXLSB@28/13@1/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 88.3% (good quality ratio 83.8%) • Quality average: 70.5% • Quality standard deviation: 29%
HCA Information:	• Successful, ratio: 70% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsb • Found Word or Excel or PowerPoint or XPS Viewer • Found warning dialog • Click Ok • Found warning dialog • Click Ok • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
15:22:03	API Interceptor	9x Sleep call for process: regsvr32.exe modified
15:22:35	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run FX11S05YSR C:\Windows\system32\regsvr32.exe -s C:\Users\user\AppData\Local\Temp\L3YD7CE.dll VE50DB
15:22:43	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run FX11S05YSR C:\Windows\system32\regsvr32.exe -s C:\Users\user\AppData\Local\Temp\L3YD7CE.dll VE50DB

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
18.117.84.120	sample.ocx	Get hash	malicious	Browse	

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
AS-26496-GO-DADDY-COM-LLCUS	#U00a0Import Custom Duty invoice & its clearance documents.exe	Get hash	malicious	Browse	• 184.168.131.241
	Payment receipt MT103.exe	Get hash	malicious	Browse	• 184.168.131.241
	research-531942606.xlsb	Get hash	malicious	Browse	• 72.167.211.83
	research-121105165.xlsb	Get hash	malicious	Browse	• 72.167.211.83
	research-76934760.xlsb	Get hash	malicious	Browse	• 72.167.211.83
	research-1960540844.xlsx	Get hash	malicious	Browse	• 72.167.211.83
	research-1110827633.xlsb	Get hash	malicious	Browse	• 72.167.211.83
	DocumentScanCopy2021_pdf.exe	Get hash	malicious	Browse	• 148.66.138.158
	New Order.exe	Get hash	malicious	Browse	• 184.168.131.241
	DocumentScanCopy202_pdf.exe	Get hash	malicious	Browse	• 148.66.138.158

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	NEW ORDER ZIP.exe	Get hash	malicious	Browse	• 184.168.131.241
	oVA5JBAJutcna88.exe	Get hash	malicious	Browse	• 184.168.131.241
	qXDtb88hht.exe	Get hash	malicious	Browse	• 184.168.131.241
	a8eC6O6okf.exe	Get hash	malicious	Browse	• 184.168.131.241
	Telex_Payment.exe	Get hash	malicious	Browse	• 184.168.131.241
	QyKNw7NioL.exe	Get hash	malicious	Browse	• 184.168.131.241
	Payment_Advice.exe	Get hash	malicious	Browse	• 184.168.131.241
	SOA #093732.exe	Get hash	malicious	Browse	• 184.168.131.241
	Invoice.exe	Get hash	malicious	Browse	• 50.62.195.83
	rHk5KU7bfT.exe	Get hash	malicious	Browse	• 184.168.131.241
MIT-GATEWAYSUS	sample.ocx	Get hash	malicious	Browse	• 18.117.84.120
	PsNZLytUyV.exe	Get hash	malicious	Browse	• 128.31.0.34
	networkservice.exe	Get hash	malicious	Browse	• 18.20.124.79
	file.msg.exe	Get hash	malicious	Browse	• 128.30.52.76
	Update-KB1484-x86.exe	Get hash	malicious	Browse	• 128.30.52.79
	nT7K5GG5km	Get hash	malicious	Browse	• 19.35.22.33
	KnAY2OIPI3	Get hash	malicious	Browse	• 19.252.51.218
	x86_unpacked	Get hash	malicious	Browse	• 19.60.14.26
	rIbyGX66Op	Get hash	malicious	Browse	• 19.21.98.61
	4JQil8gLKd	Get hash	malicious	Browse	• 19.170.175.72
	IMG001.exe	Get hash	malicious	Browse	• 19.241.222.80
	YPJ9DZYIpO	Get hash	malicious	Browse	• 19.160.35.138
	FB11.exe	Get hash	malicious	Browse	• 128.31.0.34
	messg_02620000_deupx - Copy.exe	Get hash	malicious	Browse	• 128.31.0.39
	HUahIwV82u.exe	Get hash	malicious	Browse	• 128.31.0.34
	R8WWx5t2RE.dll	Get hash	malicious	Browse	• 18.41.89.186
	KCCAfipQl2.dll	Get hash	malicious	Browse	• 19.3.169.121
	fOMSAB0Sfe.exe	Get hash	malicious	Browse	• 128.31.0.34
	530000.exe	Get hash	malicious	Browse	• 128.31.0.34
	networkmanager	Get hash	malicious	Browse	• 19.211.36.11

JA3 Fingerprints

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
8916410db85077a5460817142dcbc8de	sample.ocx	Get hash	malicious	Browse	• 18.117.84.120
	samp.exe	Get hash	malicious	Browse	• 18.117.84.120
	UJFcKUqgmf.exe	Get hash	malicious	Browse	• 18.117.84.120
	1c2102da_by_Libranalysis.dll	Get hash	malicious	Browse	• 18.117.84.120
	34d0a579_by_Libranalysis.dll	Get hash	malicious	Browse	• 18.117.84.120
	3f3cb269_by_Libranalysis.dll	Get hash	malicious	Browse	• 18.117.84.120
	fTXDq_9l7R2B0vcJRNsxuiqMxwPxzPi4LKezkpuCM_E.dll	Get hash	malicious	Browse	• 18.117.84.120
	huqgk.exe	Get hash	malicious	Browse	• 18.117.84.120
	publiclicense.vbs	Get hash	malicious	Browse	• 18.117.84.120
	Ei8IYTWG2j.exe	Get hash	malicious	Browse	• 18.117.84.120
	IU7lKa778w.exe	Get hash	malicious	Browse	• 18.117.84.120
	oi5zrjsKJG.exe	Get hash	malicious	Browse	• 18.117.84.120
	SecuriteInfo.com.RiskTool.Win32.BitCoinMiner.vho.31244.exe	Get hash	malicious	Browse	• 18.117.84.120
	b49zEBfIlL.dll	Get hash	malicious	Browse	• 18.117.84.120
	SecuriteInfo.com.UDS.Trojan.Win32.Injuke.25486.exe	Get hash	malicious	Browse	• 18.117.84.120
	XLhw6JGwC0.dll	Get hash	malicious	Browse	• 18.117.84.120
	SecuriteInfo.com.UDS.Trojan.Win32.Bsymem.19574.dll	Get hash	malicious	Browse	• 18.117.84.120
	SecuriteInfo.com.Program.Win32.Wacapew.Cml.8809.exe	Get hash	malicious	Browse	• 18.117.84.120
	ai8HRya7D6.exe	Get hash	malicious	Browse	• 18.117.84.120
	SecuriteInfo.com.FileRepMalware.16835.exe	Get hash	malicious	Browse	• 18.117.84.120
37f463bf4616ecd445d4a1937da06e19	audit-367497006.xlsb	Get hash	malicious	Browse	• 107.180.50.232
	Bills Pending Approval.html	Get hash	malicious	Browse	• 107.180.50.232
	GDrVYvtzuO.exe	Get hash	malicious	Browse	• 107.180.50.232
	9E7YOr0kp1.exe	Get hash	malicious	Browse	• 107.180.50.232

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	aKdhpWlFPg.exe	Get hash	malicious	Browse	• 107.180.50.232
	vSYEHJjK1G.exe	Get hash	malicious	Browse	• 107.180.50.232
	FaceCheck - Installer.exe	Get hash	malicious	Browse	• 107.180.50.232
	analysis-31947858.xlsb	Get hash	malicious	Browse	• 107.180.50.232
	Julie.randall Completed REFERRAL AGREEMENT 60926.html	Get hash	malicious	Browse	• 107.180.50.232
	DPSGNwkO1Z.exe	Get hash	malicious	Browse	• 107.180.50.232
	x1Q123VhUa.exe	Get hash	malicious	Browse	• 107.180.50.232
	Snc3sPQ2yl.exe	Get hash	malicious	Browse	• 107.180.50.232
	nU8kVKVAc8.exe	Get hash	malicious	Browse	• 107.180.50.232
	tmp_Client-Status-062021-952177.vbs	Get hash	malicious	Browse	• 107.180.50.232
	analysis-1593377733.xlsb	Get hash	malicious	Browse	• 107.180.50.232
	research-531942606.xlsb	Get hash	malicious	Browse	• 107.180.50.232
	New order_doc.exe	Get hash	malicious	Browse	• 107.180.50.232
	06.08.21 Inv & AP Statement - Copy.htm	Get hash	malicious	Browse	• 107.180.50.232
	#Ud83d#Udda8rocket.com 1208421(69-queue-2615.htm	Get hash	malicious	Browse	• 107.180.50.232
	research-121105165.xlsb	Get hash	malicious	Browse	• 107.180.50.232

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Local\Temp\L3YD7CE.dll	sample.ocx	Get hash	malicious	Browse	
C:\Users\user\iepfusn.dll	sample.ocx	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\rtdsgfe[1].dll	sample.ocx	Get hash	malicious	Browse	

Created / dropped Files

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

Process:	C:\Windows\System32\regsvr32.exe
File Type:	Microsoft Cabinet archive data, 60080 bytes, 1 file
Category:	dropped
Size (bytes):	60080
Entropy (8bit):	**7.995256720209506**
Encrypted:	**true**
SSDEEP:	768:O78wIEbt8Rc7GHyP7zpxeiB9jTs6cX8ENclXVbFYYDceSKZyhRhbzfgtEnz9BPNZ:A8Rc7GHyhUHsVNPOlhbz2E5BPNiUu+g4
MD5:	6045BACCF49E1EBA0E674945311A06E6
SHA1:	379C6234849EECEDE26FAD192C2EE59E0F0221CB
SHA-256:	65830A65CB913BEE83258E4AC3E140FAF131E7EB084D39F7020C7ACC825B0A58
SHA-512:	DA32AF6A730884E73956E4EB6BFF61A1326B3EF8BA0A213B5B4AAD6DE4FBD471B3550B6AC2110F1D0B2091E33C70D44E498F897376F8E1998B1D2AFAC789ABEB
Malicious:	false
Preview:	MSCF.....,.....I.....d.....R9b .authroot.stl.3..).4..CK..8T....c_.d....A.K...].M$[v.4.)7-.%.QIR..$t)Kd.-[..T\{..ne.....{..<.....Ab.<..X....sb.....e.....dbu.3...0..... ..X..00&Z....C...p0.}..2..0m.}..Cj.9U..J.j.Y...#.L..\X..O.,...,.qu..]..(B.nE~Q...)..Gcx.....}...f....zw.a..9+[.<0.'..2 .s..ya..J.....wd....OO!.s....`.WA...F6._f....6...g..2..7.$,....X.k..&. ..E...g.....>uv."..!.....xc.....C..?....P0$.Y..?u....Z0.g3.>W0&.y.(....].`>... ..R.q..wg*X.....qB!.B....Z.4..>.R.M..0.8...=.8..Ya.s.....add..)..w.4.&.z...2.&74.5]..w.j.._iK..|[.w.M.!<- .}%.C<tDX5\s._..l..*..nb.....GCQ.V..r..Y.....q...0..V)Tu>.Z..r...l...<.R{Ac..x^. .<A.....|.{.....Q...&....X..C$....e9.:..vl..x.R4...L.....%g...<..}'{....E8Sl...E".h...*.....ItVs.K..... .3.9.l..`D..e.i`....y....,..5....aSs`..W...d...t.J..]....'u3..d]7..=e....[R!:.....Q.%..@.....ga.v.~..q....{.!N.b]x..Zx.../;#}.f.)k.c9..{rmPt..z5.m=..q..%.D#<+Ex....1|.._F.

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

Process:	C:\Windows\System32\regsvr32.exe
File Type:	data
Category:	modified
Size (bytes):	328
Entropy (8bit):	3.132472625894721
Encrypted:	false
SSDEEP:	6:kKgy3Pse8N+SkQlPlEGYRMY9z+4KlDA3RUeWlK1MMx:4Ks8kPlE99SNxAhUe3OMx
MD5:	B84815C12C603EC6FB8D1EDA4CA29530
SHA1:	CD18E3BC8FCFB385C1225EF5ED0FCF1BD9DF0434
SHA-256:	961CA06C24F3E4B504765841EFB908C623E99B0EC81EBB6804928909F4360E52
SHA-512:	7771C7B0CC1743F21C13270B0B8390410E1BBD9BB849F9DF045F5A9976B99A169328F257CD09403420C24B62275F332CE54909F8603970F07C71C90501984D2F
Malicious:	false

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Preview:	p..... .....<..~]..(..... .....L.....&.....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...".0.9.0.e.6.c.f.e.3.4.c.d.7.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\Office\16.0\WebServiceCache\AllUsers\officeclient.microsoft.com\2CA63FBD-E4D0-4324-9237-CB578953FC60	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	XML 1.0 document, UTF-8 Unicode text, with very long lines, with CRLF line terminators
Category:	dropped
Size (bytes):	134915
Entropy (8bit):	5.369271958078095
Encrypted:	false
SSDEEP:	1536:lcQIKNEeBXA3gBwlpQ9DQW+z7534ZlCKWXboOilX5ENLWME9:REQ9DQW+zAXOe
MD5:	76B550BC14095A4AFBB5E04BE5F42175
SHA1:	2A74379C0333997DFED5BB5F7BDB7F707BAF68E4
SHA-256:	7F1E14B77DF7F3FCEB0C34441CA6F6A68288706308BF5B072FAE111AF6BE0817
SHA-512:	41056D2FD4A84E050F7EDC8F962B02C093AD02F3B2B8E410F424A6E155672AF6BA67D21579EC5B0BF6A56F9E8B71B2B0035C5E6B822B78072D1EB2DCBCA3E94F
Malicious:	false
Preview:	<?xml version="1.0" encoding="utf-8"?>..<o:OfficeConfig xmlns:o="urn:schemas-microsoft-com:office:office">.. <o:services o:GenerationTime="2021-06-09T13:21:51">.. Build: 16.0.14207.30526-->.. <o:default>.. <o:ticket o:headerName="Authorization" o:headerValue="{}" />.. </o:default>.. <o:service o:name="Research">.. <o:url>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:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientHome">.. <o:url>https://[MAX.BaseHost]/client/results</o:url>.. </o:service>.. <o:service o:name="ClViewClientTemplate">.. <o:url>https://ocsa.office.microsoft.com/client/15/help/template</o:url>.. </o:service>.. <o:

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\2FDD9604.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 264 x 113, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	9924
Entropy (8bit):	7.973758306371751
Encrypted:	false
SSDEEP:	192:soXrzGktAQUkDfw4om9PEK9u27pwnJyV028/tgXEoCWoB:so9G+fnVEYu27OIW/+XEoCWoB
MD5:	B34FB4F2F0F9E70B72BA3AFD028CD97C
SHA1:	C6868336F78DEA1E718965DF3341039581DB5B5A
SHA-256:	189D420D344A694FD1928ABACBEC94D9F0EF52BE036CEB8144A9D9A6DD14EAEB
SHA-512:	4795600917F8A67A6C5CBD5713CAACE74E0483F8E6BB6D98EAB63BF24A0F71E537E7F8ABD26808630B247D454A3F467595C8343EEB4EA98AFAB49D81964158D
Malicious:	false
Preview:	.PNG.....IHDR.....q.....sRGB.....pHYs.....+....&ilDATx^.Wp.G~.{"r.. H.9s.,Q.v.....\..../wu..t.o..ru...+W]....vWa).Q.b&.@d.D.q....{0....GB....8.....X,&L1.0.....b...0Xa ....a..0.0.ap.@.....'.*. `.#.6.,....aX..i.b.0..b.n.k...0...J1...H..7...C...dZ....a....Z..!.kp2.R...0Rl..r.A...58.V)..C.)..f.. `....L....!...p.\k.0.a.N.U.A..F.m.Y.5....'.*. `.#.6.,....aX..i.b.0..b.n.k...0...J1...H..7...C...dZ....a....Z..!.kp2.R...0Rl..r.A...58.V)..C.)..f.. `....L....!...p.\k.0.a.N.U.A..F.m.Y.5....'.*. ..W[....cfTDC.....V.....W`...Q!.JEaE....5O.{\N.p8b.5.#*.t.....^...p..A.+.0cC..(.v.,.....qO....-b.0.#l.....p...w...sN]m..-c.=....L....I..T...I.3....]...r.....Ae.H%..!.....O...?-.I..".4.....p...{..0..#,.....%4.;E....w..]......ga...X....#...h@.'E.'.|...I.a..J..V...!...E..?8[CQ?.'...5Qy.....X..)Y..ic 0....!..Gf..4...o.R../.^..y2.'..p.....KO..v.T....~.....-]"..u9Q..i..^e..!.i".^.....C.CKV..~Ku.4"m.$>cKP...x...7

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\3DB5784F.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 168 x 72, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	6177
Entropy (8bit):	7.959095006853368
Encrypted:	false
SSDEEP:	96:j6KDvZ3QXkQ288GMDBm6hEeWyS8ITRIVg9gPEnbYhbY0Y4pxCpAueydMT1uZMr0a:j6KTV8WBPhqd9qqYTB6peyeT1oMr0a
MD5:	C7ED6FC355D8632DB1464BE3D56BF5CC
SHA1:	615484A338922DDF00B903CFA48060AD60D70207
SHA-256:	26000244FBB0C6B2D76F80166CE85700BC96141C6CD80F8B399CA6F15FE3515C
SHA-512:	FB4AE09EACD15A4FE778BDF366808C4F9FE403C4054F86704C03C87C7016E7D7A5772677B69064FCB5F1B9345D80C4263A58EA8B5E9CA2B717E24E2B19B85A9
Malicious:	false
Preview:	.PNG.....IHDR.....H.....m)a....sRGB.....pHYs.....+.....IDATx^....E...1.Y. ..."3.(.D.....A..(....(.C.X.QP..b.UQAdA..9'I:Hf..f.....s...._.A..s.3...Vu.....Z.[.q.P.-9.b..q.....|.r F.....c..1.....e.->....@..;n.q..(.bt.q...>F9...[|\.1..]v..A..G..y._3...*3M.YG7.J.)..RK]u.j}.*^J.....R...j.:=}..qN .sV&..F.a.@..Vs.P...%.A.....~..w..P.Be.-].4..arss.9~.8d.@.d...."..?.G...z.....(.T.....G.;w.?....w....S.H.+...W.^.....E..-_.|....D-....#G.{..<r....P.K..$.{D....kzzz.R....`?..O;.....#....tb..g..gU.r>G.....:t.....a.....p..c..]..... M.6.'O.]..... 8q...RSS.YBB.M.j..}..I.&.:%J.x..7o....d.*U..233.]..... E.m}..../^..nt..X.b,..{<....=.....3....z....v..]0.e.}...?.....w..y...)S.L.F.:t..U...+F...I.....&...322.6m.../.[.J.a.=..%Kx....E...ys.....z...i.z..g...G...e.7.|.h....!C^x.5k".....<.R..k....4iR.V-.._.~....:..P.O@.y.:...:G=.\...J ...u...]%.T.n.....v..A`Y.....V...^{.X^.I`1w.q.....

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\5E6A3635.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 178 x 76, 8-bit/color RGB, non-interlaced
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\5E6A3635.png	
Size (bytes):	5744
Entropy (8bit):	7.966496386988271
Encrypted:	false
SSDEEP:	96:4uJgumnoYk22FLjJq17cpKsv+CHI5BXjI1e+HCLDl3kjH1erj+uYU2:4CgJfkfJA7ixCxqe+GDhkT1erj+uYf
MD5:	9AD30E24270C495AE68EAF3A1EEECBFB
SHA1:	8642D256E7FFBEF5804A2D2220A1FE475A99DC36
SHA-256:	6D3EAD431ABD110369EFABC6F2E474DC24FA3D7EEC28DE43456407C5BACD6D20
SHA-512:	EB156DD0686BAAE4F46B0B0C01838DA7225529D3B31912568D36A1CC07BE006EEAD31F464B0252C3A8471ACA71E86EEE9185FE705ABAE08C56B15C63CC891AD5
Malicious:	false
Preview:	.PNG.....IHDR.....L.....FpzV....sRGB.....pHYs.....+.....IDATx^.\.tTU..u...@@. .b..su....."....+k..Aeu..rX.*.feE..(M.....b..BB.P.f&S_.~w&.I.aH...'...0.....u.2.!...`....8_ ..,.T.#.....,X...N....NN-I.....5`...Z.,..-L..k.":9..Y.,Z..c.Etrja..X.0.G.....f..ha...]....2`.....,..S..e...)<:v.XD'..6.E.Sxt....NN-I.....5`...Z.,..-L..k.":9..Yt.....9.{.f;...f../Mh...B..GK.....FG.. ...s...MN.vqp"+.|.m[&11..<O....?...EQ4.H...Z'M... #.T.....vS..^..p..).....1...JJr?.gq.V..X..h..T._Zr2g..W^...A./.W...P....q.By.49..5M--.e...5}..{.!.s4M./Xx2.....`...I>s..4U...]... (5.8o>.X.[..xS.w)../.c.Lh..a..uQ.fd.....jh.Z.d..(..=.....#.....o.y....g...-....=?..X.f./..=n|`.j..k.....{.4...b..T.-h..F..;u.x....[!.\....*'Nx^....C..b...8.....|F.$.4.....&?.>#.d.\p.R..k..>t0?.-3g.. b.....s.O..E...4o...\O=.7O=z...u1$n..6..C.]A.X...Z.tX.....I..W.....P...h.@..+q..F.kcI..x\>.....0.4..p....}.~e...).w....%Q.$W.....8.....PY.k..J....T..b.I

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\682ADEB2.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 30 x 30, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	956
Entropy (8bit):	7.683552542542939
Encrypted:	false
SSDEEP:	24:64ZJH5wka2YQydYiFNcincNrtNmt5xx4tRFB:JJH5fYuW5c3wPoFB
MD5:	32C83607A5C98C5A634278E5AED3AD61
SHA1:	EDE34ADEA53C413C4AC8215EA48F2F2FD59F1362
SHA-256:	4A999E919D85EDD0CD1A772CA3B29F91AEECF77D0BEB11FD1B632B7A8A0686BF
SHA-512:	AF19A013377F0F7B47E54D99D0AFA222BE46072C47944E8640B09A4993DFDDC906B7C68F7E3DAB5B3F126C9AD1090EADBF17FF7068EE8E360D0EA46811C0DBC
Malicious:	false
Preview:	.PNG.....IHDR.....;0.....sRGB.....gAMA.....a.....pHYs.....o.d...QIDATHK.VMHTQ..2.h.X."h....A....]B...m.(h..b?.$...f.)..ta...jS..!..h.ETD.!."."C..y.....=.>8...{.s..32.0Fv.F...kz..&.|_.....9.)m."......m..$9.j...E.@.:D.-..0...L.hk..(....s.'.k.A-.-.....(.....jR[m..d..O.-?:.c..70.{..sw'X.j.^j+..d....N.. .r.....Z.[[[..c...r.../.M`l.]&#.aR..[{...<O....<d...3....F...:..s9..-...x..R...q..ON.KO;..0..^.....9.S.}..x...22.....r..f....'.....+o...A..7.....q..l...S.....s/.{.^..Pj1`.b.!t..>o..!.C.e.}....Y.....t.....r.MDq=.=..._....c..3%p...j...hI1.[.^.#..."#...e...6..I-j;.9j;o/ ...Q2...w-.?.<..r../?...0.`.;.lz.M...\. ..]x...\h^.....r..';... ...<..j..E._.E..u..g....7.X....T....7.....(&.[..... T....;V1w...EU.W"./.....m%.u'x/.u]*....@.-.L..G.....Q."..%fb.Z*.,...K.%BX.. ..]`J=.h".Vef...2..8.g.jX.2s..vY.u|.4p.\.h...W....{.r.....^Y....2$8F...>`p._.c..}.txq#.$.`:@...Y..?.j.IK.Fu....IEND.B`.

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\Content.MSO\86406406.png	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PNG image data, 288 x 77, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	23989
Entropy (8bit):	7.989754044300238
Encrypted:	false
SSDEEP:	384:SGjFc9Ll+HCggc/h3GXoQjZVVawDIPsTDGY9R9cNc+3JY0kEtWhfEWa92ppgMoF3:S5plMCgzGoOzVawisTDGY9Rs3JYhEtqy
MD5:	839795652A8FE78F26F4D86D757ABDE8
SHA1:	979E5B90C72EA3E5E9D9B506AFDC981BFCA61B60
SHA-256:	1A9EF0E2F66682B532D15457635920067C4F29EF762D2E8A3E0363B4CF39C13E
SHA-512:	E6D5CB06679832DE768E23EF42B9780E4E8327A057A3EA0A6CD5B76908B210078EF659CA44C8723960AB59A0DB85A052C45E7A29D7FA8A643275BA5F210F6773
Malicious:	false
Preview:	.PNG.....IHDR... ...M.....sRGB.....pHYs.....+....]ZIDATx^.....{fs..|.S.....d....`...9.....8..6/.....E.BB.....yw..w.-.FF.g.5~5..ivv.'..U.Tu..8.../=..R9s.Rn....Ry.....@..V.m).bCU..n....Ue.,~b;K.Q.KUlUR.`../...:.Y.Jy..Jy8.Q.K..Xzg..a.Y....X[...s.....`...Q1b....*.....|e.a..$..(...e....e.e..i$SQ.i.y....o.@.....p..yx.b.~....Z"..Xc{,..{..o....`...9K..;.....=...%.@]?.h!.....W...Z....T.Uul..V..PS[.j.....,..W...T.Z..e..T*.J)..+.K*Wt.....W.].K..4.....{.<)...V+e....u.I..A...`o..w.....jUU...b...'....EW....R\..'..b.....U.X..SKV..O&..?.).....}._....\....*..hU\..W.m.I..|.0\...o..?c.a3'.2}...u....`.9..*....q.dc....!..vq..B...9....&..rsJ.\...).}.W./._.g.5e....sy.....@l.l.J.UgW...q..o9^O.g;V.r*v...U.0..._.?.5|...x...m..Z....6...._..l.....dc.....K..`U.c+;.K.^..`.L....j:W(...fuB=.p..w=..D....q..&..8.V.....UU.b#z...Xyo..X...*...w..U.....sW2...d.u.~.~..)l....e.q.:#r.f.....m|...w_...1.i..bs.F..L.`.}..6V..w.....z

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\rtdsgfe[1].dll	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	downloaded
Size (bytes):	205312
Entropy (8bit):	6.709188825960524
Encrypted:	false
SSDEEP:	3072:o7tbwam7niPOMFJjOknVCSd/3391UnrWoTmutZ/dyQCK+VBVmICKUizHz2/bf:StbwamK1jlnnV91UrWStFdjaVF2/b
MD5:	28193BA741232F91101849F606FA8419
SHA1:	12FD2B9850C58A9384EDCBDEC2F94EFD32B0C0B5
SHA-256:	67E54B44DAD909734A59DF457950C05727B7ECF387F1F37C38C18CEF5AF579C2

C:\Users\user\AppData\Local\Microsoft\Windows\INetCache\IE\OTUW0Q90\rtdsgfe[1].dll	
SHA-512:	783213432A0CC54B92F5A49B0F314D949D48810A5D1FC36C92D26A302812E9B66618A0666FAE4BD33911DBC0542390844DA1436D4B9BC73A73D12B4C67929D1F
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 6%, Browse • Antivirus: ReversingLabs, Detection: 4%
Joe Sandbox View:	• Filename: sample.ocx, Detection: malicious, Browse
IE Cache URL:	http://https://tpfcu.com/getfile.php
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....B[..:..:..:..$Z..:..$Z..:..$Z..~:..=d..:..=d..:..=d..:..$Z..:..:..k:...:..:...d..:...dY..:...d..:...Rich.:.....PE..d....P.`......" .....p.....`.....T...d...x.....N.....l.....`.....8.....0.....text...0..... ..`.rdata..."......$.....@..@.data.....@....pdata..l.....@..@.gfids.....@..@.rsrc....N.....N.....@..@.reloc.....`.....@..B.....

C:\Users\user\AppData\Local\Temp\18720000	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	80566
Entropy (8bit):	7.893302821449264
Encrypted:	false
SSDEEP:	1536:Xelem3l7eO+dRRVnyY7lMVGoIahaDHTU6hryF70cAeWvijWGHc:bol7eO6RSY72sTU2yF70cAijW2c
MD5:	5138B6C608292E4C867FC32717C1CF59
SHA1:	836E1C79573D2D8F2E5FCED81BDCA22EEE921EF1
SHA-256:	F04037BBF157BEAF7297874FD3700B1059E20B1E6FBF199C61F2B1E112E660C7
SHA-512:	43AF1CC70CD407BBB7BD1B78B98F1054A85A44C96DDAEA6B1AA3AA2D5D0A943659D445D8566010CE5FB177C2597A57FEEA27D5440B8A8D285E2BD5891A31C7C
Malicious:	false
Preview:	.UKO.0..#...|]%n9..)..rd.`..kO..~.c.....P.*-.\.r..|.O&.+k.....k.....J..e....Va.N....l....?.&w..X..a....o.Q.`.6>.....V$....B.E..|4..w.\.S.`.._X.{....o.....,.2m3>?.;.s..!D.FK..4...;[._,....%3...Ba...iB..1.BJ..~....q.C..!.1.u.....y.m....p...Q+.nDL..RZ|e.....f?I..b.+..).7V..gN.....D^N.OH..H.w#WR...(..#.?.i3..3..+r...}.\.....O.....~s/7...{.A.&...x.}....1[.....D.ti$.D...d.....1.]."..4l..-.U..rr.!Oq.j.6/.....PK.....!.....v.....[Content_Types].xml ...(.....

C:\Users\user\AppData\Local\Temp\L3YD7CE.dll	
Process:	C:\Windows\System32\regsvr32.exe
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	205312
Entropy (8bit):	6.709188825960524
Encrypted:	false
SSDEEP:	3072:o7tbwam7niPOMFJjOknVCSd/3391UnrWoTmutZ/dyQCK+VBVmICKUizHz2/bf:StbwamK1jlnnV91UrWStFdjaVF2/b
MD5:	28193BA741232F91101849F606FA8419
SHA1:	12FD2B9850C58A9384EDCBDEC2F94EFD32B0C0B5
SHA-256:	67E54B44DAD909734A59DF457950C05727B7ECF387F1F37C38C18CEF5AF579C2
SHA-512:	783213432A0CC54B92F5A49B0F314D949D48810A5D1FC36C92D26A302812E9B66618A0666FAE4BD33911DBC0542390844DA1436D4B9BC73A73D12B4C67929D1F
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 6%, Browse • Antivirus: ReversingLabs, Detection: 4%
Joe Sandbox View:	• Filename: sample.ocx, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....B[..:..:..:..$Z..:..$Z..:..$Z..~:..=d..:..=d..:..=d..:..$Z..:..:..k:...:..:...d..:...dY..:...d..:...Rich.:.....PE..d....P.`......" .....p.....`.....T...d...x.....N.....l.....`.....8.....0.....text...0..... ..`.rdata..."......$.....@..@.data.....@....pdata..l.....@..@.gfids.....@..@.rsrc....N.....N.....@..@.reloc.....`.....@..B.....

C:\Users\user\Desktop\~$Documents_13134976_1377491379.xlsb	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	165
Entropy (8bit):	1.6081032063576088
Encrypted:	false
SSDEEP:	3:RFXI6dtt:RJ1
MD5:	7AB76C81182111AC93ACF915CA8331D5
SHA1:	68B94B5D4C83A6FB415C8026AF61F3F8745E2559
SHA-256:	6A499C020C6F82C54CD991CA52F84558C518CBD310B10623D847D878983A40EF

C:\Users\user\Desktop\~$Documents_13134976_1377491379.xlsb	
SHA-512:	A09AB74DE8A70886C22FB628BDB6A2D773D31402D4E721F9EE2F8CCEE23A569342FEECF1B85C1A25183DD370D1DFFFF75317F628F9B3AA363BBB60694F5362(7
Malicious:	**true**
Preview:	.pratesh ..p.r.a.t.e.s.h. . . . .

C:\Users\user\iepfusn.dll	
Process:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
File Type:	PE32+ executable (DLL) (GUI) x86-64, for MS Windows
Category:	dropped
Size (bytes):	205312
Entropy (8bit):	6.709188825960524
Encrypted:	false
SSDEEP:	3072:o7tbwam7niPOMFJjOknVCSd/3391UnrWoTmutZ/dyQCK+VBVmICKUizHz2/bf:StbwamK1jlnnV91UrWStFdjaVF2/b
MD5:	28193BA741232F91101849F606FA8419
SHA1:	12FD2B9850C58A9384EDCBDEC2F94EFD32B0C0B5
SHA-256:	67E54B44DAD909734A59DF457950C05727B7ECF387F1F37C38C18CEF5AF579C2
SHA-512:	783213432A0CC54B92F5A49B0F314D949D48810A5D1FC36C92D26A302812E9B66618A0666FAE4BD33911DBC0542390844DA1436D4B9BC73A73D12B4C67929D1F
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 6%, Browse • Antivirus: ReversingLabs, Detection: 4%
Joe Sandbox View:	• Filename: sample.ocx, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....B[.:..:..:..$Z..:..$Z..:..$Z..~:..=d...:..=d...:..=d...:..$Z...:..:..k:...: ..:...d...:...dY..:...d...:...Rich.:.....PE..d....P.`.....` ..... p.....`.....T...d...x.....N.....l.....`.....8..... .....0.....text...0..... ..`.rdata..."......$.....@..@.data.....@....pdata..l.....@..@.gfids..... .....@..@.rsrc....N.....N.....@..@.reloc.....`.....@..B.....

Static File Info

General

File type:	Microsoft Excel 2007+
Entropy (8bit):	7.867132102918904
TrID:	• Excel Microsoft Office Binary workbook document (47504/1) 49.74% • Excel Microsoft Office Open XML Format document (40004/1) 41.89% • ZIP compressed archive (8000/1) 8.38%
File name:	Documents_13134976_1377491379.xlsb
File size:	64636
MD5:	276bf3db434b887bb77adca0bd46e130
SHA1:	eee2be9136f2c70a28b6ca5289e73e2a38453da2
SHA256:	27180043ebeb8f2aa8728c5ee020fb5368be3df4e9008b8 f01242bf82d5780ce
SHA512:	abe0052635a1064304828a7b8fa8663997fb023d542944 db3bdb346170bd5fbe9a76b2e53184e4b3c7a9e09a7689 82a396b7253d83c309fd7f522f427262e7a
SSDEEP:	1536:LvnO2wWjlMVGoIahaDHTU6hryF70liWWGH0Ae Wl+R:LGCj2sTU2yF70liWW200+R
File Content Preview:	PK.....!.+.....[Content_Types].xml ...(..... ....!!..... .....

File Icon

Icon Hash:	74f0d0d2c6d6d0f4

Static OLE Info

General

Document Type:	OpenXML

General

Number of OLE Files:	1

OLE File "Documents_13134976_1377491379.xlsb"

Indicators

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

Macro 4.0 Code

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
06/09/21-15:22:05.833841	ICMP	382	ICMP PING Windows			192.168.2.6	8.8.7.7
06/09/21-15:22:05.833841	ICMP	384	ICMP PING			192.168.2.6	8.8.7.7
06/09/21-15:22:10.528872	ICMP	382	ICMP PING Windows			192.168.2.6	8.8.7.7
06/09/21-15:22:10.528872	ICMP	384	ICMP PING			192.168.2.6	8.8.7.7
06/09/21-15:22:20.469415	ICMP	382	ICMP PING Windows			192.168.2.6	8.8.7.7
06/09/21-15:22:20.469415	ICMP	384	ICMP PING			192.168.2.6	8.8.7.7
06/09/21-15:22:25.029456	ICMP	382	ICMP PING Windows			192.168.2.6	8.8.7.7
06/09/21-15:22:25.029456	ICMP	384	ICMP PING			192.168.2.6	8.8.7.7
06/09/21-15:22:36.677659	ICMP	382	ICMP PING Windows			192.168.2.6	8.8.7.7
06/09/21-15:22:36.677659	ICMP	384	ICMP PING			192.168.2.6	8.8.7.7
06/09/21-15:22:41.530548	ICMP	382	ICMP PING Windows			192.168.2.6	8.8.7.7
06/09/21-15:22:41.530548	ICMP	384	ICMP PING			192.168.2.6	8.8.7.7
06/09/21-15:22:49.386614	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49740	18.117.84.120	192.168.2.6
06/09/21-15:23:25.363224	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49747	18.117.84.120	192.168.2.6
06/09/21-15:23:57.298792	TCP	2023476	ET TROJAN ABUSE.CH SSL Blacklist Malicious SSL certificate detected (Dridex)	443	49750	18.117.84.120	192.168.2.6

Network Port Distribution

TCP Packets

UDP Packets

ICMP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 9, 2021 15:21:55.219571114 CEST	192.168.2.6	8.8.8.8	0x9318	Standard query (0)	tpfcu.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 9, 2021 15:21:55.279922962 CEST	8.8.8.8	192.168.2.6	0x9318	No error (0)	tpfcu.com		107.180.50.232	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
Jun 9, 2021 15:21:55.561739922 CEST	107.180.50.232	443	192.168.2.6	49715	CN=tpfcu.com, OU=Domain Control Validated CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Fri Mar 05 15:44:31 CET 2021 Tue May 03 09:00:00 CEST 2011	Wed Apr 06 16:44:31 CEST 2022 Sat May 03 09:00:00 CEST 2031	771,49196-49195-49200-49199-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,0-10-11-13-35-23-65281,29-23-24,0	37f463bf4616ecd445d4a1937da06e19
					CN=Go Daddy Secure Certificate Authority - G2, OU=http://certs.godaddy.com/repository/, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	CN=Go Daddy Root Certificate Authority - G2, O="GoDaddy.com, Inc.", L=Scottsdale, ST=Arizona, C=US	Tue May 03 09:00:00 CEST 2011	Sat May 03 09:00:00 CEST 2031		
Jun 9, 2021 15:22:49.386614084 CEST	18.117.84.120	443	192.168.2.6	49740	CN=amadeamadey.at, OU=Amadey Org, O=Amadey TM, L=Bohn, ST=Bohn, C=AT	CN=amadeamadey.at, OU=Amadey Org, O=Amadey TM, L=Bohn, ST=Bohn, C=AT	Wed Jun 09 10:22:21 CEST 2021	Thu Jun 09 10:22:21 CEST 2022	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,5-10-11-13-35-23-65281,29-23-24,0	8916410db85077a5460817142dcbc8de
Jun 9, 2021 15:23:25.363224030 CEST	18.117.84.120	443	192.168.2.6	49747	CN=amadeamadey.at, OU=Amadey Org, O=Amadey TM, L=Bohn, ST=Bohn, C=AT	CN=amadeamadey.at, OU=Amadey Org, O=Amadey TM, L=Bohn, ST=Bohn, C=AT	Wed Jun 09 10:22:21 CEST 2021	Thu Jun 09 10:22:21 CEST 2022	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,5-10-11-13-35-23-65281,29-23-24,0	8916410db85077a5460817142dcbc8de
Jun 9, 2021 15:23:57.298791885 CEST	18.117.84.120	443	192.168.2.6	49750	CN=amadeamadey.at, OU=Amadey Org, O=Amadey TM, L=Bohn, ST=Bohn, C=AT	CN=amadeamadey.at, OU=Amadey Org, O=Amadey TM, L=Bohn, ST=Bohn, C=AT	Wed Jun 09 10:22:21 CEST 2021	Thu Jun 09 10:22:21 CEST 2022	771,49196-49195-49200-49199-159-158-49188-49187-49192-49191-49162-49161-49172-49171-157-156-61-60-53-47-10,5-10-11-13-35-23-65281,29-23-24,0	8916410db85077a5460817142dcbc8de

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 6528 Parent PID: 792

General

Start time:	15:21:49
Start date:	09/06/2021
Path:	C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\Microsoft Office\Office16\EXCEL.EXE' /automation -Embedding
Imagebase:	0x10000
File size:	27110184 bytes
MD5 hash:	5D6638F2C8F8571C593999C58866007E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: regsvr32.exe PID: 6796 Parent PID: 6528

General

Start time:	15:21:55
Start date:	09/06/2021
Path:	C:\Windows\SysWOW64\regsvr32.exe
Wow64 process (32bit):	true
Commandline:	regsvr32 -s ..\iepfusn.dll
Imagebase:	0xe50000
File size:	20992 bytes
MD5 hash:	426E7499F6A7346F0410DEAD0805586B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: regsvr32.exe PID: 6848 Parent PID: 6796

General

Start time:	15:21:56
Start date:	09/06/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	-s ..\iepfusn.dll
Imagebase:	0x7ff62a730000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: cmd.exe PID: 6980 Parent PID: 6848

General

Start time:	15:22:03
Start date:	09/06/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /c ping 8.8.7.7 -n 2 & start C:\Windows\system32\regsvr32.exe -s C:\Users\user\iepfusn.dll RV0KR
Imagebase:	0x7ff7180e0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 6988 Parent PID: 6980

General

Start time:	15:22:04
Start date:	09/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: PING.EXE PID: 7032 Parent PID: 6980

General

Start time:	15:22:04
Start date:	09/06/2021
Path:	C:\Windows\System32\PING.EXE
Wow64 process (32bit):	false
Commandline:	ping 8.8.7.7 -n 2
Imagebase:	0x7ff612a90000
File size:	21504 bytes
MD5 hash:	6A7389ECE70FB97BFE9A570DB4ACCC3B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Show Windows behavior

Analysis Process: regsvr32.exe PID: 5712 Parent PID: 6980

General

Start time:	15:22:13
Start date:	09/06/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe -s C:\Users\user\iepfusn.dll RV0KR
Imagebase:	0x7ff62a730000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Written

File Read

Analysis Process: cmd.exe PID: 1724 Parent PID: 5712

General

Start time:	15:22:17
Start date:	09/06/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false

Commandline:	cmd /c ping 8.8.7.7 -n 2 & start C:\Windows\system32\regsvr32.exe -s C:\Users\user\AppData\Local\Temp\L3YD7CE.dll N8DG
Imagebase:	0x7ff7180e0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 1808 Parent PID: 1724

General

Start time:	15:22:18
Start date:	09/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: PING.EXE PID: 6196 Parent PID: 1724

General

Start time:	15:22:19
Start date:	09/06/2021
Path:	C:\Windows\System32\PING.EXE
Wow64 process (32bit):	false
Commandline:	ping 8.8.7.7 -n 2
Imagebase:	0x7ff612a90000
File size:	21504 bytes
MD5 hash:	6A7389ECE70FB97BFE9A570DB4ACCC3B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

Analysis Process: regsvr32.exe PID: 6356 Parent PID: 1724

General

Start time:	15:22:28
Start date:	09/06/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe -s C:\Users\user\AppData\Local\Temp\L3YD7CE.dll N8DG

Imagebase:	0x7ff62a730000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Key Value Created

Analysis Process: cmd.exe PID: 6896 Parent PID: 6356

General

Start time:	15:22:34
Start date:	09/06/2021
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	cmd /c ping 8.8.7.7 -n 2 & start C:\Windows\system32\regsvr32.exe -s C:\Users\user\AppData\Local\Temp\L3YD7CE.dll VE50DB
Imagebase:	0x7ff7180e0000
File size:	273920 bytes
MD5 hash:	4E2ACF4F8A396486AB4268C94A6A245F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Analysis Process: conhost.exe PID: 5680 Parent PID: 6896

General

Start time:	15:22:34
Start date:	09/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: PING.EXE PID: 6092 Parent PID: 6896

General

Start time:	15:22:35
Start date:	09/06/2021
Path:	C:\Windows\System32\PING.EXE

Wow64 process (32bit):	false
Commandline:	ping 8.8.7.7 -n 2
Imagebase:	0x7ff612a90000
File size:	21504 bytes
MD5 hash:	6A7389ECE70FB97BFE9A570DB4ACCC3B
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: regsvr32.exe PID: 6872 Parent PID: 3440

General

Start time:	15:22:43
Start date:	09/06/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\system32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\L3YD7CE.dll VE50DB
Imagebase:	0x7ff62a730000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: regsvr32.exe PID: 6824 Parent PID: 6896

General

Start time:	15:22:44
Start date:	09/06/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\regsvr32.exe -s C:\Users\user\AppData\Local\Temp\L3YD7CE.dll VE50DB
Imagebase:	0x7ff62a730000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Analysis Process: regsvr32.exe PID: 400 Parent PID: 3440

General

Start time:	15:22:51
Start date:	09/06/2021
Path:	C:\Windows\System32\regsvr32.exe
Wow64 process (32bit):	false

Commandline:	'C:\Windows\system32\regsvr32.exe' -s C:\Users\user\AppData\Local\Temp\L3YD7CE.dll VE50DB
Imagebase:	0x7ff62a730000
File size:	24064 bytes
MD5 hash:	D78B75FC68247E8A63ACBA846182740E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

File Activities Show Windows behavior

Disassembly

Code Analysis