ID: 715163
Sample Name:
watermarkedMagistrates.cmd
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 17:37:10
Date: 03/10/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Copyright Joe Security LLC 2022

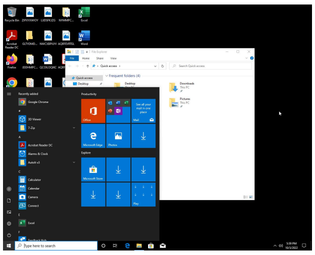
Windows Analysis Report

watermarkedMagistrates.cmd

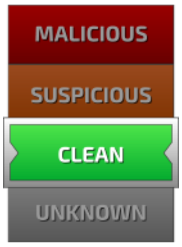
Overview

General Information

Sample Name:	watermarkedMagistrates.cmd
Analysis ID:	715163
MD5:	500e9b6f69d6c7..
SHA1:	285c236c26d1ad..
SHA256:	c6b2b705be1790..
Infos:	



Detection

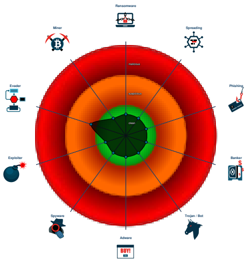


Score:	1
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Sample execution stops while proce…
- Program does not show much activi…

Classification



Process Tree

- **System is w10x64_ra**
- cmd.exe (PID: 4920 cmdline: C:\Windows\system32\cmd.exe /c ""C:\Users\user\Desktop\watermarkedMagistrates.cmd" " MD5: 9D59442313565C2E0860B88BF32B2277)
  - conhost.exe (PID: 5584 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: C5E9B1D1103EDCEA2E408E9497A5A88F)
- **cleanup**

Malware Configuration

No configs have been found

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

No Snort rule has matched

Copyright Joe Security LLC 2022

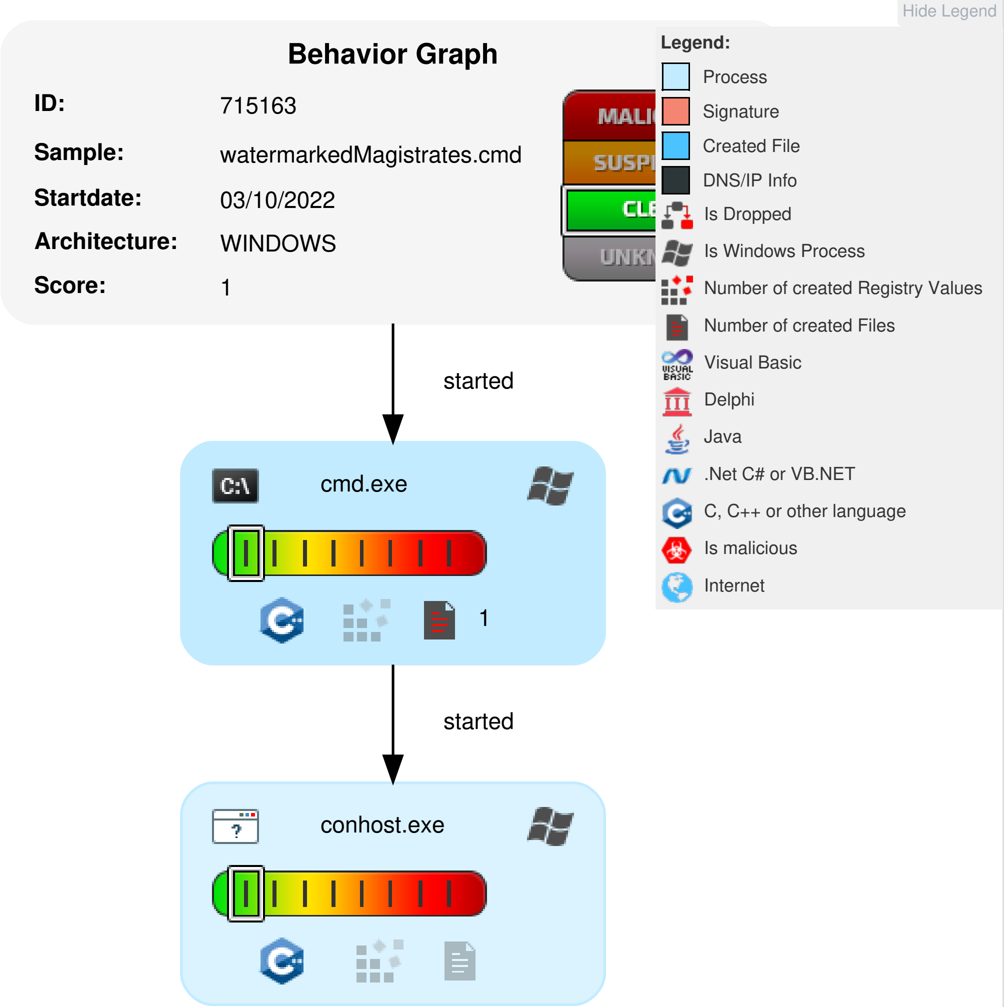
Joe Sandbox Signatures

There are no malicious signatures, click here to show all signatures.

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	Windows Management Instrumentation	Path Interception	1 Process Injection	1 Process Injection	OS Credential Dumping	System Service Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	Data Obfuscation	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition

Behavior Graph

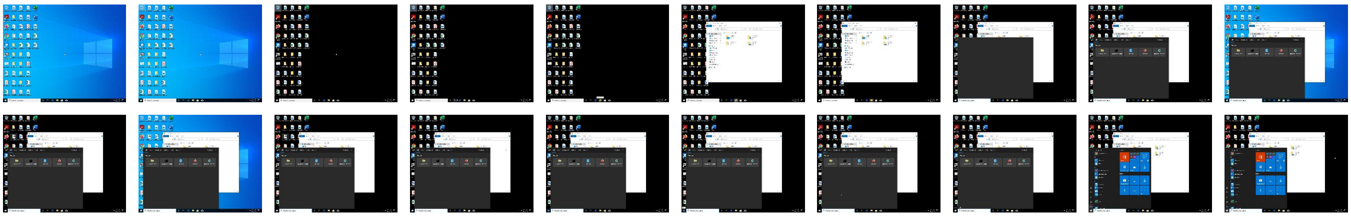


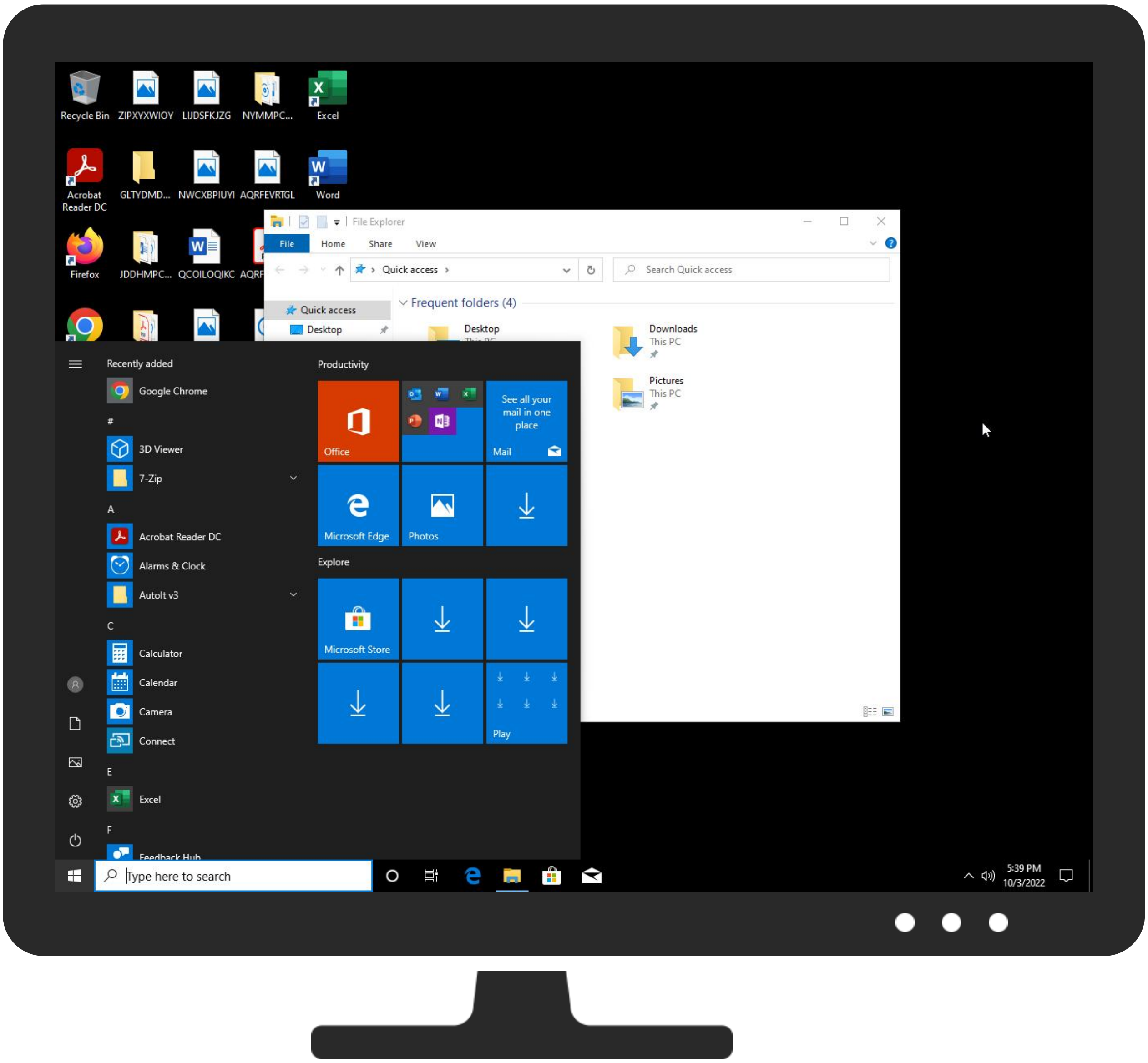
ID:	715163
Sample:	watermarkedMagistrates.cmd
Startdate:	03/10/2022
Architecture:	WINDOWS
Score:	1

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
watermarkedMagistrates.cmd	0%	ReversingLabs		
watermarkedMagistrates.cmd	0%	Virustotal		Browse

Dropped Files

⊘ **No Antivirus matches**

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	715163
Start date and time:	2022-10-03 17:37:10 +02:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 3m 39s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	watermarkedMagistrates.cmd
Cookbook file name:	defaultwindowsinteractivecookbook.jbs
Analysis system description:	Windows 10 64 bit version 1909 (MS Office 2019, IE 11, Chrome 104, Firefox 88, Adobe Reader DC 21, Java 8 u291, 7-Zip)
Number of analysed new started processes analysed:	23
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:	CLEAN
Classification:	clean1.winCMD@2/0@0/0
EGA Information:	Failed
HDC Information:	Failed
HCA Information:	• Successful, ratio: 100% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Found application associated with file extension: .cmd

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, RuntimeBroker.exe, SIHClient.exe, SgrmBroker.exe, backgroundTaskHost.exe, usocoreworker.exe, svchost.exe
- Excluded domains from analysis (whitelisted): www.bing.com, fs.microsoft.com, login.live.com, slscr.update.microsoft.com, ctldl.windowsupdate.com

- Not all processes where analyzed, report is missing behavior information

Simulations

Behavior and APIs

⊘ **No simulations**

Joe Sandbox View / Context

IPs

⊘ **No context**

Domains

⊘ **No context**

ASNs

⊘ **No context**

JA3 Fingerprints

⊘ **No context**

Dropped Files

⊘ **No context**

Created / dropped Files

⊘ **No created / dropped files found**

Static File Info

General

File type:	DOS batch file, ASCII text, with CRLF line terminators
Entropy (8bit):	4.792320101413539
TrID:	
File name:	watermarkedMagistrates.cmd
File size:	157
MD5:	500e9b6f69d6c73c8d230e5a5aaecb9f
SHA1:	285c236c26d1adfb7a7a38b22fa9777a7b963e87
SHA256:	c6b2b705be17902eb4cb8c5f1c587e74e2206e2d6f67a4b6b90b0e24d0395f5a
SHA512:	59ccb06476dd6d737534289479ad587cee75449a86e738c55789a7db7d709ebe9a5f39b75abfa48e0a1cd2ed6f5f3aca25dbe427c7ec6ebc6e33f2db4d791aea
SSDEEP:	3:mKDD4YlsVERKC1VwLYWbH2MUcFwmtU3dzWo0XAGMVERKC1VwLAAQYNsPGEFBHyo6:hcYlseKC1Vw3qoCmmtyAGMeKC1Vw5QLm
TLSH:	EAC08C0B58EB0977A44A3421087901C660AB09708403E80FFA5931EA44B693C838AD1B
File Content Preview:	@echo off.....set anticipatingPerception=sv...set overnightHusky=.....:: quillwortImmunizes...reg%anticipatingPerception%%1 gaffes\chronological.db....exit..

File Icon

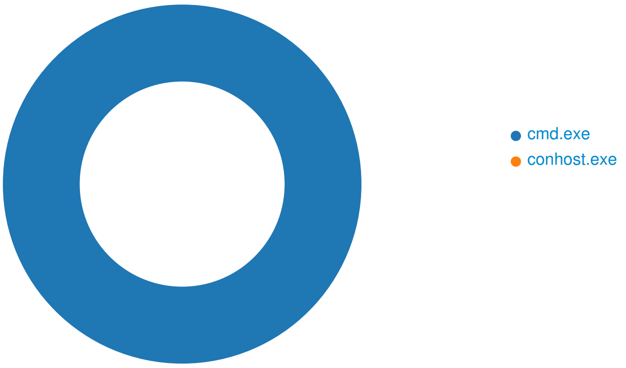
Icon Hash:	988686829e9ae600

Network Behavior

No network behavior found

Statistics

Behavior



Click to jump to process

System Behavior

Analysis Process: cmd.exe PID: **4920**, Parent PID: **3800**

General

Target ID:	0
Start time:	17:37:35
Start date:	03/10/2022
Path:	C:\Windows\System32\cmd.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\cmd.exe /c ""C:\Users\user\Desktop\watermarkedMagistrates.cmd" "
Imagebase:	0x7ff758c90000
File size:	280064 bytes
MD5 hash:	9D59442313565C2E0860B88BF32B2277
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities

Analysis Process: conhost.exe PID: **5584**, Parent PID: **4920**

General

Copyright Joe Security LLC 2022

Target ID:	1
Start time:	17:37:35
Start date:	03/10/2022
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff74e0f0000
File size:	885760 bytes
MD5 hash:	C5E9B1D1103EDCEA2E408E9497A5A88F
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**