



ID: 736959
Sample Name:
Chrom#U0435.U#U0440dat#U0435.zip
Cookbook:
defaultwindowsinteractivecookbook.jbs
Time: 12:34:09
Date: 03/11/2022
Version: 36.0.0 Rainbow Opal

Table of Contents

Table of Contents 2
Windows Analysis Report Chrom#U0435.U#U0440dat#U0435.zip 3
Overview 3
General Information 3
Detection 3
Signatures 3
Classification 3
Process Tree 3
Yara Signatures 3
Sigma Signatures 3
Snort Signatures 3
Joe Sandbox Signatures 4
Networking 4
HIPS / PFW / Operating System Protection Evasion 4
Mitre Att&ck Matrix 4
Screenshots 4
Thumbnails 4
Antivirus, Machine Learning and Genetic Malware Detection 5
Initial Sample 5
Dropped Files 5
Unpacked PE Files 5
Domains 5
URLs 5
Domains and IPs 6
Contacted Domains 6
World Map of Contacted IPs 6
Public IPs 6
General Information 6
Warnings 7
Created / dropped Files 7
Static File Info 7
General 7
File Icon 7

Copyright Joe Security LLC 2022

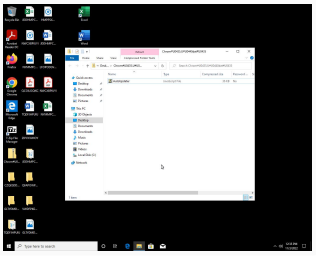
Windows Analysis Report

Chrom#U0435.U#U0440dat#U0435.zip

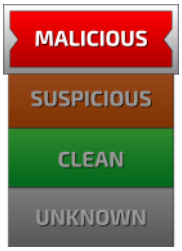
Overview

General Information

Sample Name:	Chrom#U0435.U#U0440dat#U0435.zip
Analysis ID:	736959
MD5:	c4971c73424f27…
SHA1:	00636308cac7b4..
SHA256:	26106b07597873.



Detection

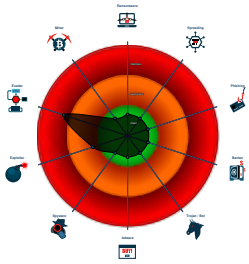


Score:	56
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- System process connects to networ…
- Snort IDS alert for network traffic
- Program does not show much activi…
- Found WSH timer for Javascript or V…

Classification



Process Tree

- **System is w10x64_ra**
- wscript.exe (PID: 888 cmdline: "C:\Windows\System32\WScript.exe" "C:\Users\alfredo\AppData\Local\Temp\Temp1_Chrom#U0435.U#U0440dat#U0435.zip\AutoUpdater.js" MD5: 563EDAE37876138FDFF47F3E7A9A78FD)
- wscript.exe (PID: 6516 cmdline: "C:\Windows\System32\WScript.exe" "C:\Users\alfredo\AppData\Local\Temp\Temp1_Chrom#U0435.U#U0440dat#U0435.zip\AutoUpdater.js" MD5: 563EDAE37876138FDFF47F3E7A9A78FD)
- **cleanup**

Yara Signatures

No yara matches

Sigma Signatures

No Sigma rule has matched

Snort Signatures

ET TROJAN SocGholish CnC Domain in DNS Lookup (portraits .studio-94-photography .com) - Source IP: 192.168.2.3 - Destination IP: 1.1.1.1

Timestamp:	192.168.2.31.1.1.153158532039597 11/03/22-12:35:25.057076
SID:	2039597
Source Port:	53158
Destination Port:	53
Protocol:	UDP

Copyright Joe Security LLC 2022

Classtype:	A Network Trojan was detected

ET TROJAN SocGholish CnC Domain in DNS Lookup (portraits .studio-94-photography .com) - Source IP: 192.168.2.3 - Destination IP: 1.1.1.1	
Timestamp:	192.168.2.31.1.1.156466532039597 11/03/22-12:35:01.413784
SID:	2039597
Source Port:	56466
Destination Port:	53
Protocol:	UDP
Classtype:	A Network Trojan was detected

Joe Sandbox Signatures

Networking



System process connects to network (likely due to code injection or exploit)

Snort IDS alert for network traffic

HIPS / PFW / Operating System Protection Evasion



System process connects to network (likely due to code injection or exploit)

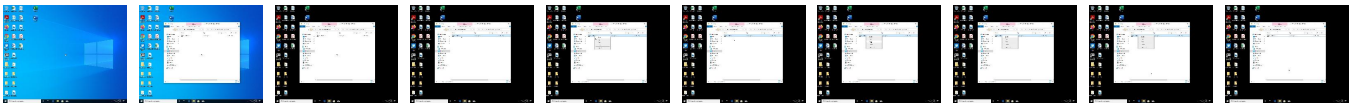
Mitre Att&ck Matrix

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 Scripting	Path Interception	1 1 Process Injection	1 1 Process Injection	OS Credential Dumping	2 System Information Discovery	Remote Services	Data from Local System	Exfiltration Over Other Network Medium	2 Encrypted Channel	Eavesdrop on Insecure Network Communication	Remotely Track Device Without Authorization	Modify System Partition
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Boot or Logon Initialization Scripts	1 Scripting	LSASS Memory	1 Remote System Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	1 Application Layer Protocol	Exploit SS7 to Redirect Phone Calls/SMS	Remotely Wipe Data Without Authorization	Device Lockout

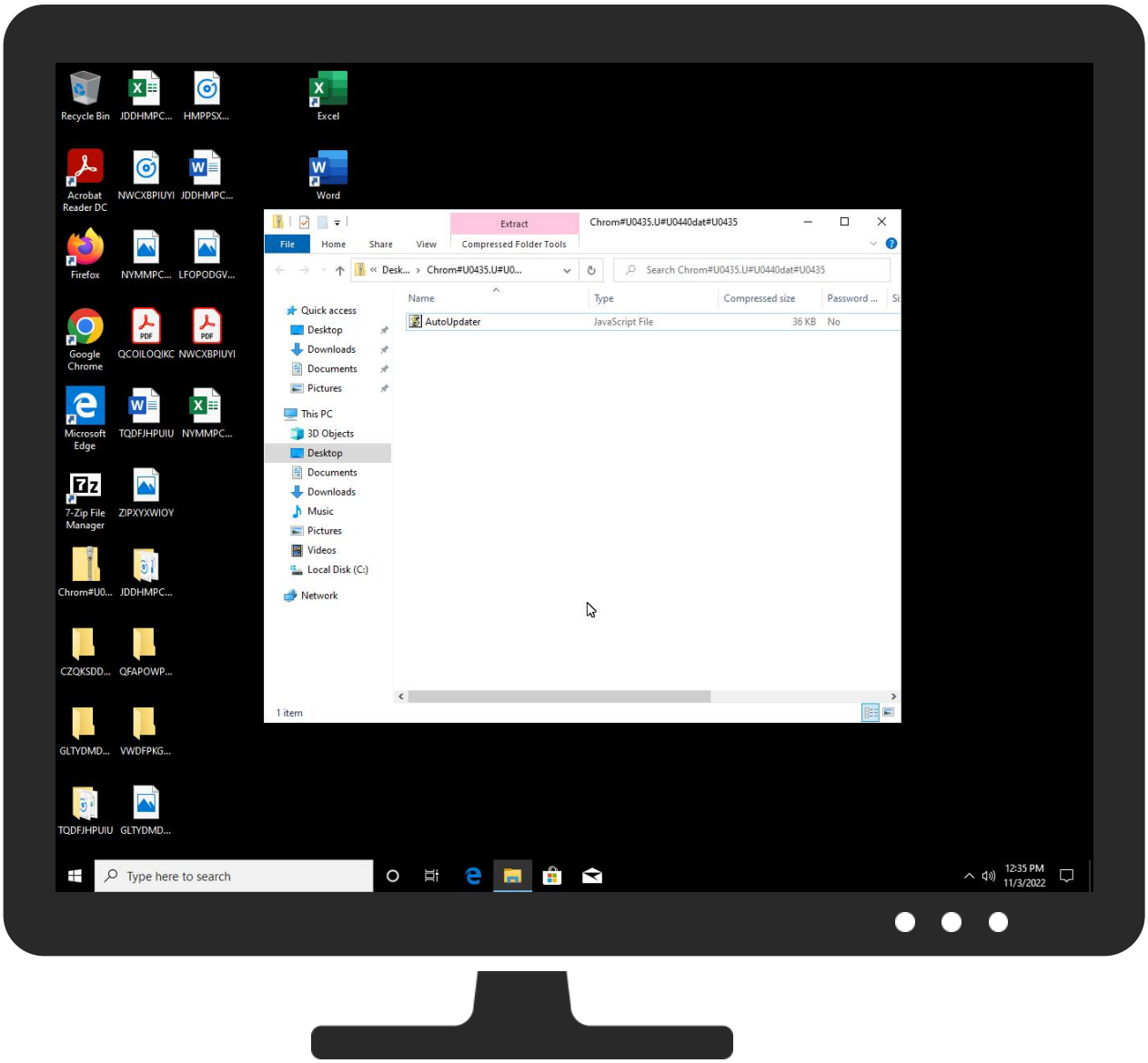
Screenshots

Thumbnails

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



Copyright Joe Security LLC 2022



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

Source	Detection	Scanner	Label	Link
Chrom#U0435.U#U0440dat#U0435.zip	2%	Virustotal		Browse

Dropped Files

No Antivirus matches

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

No Antivirus matches

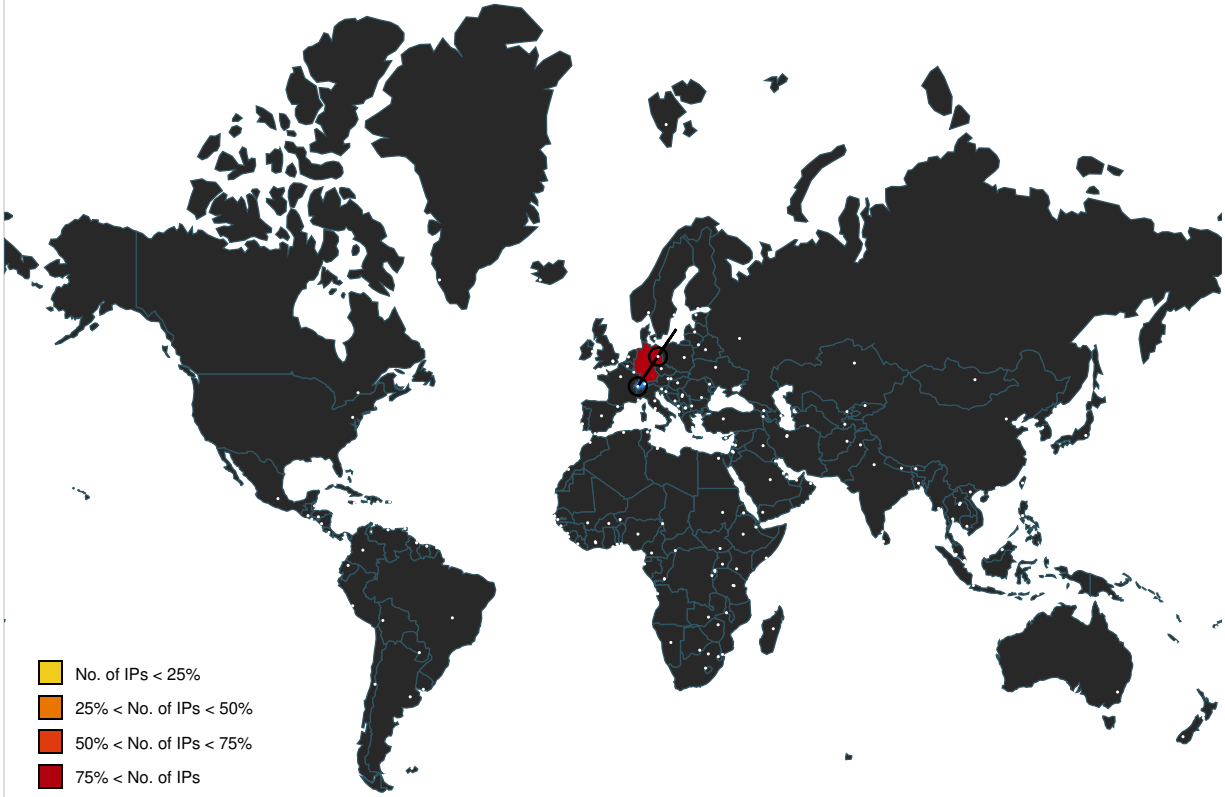
Copyright Joe Security LLC 2022

Domains and IPs

Contacted Domains

No contacted domains info

World Map of Contacted IPs



Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
188.138.69.102	unknown	Germany		8972	GD-EMEA-DC-SXB1DE	true

General Information

Joe Sandbox Version:	36.0.0 Rainbow Opal
Analysis ID:	736959
Start date and time:	2022-11-03 12:34:09 +01:00
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Chrom#U0435.U#U0440dat#U0435.zip
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:	12
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:	• EGA enabled
Analysis Mode:	stream
Analysis stop reason:	Timeout
Detection:	MAL

Copyright Joe Security LLC 2022

Classification:	mal56.evad.winZIP@2/0@0/11
Cookbook Comments:	• Found application associated with file extension: .zip

Warnings

- Exclude process from analysis (whitelisted): dllhost.exe, rundll32.exe, svchost.exe
- Excluded IPs from analysis (whitelisted): 40.126.32.76, 40.126.32.68, 20.190.160.14, 40.126.32.138, 20.190.160.20, 40.126.32.74, 20.190.160.22, 40.126.32.134
- Excluded domains from analysis (whitelisted): fs.microsoft.com, prda.aadg.msidentity.com, login.live.com, login.msa.msidentity.com, www.tm.a.prd.aadg.trafficmanager.net, www.tm.lg.prod.aadmsa.trafficmanager.net
- 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.

Created / dropped Files

No created / dropped files found

Static File Info

General

File type:	Zip archive data, at least v2.0 to extract, compression method=deflate
Entropy (8bit):	7.989712194941986
TrID:	• ZIP compressed archive (8000/1) 100.00%
File name:	Chrom#U0435.U#U0440dat#U0435.zip
File size:	35984
MD5:	c4971c73424f2728ef8771d8dcc5d7bc
SHA1:	00636308cac7b4d8dadd2590042ff1bbeb702e43
SHA256:	26106b07597873612b6cffd05d7f46564db4a2f90964c49906191bf0c8d7b180
SHA512:	c7ee9f54aa268876a41bd80531f73d7ebe64b872045d575e42dd2219fd2a0f8d3d35273ee2eb71aacfa4c25f2e333e764a69c69b8b9b6c9b10f327993aa5b043
SSDEEP:	768:2O4RfJ6aSiQdlwKFiPXG/fv4OnPQKvUprXo4RiixFcSinbIS3LzQS:2FRR6aSnrFiP2/fv4On1soIxWBn87S
TLSH:	47F2F12C494935ACC1E32A3A527947880F96E3635433E0AF972D9D6177EB2E56C83234
File Content Preview:	PK.....%YcU~e.`.....AutoUpdater.js...w.I.0.....I%.[.. ....*$).5."|AB..Z.....kn...d...=...iR....mn....h....7.7...**6._uY.....Ku._U....N.....vr.*U.*g:+....o..I..Q.....sVlo..Og.....s.....d./.....:.....;....+i.6..e:.....8~f..0.

File Icon



Icon Hash:	f4ccccccccccccdc