ID: 624181
Sample Name: EPAYMENT.exe
Cookbook: default.jbs
Time: 10:24:41
Date: 11/05/2022
Version: 34.0.0 Boulder Opal

Table of Contents

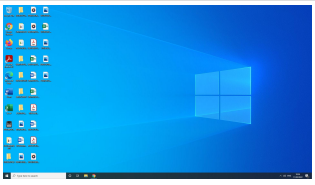
Windows Analysis Report

EPAYMENT.exe

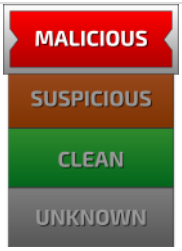
Overview

General Information

Sample Name:	EPAYMENT.exe
Analysis ID:	624181
MD5:	9811d64e29ef53..
SHA1:	b6e84580f902a0..
SHA256:	e94bcf64e3affd0..
Infos:	



Detection



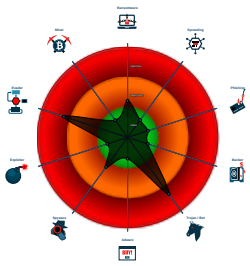
GuLoader

Score:	88
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Multi AV Scanner detection for subm…
- Yara detected GuLoader
- Initial sample is a PE file and has a…
- Writes to foreign memory regions
- Tries to detect Any.run
- Tries to detect sandboxes and other…
- Executable has a suspicious name …
- C2 URLs / IPs found in malware con…
- Uses 32bit PE files
- May sleep (evasive loops) to hinder…
- Contains functionality to shutdown /…

Classification



Process Tree

- **System is w10x64native**
- EPAYMENT.exe (PID: 1976 cmdline: "C:\Users\user\Desktop\EPAYMENT.exe" MD5: 9811D64E29EF53E107F9379526CFD338)
  - CasPol.exe (PID: 2376 cmdline: "C:\Users\user\Desktop\EPAYMENT.exe" MD5: 7BAE06CBE364BB42B8C34FCFB90E3EBD)
  - CasPol.exe (PID: 6908 cmdline: "C:\Users\user\Desktop\EPAYMENT.exe" MD5: 7BAE06CBE364BB42B8C34FCFB90E3EBD)
    - conhost.exe (PID: 7164 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: 81CA40085FC75BABD2C91D18AA9FFA68)
- **cleanup**

Malware Configuration

Threatname: GuLoader


```
{
  "Payload URL": "https://cdn.discordapp.com/attachments/973717070128771135/973717952987820073/a1.exe"
}
```


Yara Signatures

Memory Dumps

Source	Rule	Description	Author	Strings
0000000A.00000002.230879622484.0000000000F90000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
0000000A.00000000.225982150371.0000000000F90000.00000040.00000400.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	
00000002.00000002.226641346384.0000000003278000.00000040.00000800.00020000.00000000.sdmp	JoeSecurity_GuLoader_2	Yara detected GuLoader	Joe Security	

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Joe Sandbox Signatures

AV Detection

Found malware configuration

Multi AV Scanner detection for submitted file

Networking

C2 URLs / IPs found in malware configuration

System Summary

Initial sample is a PE file and has a suspicious name

Executable has a suspicious name (potential lure to open the executable)

Data Obfuscation

Yara detected GuLoader

Malware Analysis System Evasion

Tries to detect Any.run

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

HIPS / PFW / Operating System Protection Evasion

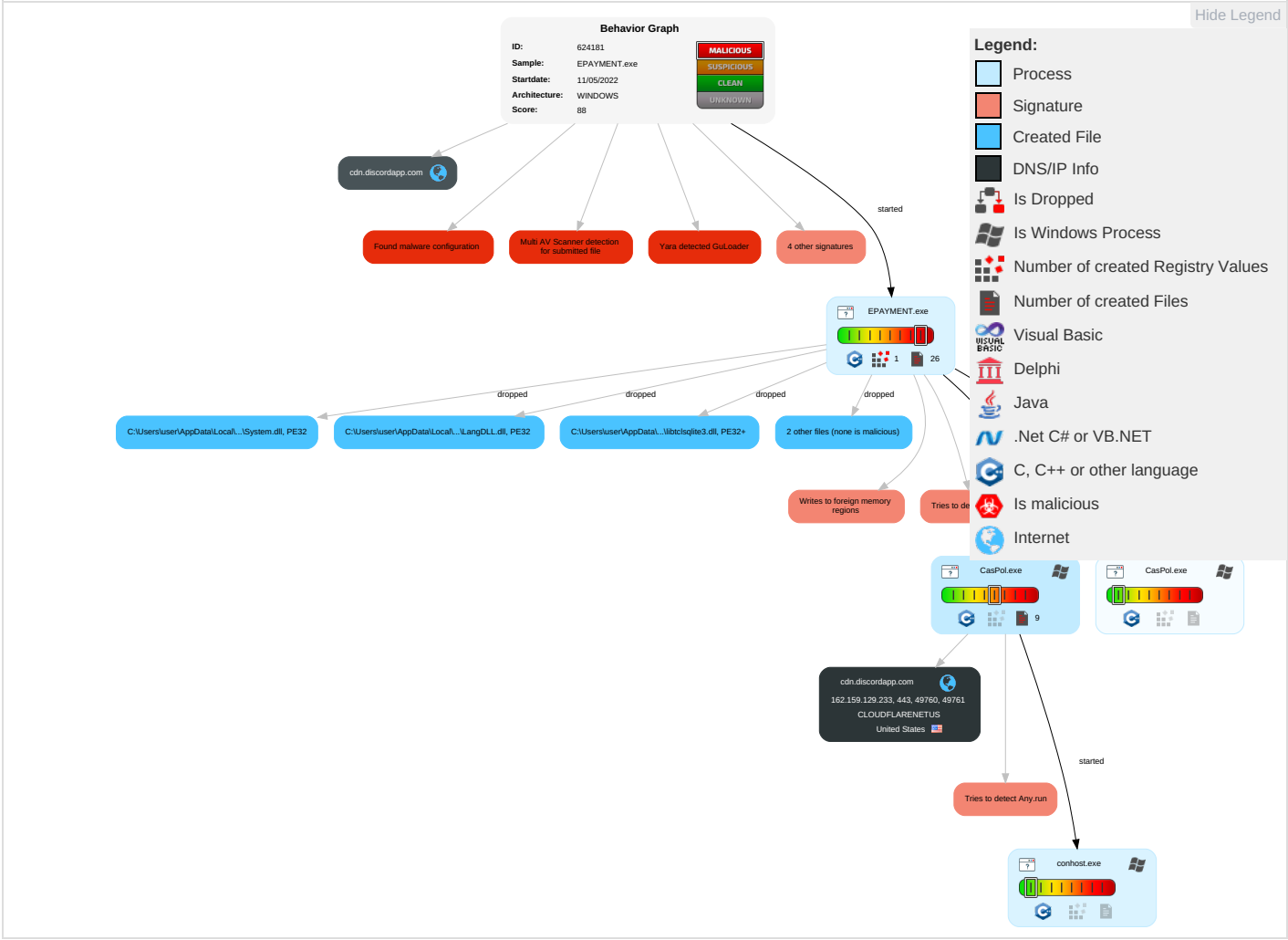
Writes to foreign memory regions

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Valid Accounts	1 Native API	1 DLL Side-Loading	1 Access Token Manipulation	1 2 Virtualization/Sandbox Evasion	OS Credential Dumping	2 2 1 Security Software Discovery	Remote Services	1 Archive Collected Data	Exfiltration Over Other Network Medium	1 2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	1 System Shutdown/ Reboot
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	1 1 1 Process Injection	1 Access Token Manipulation	LSASS Memory	1 2 Virtualization/Sandbox Evasion	Remote Desktop Protocol	1 Clipboard Data	Exfiltration Over Bluetooth	1 Non-Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects	Remote Service Effects	Impact
Domain Accounts	At (Linux)	Logon Script (Windows)	1 DLL Side-Loading	1 1 1 Process Injection	Security Account Manager	1 Application Window Discovery	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	1 2 Application Layer Protocol	Exploit SS7 to Track Device Location	Obtain Device Cloud Backups	Delete Device Data
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	1 Obfuscated Files or Information	NTDS	2 File and Directory Discovery	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap		Carrier Billing Fraud
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	1 DLL Side-Loading	LSA Secrets	4 System Information Discovery	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication		Manipulate App Store Rankings or Ratings

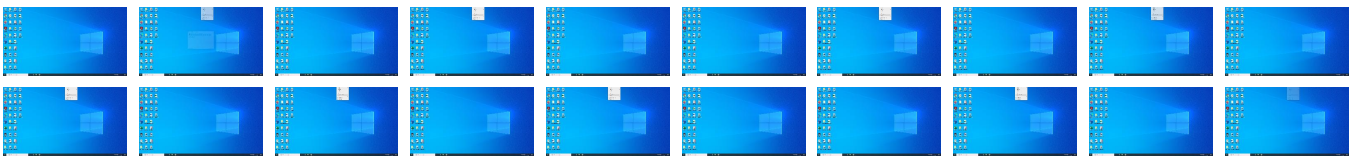
Behavior Graph

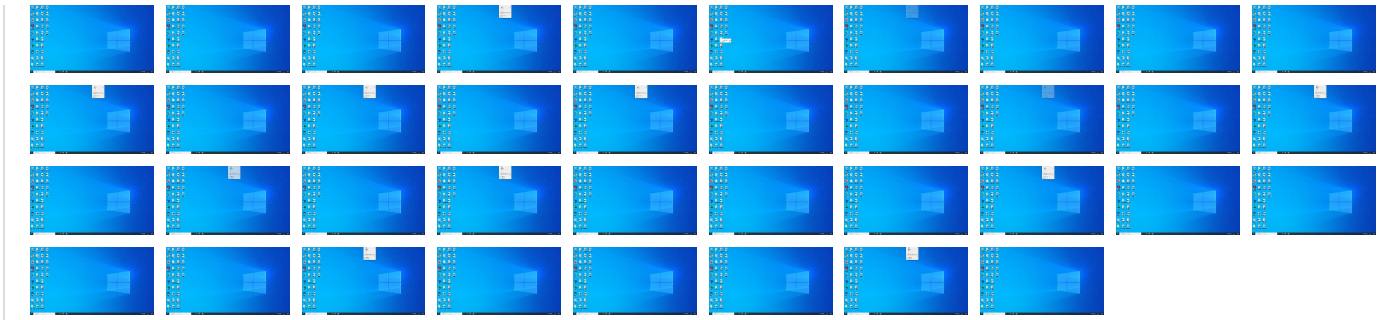


Screenshots

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
EPAYMENT.exe	17%	ReversingLabs	Win32.Trojan.Nemesis	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Local\Temp\ArmouryCrate.AppServiceBridge.exe	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\ArmouryCrate.AppServiceBridge.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\NeroCmd.exe	5%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\NeroCmd.exe	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\libtclsqlite3.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\libtclsqlite3.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsm2F8C.tmp\LangDLL.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsm2F8C.tmp\LangDLL.dll	0%	ReversingLabs		
C:\Users\user\AppData\Local\Temp\nsm2F8C.tmp\System.dll	0%	Metadefender		Browse
C:\Users\user\AppData\Local\Temp\nsm2F8C.tmp\System.dll	0%	ReversingLabs		

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	1%	Virustotal		Browse
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	0%	Avira URL Cloud	safe	
http://ocsp.sectigo.com0	0%	Avira URL Cloud	safe	
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	1%	Virustotal		Browse
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	0%	Avira URL Cloud	safe	
http://ocsp.thawte.com0	0%	Avira URL Cloud	safe	
http://https://sectigo.com/CPS0D	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
cdn.discordapp.com	162.159.129.233	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://https://cdn.discordapp.com/attachments/973717070128771135/973717952987820073/a1.exe	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://cdn.discordapp.com/lowedCert_AutoUpdate_1	CasPol.exe, 0000000A.00000003.2263822630 87.000000000117E000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://crl.sectigo.com/SectigoRSATimeStampingCA.crl0t	EPAYMENT.exe	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://cdn.discordapp.com/(	CasPol.exe, 0000000A.00000003.2277376472 33.000000000117E000.00000004.00000020.00 020000.00000000.sdmp, CasPol.exe, 000000 0A.00000003.226382263087.000000000117E00 0.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 0000000A.00000003.228270745395.000 000000117E000.00000004.00000020.00020000 .00000000.sdmp	false		high
http://https://cdn.discordapp.com/H	CasPol.exe, 0000000A.00000002.2308809788 04.000000000117E000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://creativecommons.org/licenses/by-sa/4.0/	audio-x-generic.png.2.dr	false		high
http://crl.thawte.com/ThawteTimestampingCA.crl0	EPAYMENT.exe, 00000002.00000002.22664025 9314.000000000292D000.00000004.00000800. 00020000.00000000.sdmp, NeroCmd.exe.2.dr	false		high
http://ocsp.sectigo.com0	EPAYMENT.exe	false	• Avira URL Cloud: safe	unknown
http://www.symauth.com/rpa00	EPAYMENT.exe, 00000002.00000002.22664025 9314.000000000292D000.00000004.00000800. 00020000.00000000.sdmp, NeroCmd.exe.2.dr	false		high
http://crt.sectigo.com/SectigoRSATimeStampingCA.crt0#	EPAYMENT.exe	false	• 1%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://cdn.discordapp.com/attachments/97371707012 8771135/973718274879651920/divinbot_LnXMPAfP50 .bin	CasPol.exe, 0000000A.00000003.2271938043 40.000000000117E000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://ocsp.thawte.com0	EPAYMENT.exe, 00000002.00000002.22664025 9314.000000000292D000.00000004.00000800. 00020000.00000000.sdmp, NeroCmd.exe.2.dr	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.nero.com	NeroCmd.exe.2.dr	false		high
http://https://cdn.discordapp.com/soft	CasPol.exe, 0000000A.00000003.2271938043 40.000000000117E000.00000004.00000020.00 020000.00000000.sdmp	false		high
http://https://sectigo.com/CPS0D	EPAYMENT.exe	false	• Avira URL Cloud: safe	unknown
http://https://cdn.discordapp.com/X	CasPol.exe, 0000000A.00000003.2277376472 33.000000000117E000.00000004.00000020.00 020000.00000000.sdmp, CasPol.exe, 000000 0A.00000003.229375840195.000000000117E00 0.00000004.00000020.00020000.00000000.sdmp	false		high
http://https://cdn.discordapp.com/	CasPol.exe, 0000000A.00000002.2308809788 04.000000000117E000.00000004.00000020.00 020000.00000000.sdmp, CasPol.exe, 000000 0A.00000003.227737647233.000000000117E00 0.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 0000000A.00000003.228289426325.000 000000117E000.00000004.00000020.00020000 .00000000.sdmp, CasPol.exe, 0000000A.000 00003.226382263087.000000000117E000.0000 0004.00000020.00020000.00000000.sdmp, Ca sPol.exe, 0000000A.00000002.230880062647 .00000000010D2000.00000004.00000020.0002 0000.00000000.sdmp, CasPol.exe, 0000000A .00000003.230470347663.00000000010D2000. 00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 0000000A.00000003.22937609 3740.00000000010D2000.00000004.00000020. 00020000.00000000.sdmp, CasPol.exe, 0000 000A.00000003.228270370287.0000000001127 000.00000004.00000020.00020000.00000000.sdmp, CasPol.exe, 0000000A.00000003.230469971603.0 00000001D768000.00000004.00000800.000200 00.00000000.sdmp, CasPol.exe, 0000000A.0 0000003.228270745395.000000000117E000.00 000004.00000020.00020000.00000000.sdmp, CasPol.exe, 0000000A.00000003.2293758401 95.000000000117E000.00000004.00000020.00 020000.00000000.sdmp, CasPol.exe, 000000 0A.00000003.227193804340.000000000117E00 0.00000004.00000020.00020000.00000000.sdmp	false		high
http://nsis.sf.net/NSIS_ErrorError	EPAYMENT.exe	false		high
http://https://cdn.discordapp.com/attachments/973717070128771135/973717952987820073/a1.exehttps://cdn.disco	CasPol.exe, 0000000A.00000002.2308812112 63.00000000012D1000.00000004.00000800.00 020000.00000000.sdmp	false		high
http://www.symauth.com/cps0(	EPAYMENT.exe, 00000002.00000002.22664025 9314.000000000292D000.00000004.00000800. 00020000.00000000.sdmp, NeroCmd.exe.2.dr	false		high

World Map of Contacted IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
162.159.129.233	cdn.discordapp.com	United States		13335	CLOUDFLARENETUS	false

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	624181
Start date and time: 11/05/202210:24:41	2022-05-11 10:24:41 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 21s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	EPAYMENT.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit 20H2 Native **physical Machine for testing VM-aware malware** (Office 2019, IE 11, Chrome 93, Firefox 91, Adobe Reader DC 21, Java 8 Update 301
Run name:	Suspected Instruction Hammering
Number of analysed new started processes analysed:	24
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:	mal88.troj.evad.winEXE@7/10@1/1
EGA Information:	• Successful, ratio: 100%

HDC Information:	• Successful, ratio: 26.3% (good quality ratio 25.9%) • Quality average: 88.6% • Quality standard deviation: 21.6%
HCA Information:	• Successful, ratio: 95% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .exe • Adjust boot time • Enable AMSI

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, BackgroundTransferHost.exe, RuntimeBroker.exe, backgroundTaskHost.exe, svchost.exe
- TCP Packets have been reduced to 100
- Excluded domains from analysis (whitelisted): ris.api.iris.microsoft.com, wdcpalt.microsoft.com, client.wns.windows.com, ctldl.windowsupdate.com, wdcp.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, arc.msn.com
- Not all processes where analyzed, report is missing behavior information
- Report size exceeded maximum capacity and may have missing network information.
- Report size getting too big, too many NtDeviceIoControlFile calls found.
- Report size getting too big, too many NtOpenKeyEx calls found.
- Report size getting too big, too many NtProtectVirtualMemory calls found.
- Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
10:27:12	API Interceptor	1558x Sleep call for process: CasPol.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASNs

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\ArmouryCrate.AppServiceBridge.exe

Process:	C:\Users\user\Desktop\EPAYMENT.exe
File Type:	PE32 executable (console) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	23272

Entropy (8bit):	6.162753529320517
Encrypted:	false
SSDEEP:	384:VHgV9NMVOQA17TvjHj9vtqM1J/FMPjbyJ5WMQJK2wKucYUyGJhHH:VADCVc7ZFHF6juJ5D2X9DJhH
MD5:	19E44C0A8284EFB1E82BD1BB2ACC8EB1
SHA1:	1321814D12BA3FB035071BFB036F762E14824A85
SHA-256:	80F180CEC8BB6E524E7A3D5B9858020AF99869EDABFAD1F594A62DD246F1194E
SHA-512:	7531A6EED220BD1AA1C92E33B35D9D2CE824B75D007C8D581A030EE52EEECA0ADDECE6B6352FE77BE2146EF7F247E65C70ACE344B2296FAB1939046D783F427F
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Z....."...0..0.....&N... ...`....@.. .....`.....M..O...`..L.....<.....L.....text...,.... ...0..... ..`.rsrc...L....`.....2.....@..@.rel oc.....:.....@..B.....N.....H.....1.....0.....(...+.@.....s.....(.....o.....s...%o....&%o.....o.....o..... ...,...o.....,...o.....&.....9d...s.....o.....o.....o.....+. ....(.....o...,...o.....:.....(.....o .....+. ....(.....o....,...o!.....o"...:.....o#...r...po$...,...o#...r...po%.....+. .....o#...r. ..po$...,}..o#...r...po%...t....(....o.....(.....j ....jo&.....

C:\Users\user\AppData\Local\Temp\NeroCmd.exe

Process:	C:\Users\user\Desktop\EPAYMENT.exe
File Type:	PE32 executable (console) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	215928
Entropy (8bit):	5.786985951434551
Encrypted:	false
SSDEEP:	3072:vMYGi18N39JYhuryGeqD01AYy5WKKB0vO9/s7oJfhLndhh9vCEyBinlYNZTy7F9Z:vRuryGpoksksnTSvM
MD5:	D74AB8F08D67A289D01DEFC064BFCDA9
SHA1:	FD407C22AE7E90CA599A5B6150AD2E256750400F
SHA-256:	FC26BCD62EDF699C82D67A354F223430F9CD9844189A0933D3402A2BAC4C2005
SHA-512:	119E680A65FE50636BE199A5ED203FFFDD22C4FA1B75BA92DF536951B5002A907FE404F3BB548AB39BC5E54D34E1547FBAAE988147D80790CDFC4382E5F803A3
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 5%, Browse • Antivirus: ReversingLabs, Detection: 0%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....(...{...{...{H=X{...{H=[{...{H=^{...{H=Z{...{...{...{.f>{...{{.Z{...{..^{...{...{...{..Z{...{..\{...{..Y{...{Rich...{.....PE..L....W.V.....u.....@.....p.....c....@.....@.....x3...P.....@...8.....@.....text...;..... ..`.rdata..rb.....d.....@..@.data.....@....shared.....0.....@. ...rsrc.....@.....@..@.reloc..R....P.....@..B..... .....

C:\Users\user\AppData\Local\Temp\Nysene7.Bru4

Process:	C:\Users\user\Desktop\EPAYMENT.exe
File Type:	data
Category:	dropped
Size (bytes):	78447
Entropy (8bit):	6.497483193133565
Encrypted:	false
SSDEEP:	1536:brvB0TYtiX9UmRWO38QRb17dFiGBdaB0CgzFkkv7j1nn:/vYLA7ab1Xp3aB0CIq2B
MD5:	BA4672E4475BDC8152DBD5DF6605682C
SHA1:	A808B14BC9935E47495E721B75B0241E84084769
SHA-256:	73C68FE84E10437CEF3CB3E7159CB81913E622FCAA04A3D5A8751DEBAF70881B
SHA-512:	DF503DEC8D30269C491C0B699228D35B5D26C707B36F6F553882F290560E5346793F0D2A041BF0685CA7B42B1421CF71FFDD1197FF192DD3275342E91AC34F6E
Malicious:	false
Antivirus:	
Reputation:	low
Preview:	.....Hm.....-[..N.....f.f..,.).x888888888888888888888888888888888888888_.....'.2P.HHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHHH<..t....'...n.....f.....*j%.C.....2H.....<A.....@/h22222222222222222222222222222222222222222<.....7.8}!.....1..e.....cl;.....`..0...njjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjjj..~....5..$/.....+]4w..... .....<{.....8Y."..iiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii..Y.....4..... ..K1.....q....W.;IIIIIIIIIIIIIIIIIIIIIIIIII.....5.X.~..... .....4$.....c...4...d.....

C:\Users\user\AppData\Local\Temp\a1.exe

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
File Type:	XML 1.0 document text

Category:	dropped
Size (bytes):	223
Entropy (8bit):	4.745008847905136
Encrypted:	false
SSDEEP:	6:TM3i0b9ZjZvKtWRbtmdsfbPAxjqm1bANKvn:TM3i0b9BZKtWRbtmdsfbPAxjqSkNKv
MD5:	A6A676051F857D516F6C4BEC595A7CFB
SHA1:	10E7C48A109FFBE60FA7AB3585C4BD711942CBD2
SHA-256:	98686E602B5F75BBCEB801CA315617579AD9FFE9E2DF66D49673EA35A7E1F343
SHA-512:	DF302B28E5897BAC668AD1AE2B32D2424AF7C8CDF4527AC54EA268E6E9FBF41EFE28B236AF25CEACB5E5ACD95B6C99B8CF95FA735687358A265BD59E2B127BA6
Malicious:	false
Preview:	<?xml version='1.0' encoding='UTF-8'?><Error><Code>AccessDenied</Code><Message>Access denied.</Message><Details>Anonymous caller does not have storage .objects.get access to the Google Cloud Storage object.</Details></Error>

C:\Users\user\AppData\Local\Temp\audio-x-generic.png

Process:	C:\Users\user\Desktop\EPAYMENT.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	857
Entropy (8bit):	7.4319481758097155
Encrypted:	false
SSDEEP:	12:6v/7wtZB4RO4HE+swFIP2sdDYJYRelujZwNjCitHn9q+kfbtvMy+3HgZUh2:Xtk15/OmYRe7CitH9qPbtv83HgZU2
MD5:	CA015E7C4B05BD9FB87AF3772AD92E5C
SHA1:	E31B3BF7D29D3185FCE5A5E36D54DD804FB74564
SHA-256:	F7C132E53160C6A7CC9A79CB74DCCC3762C4A96BB4987B6E1A8755A270905976
SHA-512:	FFF2A7B0878F32C4D21FA0512FC5606611CB9726DDCE5C4542470AC6E2AC7A6CB31B38E5E27CEA750165ED0E7DFF7EC3814EB06A5AC059B1D9B81A523ADF243
Malicious:	false
Preview:	.PNG.....IHDR.....a....sBIT....|.d.....pHYs.....+.....tEXtSoftware.www.inkscape.org..<.....tEXtTitle.Adwaita Icon Template...?....tEXtAuthor.GNOME Design Team`.v~...RtEXtCopyright.CC Attribution-ShareAlike http://creativecommons.org/licenses/by-sa/4.0/.Tb....-IDAT8...?hTA....v.K.wG...c..@H. .....F-$...J...2(Vj!..b.....$E.s.\.. .....X.....r...7...Yjg..[.YE..U..tnv.X.....J.....].!*.....I.AA.....w7..{ V..\..F.Th..g...~}...D..... >..{...q....E..u{.D....W....03#..!PS.....bfk.fex.2.r_..x.1.`K@.9.....U..9..@..... ]6Wg..WG....2|.)..I..21.a.*..>1946<.K...kH..}.(.....U.}=.LzP..P..L$H....`e.._B...lbT.w.T<.A...5.....9`..!.7p..7..8..)...8`.f. .K.1c.~.h.G=k.a3...j,.h....?.6#..l...(....D.!b.7...o.f.....V7.s 7Q..n.S[.n.K..]@....K?5....(....;.{.{ >....+.Wj/.....x.R....._..O5.....IEND.B`.

C:\Users\user\AppData\Local\Temp\camera-photo.png

Process:	C:\Users\user\Desktop\EPAYMENT.exe
File Type:	PNG image data, 16 x 16, 8-bit/color RGBA, non-interlaced
Category:	dropped
Size (bytes):	764
Entropy (8bit):	7.7061001591040155
Encrypted:	false
SSDEEP:	12:6v/7UuL/1leVdkTaP4LAtxU5Tslf/4qlgOa9WG6q9STu/Z4E5sJekNLo21VPulL4:7uL/zCkTaHt/lf/4rxMG6G7sJbcuP7
MD5:	649C9AB161501E1AA88B3D32C4F71023
SHA1:	A916E4161B6A0F11F0DA539EEEF4513E5FB08FE2
SHA-256:	D69CFE54FF9E3249DA241654FFA768D23E52297E7459FE61662C4129850D16AF
SHA-512:	8F1C8215B98C5488B53DB538E7980F82CC9C4B0A872DFD23E63412B50B629F08DB2D085E8B7A15A0BEE5527560708917D4D2B4D6C794C3D352DE056AB2F57E2
Malicious:	false
Preview:	.PNG.....IHDR.....a....IDATx.....dW.@.{.0...m.VX.q...V....m..5.{o9A}.k.+.P(..P..=....:.....2.e.!.k..v..#GV,^..*..TVV..l...o..l."..."....G..@y...t:...Pq.....9.i.X,.TU..p.A2.... ...].:333.....X&g.....y.8....;..{p{.TUU.k.S3.:..`..O?.Lh..W...05....m.6$rU._S].7.DeE9R~zf.C.9~..n....T1.....>..^..5..c.y..|..as:....KJP)p.....p.5. ....v$9..(.n..+.....&.....BU...D... &....$.....x....<..+.....p(D.....%.I....zm1..t#>._.....Y.. ..0.d.....*....`bb....d..C..Q..+.....R_WGbh.F..d`X.j.eee....#.L.I.h*C1V.....jkk..o9.....E9z.8S.c.....D..#-...Y.|..d.2.G.W.. ...}.O.....f.....O.....q.q.\.....X.f..\.....X./r2w...Q.:M..K.n..I(..Y...OX.b.Z.A.y..I.R.v.2....x.....;.<`).4.....~..B>.QE"....IEND.B`.

C:\Users\user\AppData\Local\Temp\libtclsqlite3.dll

Process:	C:\Users\user\Desktop\EPAYMENT.exe
File Type:	PE32+ executable (DLL) (console) x86-64, for MS Windows
Category:	dropped
Size (bytes):	172061
Entropy (8bit):	5.423536082857285
Encrypted:	false
SSDEEP:	1536:cRG/dDih4WuPLfJ0NJ/OdJLpppxejxgE2h7iK9nXHe2n0S0uf44PO:JkeEOJLpppm6N0Sr4aO
MD5:	97F6D21CE726247E03A03D7F03D0A847
SHA1:	4D94D170078B3422E410D5E6DE3DCA74CB7E6457

SHA-256:	9E81CE570879BC87D332989561234AD5BB8BDA62D30A320A76A4373863BF6012
SHA-512:	983E78C81AD69F52E4594D19BB3D1BC06C55DE54E2569290566185934B184B4F81D13F80ABBBDE749894599E7071CE52935988CD527BF21C9CE246914AE9C0D
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..d...`L.`.....& ...$.....P..... ..`... .....0.....@.....h.....(.....D.....text.....`.P`.data...`.....@.` ..rdata.....@.`@.pdata..h.....@.0@.xdata.....@.0@.bss....0.... .....`..edata.....0.....@.0@.idata.....@..... .....@.0..CRT....X...`.....@.@..tls.....p.....@.@..reloc.....@.0B/4.....@.PB/19.....C.....@.. B/31..... .....@..B/45.....@... .....@..B/57.....

C:\Users\user\AppData\Local\Temp\list-drag-handle-symbolic.svg

Process:	C:\Users\user\Desktop\EPAYMENT.exe
File Type:	SVG Scalable Vector Graphics image
Category:	dropped
Size (bytes):	624
Entropy (8bit):	3.5629799376743088
Encrypted:	false
SSDEEP:	12:t4CDqKIUMUMfUMUMK5UM4IIUMUMfUMUMK5UM4JIUMUMfUMUMK5UM4IIUMUMfUMUo:t4CVI55f55U5rI55f55U5sI55f55U5rs
MD5:	1BA333F3E126D8A83CA3C6FCFB71FBC8
SHA1:	D54F87C1937D6A08455C903B4E60F6B390A9C583
SHA-256:	7DEC55F99B6FA48395B801EDE687C47330E79C4045F48B7AF673FB259F29FF32
SHA-512:	AA2E2E617E28925B3C69C25E9CD87073D7346544CFDA1B106D4A2198818F82895355B4F8FA6EF98242730565153C1EF3BDBDAF63864A3F186171AB81E3DE342A
Malicious:	false
Preview:	<svg xmlns="http://www.w3.org/2000/svg" width="16" height="16"><path d="M4.494 0a1.5 1.5 0 00-1.5 1.5 1.5 1.5 0 001.5 1.5 1.5 1.5 0 001.5-1.5 1.5 1.5 0 00-1.5-1 .5zm6 0a1.5 1.5 0 00-1.5 1.5 1.5 1.5 0 001.5 1.5 1.5 1.5 0 001.5-1.5 1.5 1.5 0 00-1.5-1.5zm-6 6a1.5 1.5 0 00-1.5 1.5 1.5 1.5 0 001.5 1.5 1.5 1.5 0 001.5-1.5 1.5 1.5 0 00- 1.5-1.5zm6 0a1.5 1.5 0 00-1.5 1.5 1.5 1.5 0 001.5 1.5 1.5 1.5 0 001.5-1.5 1.5 1.5 0 00-1.5-1.5zm-6 6a1.5 1.5 0 00-1.5 1.5 1.5 1.5 0 001.5 1.5 1.5 1.5 0 001.5-1.5 1.5 1.5 0 00-1.5-1.5zm6 0a1.5 1.5 0 00-1.5 1.5 1.5 1.5 0 001.5 1.5 1.5 1.5 0 001.5-1.5 1.5 1.5 0 00-1.5-1.5z" fill="#2e3436"/></svg>

C:\Users\user\AppData\Local\Temp\nsm2F8C.tmp\LangDLL.dll

Process:	C:\Users\user\Desktop\EPAYMENT.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	5632
Entropy (8bit):	3.81812520226775
Encrypted:	false
SSDEEP:	48:S46+/nTKYKxbWsptIpBtWZ0iV8jAWiAJCvxft2O2B8mFofjLl:zFuPbOBtWZBV8jAWiAJCdv2Cm0L
MD5:	68B287F4067BA013E34A1339AFDB1EA8
SHA1:	45AD585B3CC8E5A6AF7B68F5D8269C97992130B3
SHA-256:	18E8B40BA22C7A1687BD16E8D585380BC2773FFF5002D7D67E9485FCC0C51026
SHA-512:	06C38BBB07FB55256F3CDC24E77B3C8F3214F25BFD140B521A39D167113BF307A7E8D24E445D510BC5E4E41D33C9173BB14E3F2A38BC29A0E3D08C1F0DCA4E DB
Malicious:	false
Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....>.....:.....Rich.....PE..L....Oa.....!... .....".....?..... .....p.....@.....`"..I...\ ..P....P..`.....`..... ..\.....text..... .. `.rdata..... .....@..@.data.....0.....@....rsrc...`....P.....@..@.reloc..`....`.....@..B..... .....

C:\Users\user\AppData\Local\Temp\nsm2F8C.tmp\System.dll

Process:	C:\Users\user\Desktop\EPAYMENT.exe
File Type:	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
Category:	modified
Size (bytes):	12288
Entropy (8bit):	5.814115788739565
Encrypted:	false
SSDEEP:	192:Zjvco0qWTlt70m5Aj/lQ0sEWD/wtYbBHFNaDybC7y+XBz0QPi:FHQlt70mij/lQRv/9VMjzr
MD5:	CFF85C549D536F651D4FB8387F1976F2
SHA1:	D41CE3A5FF609DF9CF5C7E207D3B59BF8A48530E
SHA-256:	8DC562CDA7217A3A52DB898243DE3E2ED68B80E62DDCB8619545ED0B4E7F65A8
SHA-512:	531D6328DAF3B86D85556016D299798FA06FEFC81604185108A342D000E203094C8C12226A12BD6E1F89B0DB501FB66F827B610D460B933BD4AB936AC2FD8A88
Malicious:	false

Antivirus:	• Antivirus: Metadefender, Detection: 0%, Browse • Antivirus: ReversingLabs, Detection: 0%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....qr*.5.D.5.D.5.D...J.2.D.5.E.!.D.....2.D.a0t.1.D.V1n.4.D..3@.4. D.Rich5.D.....PE..L.....Oa.....!.....".....*.....@.....p.....@.....B.....@..P.....`.....@..X. .....text.... .....".....  ..`.rdata..c...@.....&.....@..@.data...x...P.....*.....@....reloc.....`.....,.....@..B..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	6.93430870701767
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	EPAYMENT.exe
File size:	384544
MD5:	9811d64e29ef53e107f9379526cfd338
SHA1:	b6e84580f902a0c3d3f77748a2a027c9fe42db68
SHA256:	e94bcf64e3affd0a755df05fc1f8c7fba1fb98303e433edff4d98f75d1e4fdf8
SHA512:	c6846c98cdd741f95273166b88081709125ce4e7f25ea7ab5841fdbb147cc29663ab7a881f059cc8e54735ab2ef680998ae59c8bcbd0a3b6e4f7629abf54c91e
SSDEEP:	6144:cYa6FhyPsCD05Fo1/atIU3jNJ7CIzAlb5Eyy77XEwPBkbCt:cYve1/OIMB1RzAlb8zE08C
TLSH:	DE84BFA63F19CC11C39094FD6621E1E999B56E2027BA8662F3E13F6F756CF427D0D202
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....1...Pf..Pf..Pf.*_9..Pf..Pg.LPf.*_;..Pf..sV..Pf..V`..Pf.Rich.Pf.....PE..L.....Oa.....h...*.....

File Icon

Icon Hash:	d0d4d6ccb2ece8d2

Static PE Info

General

Entrypoint:	0x403640
Entrypoint Section:	.text
Digitally signed:	true
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x614F9B1F [Sat Sep 25 21:56:47 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	61259b55b8912888e90f516ca08dc514

Authenticode Signature

Signature Valid:	**false**
Signature Issuer:	CN="Athyria Nongrounding6 ", O=Love, L=East Somerton, S=England, C=GB
Signature Validation Error:	**A certificate chain processed, but terminated in a root certificate which is not trusted by the trust provider**
Error Number:	-2146762487
Not Before, Not After	• 10/05/2022 23:50:02 10/05/2023 23:50:02

Subject Chain	• CN="Athyria Nongrounding6 ", O=Love, L=East Somerton, S=England, C=GB
Version:	3
Thumbprint MD5:	1C850933333AFF3DA0E7F4C963D569F0
Thumbprint SHA-1:	07B50D61787E7BBD1B41CA33E6A1258B648D7650
Thumbprint SHA-256:	1477FB61D72ED9022411300487096BB783B852377EA8078EB9A562BE2CB599E8
Serial:	935DAD340200F0CA

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
sub esp, 000003F4h
push ebx
push esi
push edi
push 00000020h
pop edi
xor ebx, ebx
push 00008001h
mov dword ptr [ebp-14h], ebx
mov dword ptr [ebp-04h], 0040A230h
mov dword ptr [ebp-10h], ebx
call dword ptr [004080C8h]
mov esi, dword ptr [004080CCh]
lea eax, dword ptr [ebp-00000140h]
push eax
mov dword ptr [ebp-0000012Ch], ebx
mov dword ptr [ebp-2Ch], ebx
mov dword ptr [ebp-28h], ebx
mov dword ptr [ebp-00000140h], 0000011Ch
call esi
test eax, eax
jne 00007FC13D437B1Ah
lea eax, dword ptr [ebp-00000140h]
mov dword ptr [ebp-00000140h], 00000114h
push eax
call esi
mov ax, word ptr [ebp-0000012Ch]
mov ecx, dword ptr [ebp-00000112h]
sub ax, 00000053h
add ecx, FFFFFFD0h
neg ax
sbb eax, eax
mov byte ptr [ebp-26h], 00000004h
not eax
and eax, ecx
mov word ptr [ebp-2Ch], ax
cmp dword ptr [ebp-0000013Ch], 0Ah
jnc 00007FC13D437AEAh
and word ptr [ebp-00000132h], 0000h
mov eax, dword ptr [ebp-00000134h]
movzx ecx, byte ptr [ebp-00000138h]
mov dword ptr [0042A318h], eax
xor eax, eax
mov ah, byte ptr [ebp-0000013Ch]
movzx eax, ax
or eax, ecx
xor ecx, ecx
mov ch, byte ptr [ebp-2Ch]
movzx ecx, cx

Instruction
shl eax, 10h
or eax, ecx

Rich Headers

Programming Language:	• [EXP] VC++ 6.0 SP5 build 8804

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x8504	0xa0	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x52000	0x28408	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x5c458	0x19c8	.rsrc
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x8000	0x2b0	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x6676	0x6800	False	0.656813401442	data	6.41745998719	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x8000	0x139a	0x1400	False	0.4498046875	data	5.14106681717	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0xa000	0x20378	0x600	False	0.509765625	data	4.11058212765	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x2b000	0x27000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x52000	0x28408	0x28600	False	0.228412828947	data	4.94608860234	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_ICON	0x52328	0x10828	dBase IV DBT, blocks size 0, block length 2048, next free block index 40, next free block 0, next used block 0	English	United States
RT_ICON	0x62b50	0x94a8	data	English	United States
RT_ICON	0x6bff8	0x5488	data	English	United States
RT_ICON	0x71480	0x4228	dBase IV DBT of \200.DBF, blocks size 0, block length 16896, next free block index 40, next free block 4294967295, next used block 4294967295	English	United States
RT_ICON	0x756a8	0x25a8	data	English	United States
RT_ICON	0x77c50	0x10a8	data	English	United States
RT_ICON	0x78cf8	0x988	data	English	United States
RT_ICON	0x79680	0x468	GLS_BINARY_LSB_FIRST	English	United States
RT_DIALOG	0x79ae8	0x100	data	English	United States
RT_DIALOG	0x79be8	0x11c	data	English	United States
RT_DIALOG	0x79d08	0x60	data	English	United States
RT_GROUP_ICON	0x79d68	0x76	data	English	United States
RT_VERSION	0x79de0	0x2e4	data	English	United States

Name	RVA	Size	Type	Language	Country
RT_MANIFEST	0x7a0c8	0x33e	XML 1.0 document, ASCII text, with very long lines, with no line terminators	English	United States

Imports

DLL	Import
ADVAPI32.dll	RegCreateKeyExW, RegEnumKeyW, RegQueryValueExW, RegSetValueExW, RegCloseKey, RegDeleteValueW, RegDeleteKeyW, AdjustTokenPrivileges, LookupPrivilegeValueW, OpenProcessToken, SetFileSecurityW, RegOpenKeyExW, RegEnumValueW
SHELL32.dll	SHGetSpecialFolderLocation, SHFileOperationW, SHBrowseForFolderW, SHGetPathFromIDListW, ShellExecuteExW, SHGetFileInfoW
ole32.dll	OleInitialize, OleUninitialize, CoCreateInstance, IIDFromString, CoTaskMemFree
COMCTL32.dll	ImageList_Create, ImageList_Destroy, ImageList_AddMasked
USER32.dll	GetClientRect, EndPaint, DrawTextW, IsWindowEnabled, DispatchMessageW, wsprintfA, CharNextA, CharPrevW, MessageBoxIndirectW, GetDlgItemTextW, SetDlgItemTextW, GetSystemMetrics, FillRect, AppendMenuW, TrackPopupMenu, OpenClipboard, SetClipboardData, CloseClipboard, IsWindowVisible, CallWindowProcW, GetMessagePos, CheckDlgButton, LoadCursorW, SetCursor, GetSysColor, SetWindowPos, GetWindowLongW, PeekMessageW, SetClassLongW, GetSystemMenu, EnableMenuItem, GetWindowRect, ScreenToClient, EndDialog, RegisterClassW, SystemParametersInfoW, CreateWindowExW, GetClassInfoW, DialogBoxParamW, CharNextW, ExitWindowsEx, DestroyWindow, CreateDialogParamW, SetTimer, SetWindowTextW, PostQuitMessage, SetForegroundWindow, ShowWindow, wsprintfW, SendMessageTimeoutW, FindWindowExW, IsWindow, GetDlgItem, SetWindowLongW, LoadImageW, GetDC, ReleaseDC, EnableWindow, InvalidateRect, SendMessageW, DefWindowProcW, BeginPaint, EmptyClipboard, CreatePopupMenu
GDI32.dll	SetBkMode, SetBkColor, GetDeviceCaps, CreateFontIndirectW, CreateBrushIndirect, DeleteObject, SetTextColor, SelectObject
KERNEL32.dll	GetExitCodeProcess, WaitForSingleObject, GetModuleHandleA, GetProcAddress, GetSystemDirectoryW, lstrcatW, Sleep, lstrcpyA, WriteFile, GetTempFileNameW, lstrcmpiA, RemoveDirectoryW, CreateProcessW, CreateDirectoryW, GetLastError, CreateThread, GlobalLock, GlobalUnlock, GetDiskFreeSpaceW, WideCharToMultiByte, lstrcpynW, lstrlenW, SetErrorMode, GetVersionExW, GetCommandLineW, GetTempPathW, GetWindowsDirectoryW, SetEnvironmentVariableW, CopyFileW, ExitProcess, GetCurrentProcess, GetModuleFileNameW, GetFileSize, CreateFileW, GetTickCount, MulDiv, SetFileAttributesW, GetFileAttributesW, SetCurrentDirectoryW, MoveFileW, GetFullPathNameW, GetShortPathNameW, SearchPathW, CompareFileTime, SetFileTime, CloseHandle, lstrcmpiW, lstrcmpW, ExpandEnvironmentStringsW, GlobalFree, GlobalAlloc, GetModuleHandleW, LoadLibraryExW, MoveFileExW, FreeLibrary, WritePrivateProfileStringW, GetPrivateProfileStringW, lstrlenA, MultiByteToWideChar, ReadFile, SetFilePointer, FindClose, FindNextFileW, FindFirstFileW, DeleteFileW

Version Infos

Description	Data
LegalCopyright	Triad Hospitals Inc
FileVersion	22.18.23
CompanyName	Lawson Software
LegalTrademarks	R.J. Reynolds Tobacco Company
Comments	Tecumseh Products Company
ProductName	Bell Microproducts Inc.
FileDescription	Rohm & Haas Co.
Translation	0x0409 0x04b0

Possible Origin

Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2022 10:27:12.100692034 CEST	49760	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:12.100784063 CEST	443	49760	162.159.129.233	192.168.11.20
May 11, 2022 10:27:12.100961924 CEST	49760	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:12.129106998 CEST	49760	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:12.129131079 CEST	443	49760	162.159.129.233	192.168.11.20

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2022 10:27:12.153850079 CEST	443	49760	162.159.129.233	192.168.11.20
May 11, 2022 10:27:12.154047966 CEST	49760	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:12.271070957 CEST	49760	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:12.271826029 CEST	443	49760	162.159.129.233	192.168.11.20
May 11, 2022 10:27:12.271997929 CEST	49760	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:12.275578022 CEST	49760	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:12.318500042 CEST	443	49760	162.159.129.233	192.168.11.20
May 11, 2022 10:27:12.461464882 CEST	443	49760	162.159.129.233	192.168.11.20
May 11, 2022 10:27:12.461642027 CEST	49760	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:12.461692095 CEST	443	49760	162.159.129.233	192.168.11.20
May 11, 2022 10:27:12.461833000 CEST	49760	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:12.461944103 CEST	49760	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:12.462421894 CEST	443	49760	162.159.129.233	192.168.11.20
May 11, 2022 10:27:12.462579012 CEST	443	49760	162.159.129.233	192.168.11.20
May 11, 2022 10:27:12.462965012 CEST	49760	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:12.463004112 CEST	49760	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:12.942066908 CEST	49761	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:12.942145109 CEST	443	49761	162.159.129.233	192.168.11.20
May 11, 2022 10:27:12.942429066 CEST	49761	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:12.942828894 CEST	49761	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:12.942881107 CEST	443	49761	162.159.129.233	192.168.11.20
May 11, 2022 10:27:12.965676069 CEST	443	49761	162.159.129.233	192.168.11.20
May 11, 2022 10:27:12.965854883 CEST	49761	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:12.966177940 CEST	49761	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:12.966311932 CEST	49761	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:12.966557026 CEST	443	49761	162.159.129.233	192.168.11.20
May 11, 2022 10:27:13.138885975 CEST	443	49761	162.159.129.233	192.168.11.20
May 11, 2022 10:27:13.139060974 CEST	49761	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:13.139090061 CEST	443	49761	162.159.129.233	192.168.11.20
May 11, 2022 10:27:13.139266014 CEST	49761	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:13.139350891 CEST	49761	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:13.139537096 CEST	443	49761	162.159.129.233	192.168.11.20
May 11, 2022 10:27:13.139574051 CEST	443	49761	162.159.129.233	192.168.11.20
May 11, 2022 10:27:13.139782906 CEST	49761	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:13.139801979 CEST	49761	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:13.258728027 CEST	49762	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:13.258807898 CEST	443	49762	162.159.129.233	192.168.11.20
May 11, 2022 10:27:13.259001017 CEST	49762	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:13.259418964 CEST	49762	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:13.259471893 CEST	443	49762	162.159.129.233	192.168.11.20
May 11, 2022 10:27:13.283235073 CEST	443	49762	162.159.129.233	192.168.11.20
May 11, 2022 10:27:13.283427954 CEST	49762	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:13.283845901 CEST	49762	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:13.283991098 CEST	49762	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:13.284178972 CEST	443	49762	162.159.129.233	192.168.11.20
May 11, 2022 10:27:13.457360029 CEST	443	49762	162.159.129.233	192.168.11.20
May 11, 2022 10:27:13.457551956 CEST	443	49762	162.159.129.233	192.168.11.20
May 11, 2022 10:27:13.457587957 CEST	49762	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:13.457706928 CEST	49762	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:13.457906008 CEST	49762	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:13.457946062 CEST	443	49762	162.159.129.233	192.168.11.20
May 11, 2022 10:27:13.587097883 CEST	49763	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:13.587212086 CEST	443	49763	162.159.129.233	192.168.11.20
May 11, 2022 10:27:13.587424040 CEST	49763	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:13.587825060 CEST	49763	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:13.587893963 CEST	443	49763	162.159.129.233	192.168.11.20
May 11, 2022 10:27:13.611557007 CEST	443	49763	162.159.129.233	192.168.11.20
May 11, 2022 10:27:13.611768007 CEST	49763	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:13.613440037 CEST	49763	443	192.168.11.20	162.159.129.233

Timestamp	Source Port	Dest Port	Source IP	Dest IP
May 11, 2022 10:27:13.614147902 CEST	49763	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:13.614281893 CEST	443	49763	162.159.129.233	192.168.11.20
May 11, 2022 10:27:13.792226076 CEST	443	49763	162.159.129.233	192.168.11.20
May 11, 2022 10:27:13.792412996 CEST	443	49763	162.159.129.233	192.168.11.20
May 11, 2022 10:27:13.792467117 CEST	49763	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:13.792570114 CEST	49763	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:13.792824030 CEST	49763	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:13.792876005 CEST	443	49763	162.159.129.233	192.168.11.20
May 11, 2022 10:27:13.916237116 CEST	49764	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:13.916349888 CEST	443	49764	162.159.129.233	192.168.11.20
May 11, 2022 10:27:13.916575909 CEST	49764	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:13.916840076 CEST	49764	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:13.916887999 CEST	443	49764	162.159.129.233	192.168.11.20
May 11, 2022 10:27:13.940315962 CEST	443	49764	162.159.129.233	192.168.11.20
May 11, 2022 10:27:13.940498114 CEST	49764	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:13.940912962 CEST	49764	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:13.941097975 CEST	49764	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:13.941289902 CEST	443	49764	162.159.129.233	192.168.11.20
May 11, 2022 10:27:14.103734016 CEST	443	49764	162.159.129.233	192.168.11.20
May 11, 2022 10:27:14.103991032 CEST	49764	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:14.104003906 CEST	443	49764	162.159.129.233	192.168.11.20
May 11, 2022 10:27:14.104191065 CEST	49764	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:14.104257107 CEST	49764	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:14.104327917 CEST	443	49764	162.159.129.233	192.168.11.20
May 11, 2022 10:27:14.227530956 CEST	49765	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:14.227643013 CEST	443	49765	162.159.129.233	192.168.11.20
May 11, 2022 10:27:14.227904081 CEST	49765	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:14.228355885 CEST	49765	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:14.228410006 CEST	443	49765	162.159.129.233	192.168.11.20
May 11, 2022 10:27:14.253670931 CEST	443	49765	162.159.129.233	192.168.11.20
May 11, 2022 10:27:14.253936052 CEST	49765	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:14.254295111 CEST	49765	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:14.254498959 CEST	49765	443	192.168.11.20	162.159.129.233
May 11, 2022 10:27:14.254690886 CEST	443	49765	162.159.129.233	192.168.11.20
May 11, 2022 10:27:14.418869972 CEST	443	49765	162.159.129.233	192.168.11.20
May 11, 2022 10:27:14.419044018 CEST	49765	443	192.168.11.20	162.159.129.233

DNS Queries

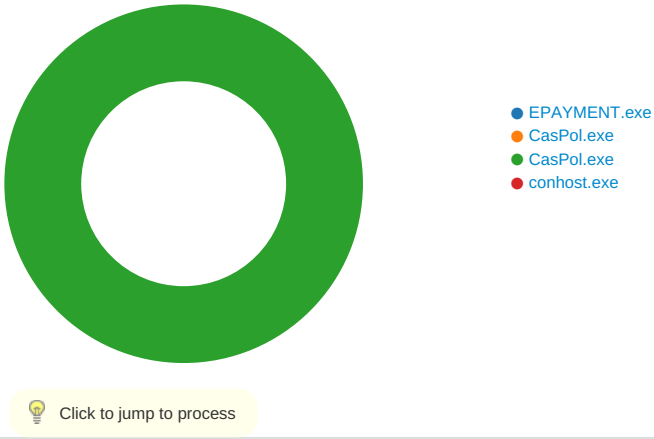
Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
May 11, 2022 10:27:12.080164909 CEST	192.168.11.20	1.1.1.1	0x477c	Standard query (0)	cdn.discordapp.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
May 11, 2022 10:27:12.090205908 CEST	1.1.1.1	192.168.11.20	0x477c	No error (0)	cdn.discordapp.com		162.159.129.233	A (IP address)	IN (0x0001)
May 11, 2022 10:27:12.090205908 CEST	1.1.1.1	192.168.11.20	0x477c	No error (0)	cdn.discordapp.com		162.159.130.233	A (IP address)	IN (0x0001)
May 11, 2022 10:27:12.090205908 CEST	1.1.1.1	192.168.11.20	0x477c	No error (0)	cdn.discordapp.com		162.159.133.233	A (IP address)	IN (0x0001)
May 11, 2022 10:27:12.090205908 CEST	1.1.1.1	192.168.11.20	0x477c	No error (0)	cdn.discordapp.com		162.159.134.233	A (IP address)	IN (0x0001)
May 11, 2022 10:27:12.090205908 CEST	1.1.1.1	192.168.11.20	0x477c	No error (0)	cdn.discordapp.com		162.159.135.233	A (IP address)	IN (0x0001)

Statistics

Behavior



System Behavior

Analysis Process: EPAYMENT.exe PID: **1976**, Parent PID: **4864**

General

Target ID:	2
Start time:	10:26:46
Start date:	11/05/2022
Path:	C:\Users\user\Desktop\EPAYMENT.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\EPAYMENT.exe"
Imagebase:	0x400000
File size:	384544 bytes
MD5 hash:	9811D64E29EF53E107F9379526CFD338
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 00000002.00000002.226641346384.0000000003278000.00000040.00000800.00020000.00000000.sdmp, Author: Joe Security
Reputation:	low

File Activities

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

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

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

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: CasPol.exe PID: **2376**, Parent PID: **1976**

General	
Target ID:	9
Start time:	10:27:01
Start date:	11/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
Wow64 process (32bit):	false
Commandline:	"C:\Users\user\Desktop\EPAYMENT.exe"
Imagebase:	0x610000
File size:	106496 bytes
MD5 hash:	7BAE06CBE364BB42B8C34FCFB90E3EBD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

Analysis Process: CasPol.exe PID: **6908**, Parent PID: **1976**

General	
Target ID:	10
Start time:	10:27:01
Start date:	11/05/2022
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\CasPol.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\EPAYMENT.exe"
Imagebase:	0xbb0000
File size:	106496 bytes
MD5 hash:	7BAE06CBE364BB42B8C34FCFB90E3EBD
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000000A.00000002.230879622484.0000000000F90000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security • Rule: JoeSecurity_GuLoader_2, Description: Yara detected GuLoader, Source: 0000000A.00000000.225982150371.0000000000F90000.00000040.00000400.00020000.00000000.sdmp, Author: Joe Security
Reputation:	moderate

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	FA1EEE	InternetOpenUrlA
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	FA1EEE	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCache	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	FA1EEE	InternetOpenUrlA
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	FA1EEE	InternetOpenUrlA

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	FA1EEE	InternetOpenUrlA
C:\Users\user\AppData\Local\Microsoft\Windows\INetCookies	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	FA1EEE	InternetOpenUrlA
C:\Users\user\AppData\Local\Temp\a1.exe	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	FA1EEE	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\a1.exe	0	223	3c 3f 78 6d 6c 20 76 65 72 73 69 6f 6e 3d 27 31 2e 30 27 20 65 6e 63 6f 64 69 6e 67 3d 27 55 54 46 2d 38 27 3f 3e 3c 45 72 72 6f 72 3e 3c 43 6f 64 65 3e 41 63 63 65 73 73 44 65 6e 69 65 64 3c 2f 43 6f 64 65 3e 3c 4d 65 73 73 61 67 65 3e 41 63 63 65 73 73 20 64 65 6e 69 65 64 2e 3c 2f 4d 65 73 73 61 67 65 3e 3c 44 65 74 61 69 6c 73 3e 41 6e 6f 6e 79 6d 6f 75 73 20 63 61 6c 6c 65 72 20 64 6f 65 73 20 6e 6f 74 20 68 61 76 65 20 73 74 6f 72 61 67 65 2e 6f 62 6a 65 63 74 73 2e 67 65 74 20 61 63 63 65 73 73 20 74 6f 20 74 68 65 20 47 6f 6f 67 6c 65 20 43 6c 6f 75 64 20 53 74 6f 72 61 67 65 20 6f 62 6a 65 63 74 2e 3c 2f 44 65 74 61 69 6c 73 3e 3c 2f 45 72 72 6f 72 3e	<?xml version='1.0' encoding='UTF-8'?> <Error> <Code>AccessDenied</Code> <Message>Access denied.</Message> <Details>Anonymous caller does not have storage.objects.get access to the Google Cloud Storage object. </Details></Error>	success or wait	1	F957CA	WriteFile

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Analysis Process: conhost.exe PID: **7164**, Parent PID: **6908**

General

Target ID:	11
Start time:	10:27:01
Start date:	11/05/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff75fc90000
File size:	875008 bytes
MD5 hash:	81CA40085FC75BABD2C91D18AA9FFA68
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

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

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Disassembly

No disassembly