ID: 433114
Sample Name: Minutes of meeting June 9th.exe
Cookbook: default.jbs
Time: 10:33:15
Date: 11/06/2021
Version: 32.0.0 Black Diamond

Table of Contents

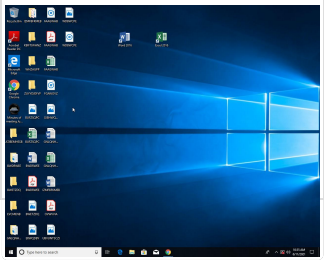
Analysis Report Minutes of meeting June 9th.exe

Overview

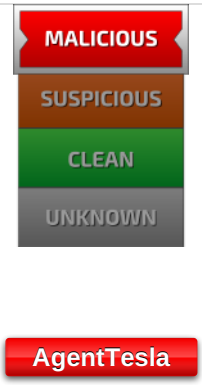
General Information

Sample Name:	Minutes of meeting June 9th.exe
Analysis ID:	433114
MD5:	ee4b5d2d220b8b..
SHA1:	4bfa8d3abf280cc..
SHA256:	31e702dd0fc8ae1.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

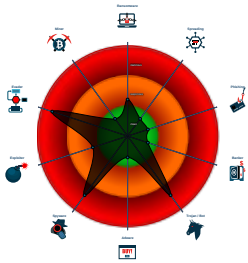


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Yara detected AgentTesla
- Yara detected AgentTesla
- Yara detected AntiVM3
- .NET source code contains very larg…
- Injects a PE file into a foreign proce…
- Queries sensitive BIOS Information …
- Queries sensitive network adapter in…
- Tries to detect sandboxes and other…
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal browser in…
- Tries to harvest and steal ftp login c…

Classification



Process Tree

- **System is w10x64**
- Minutes of meeting June 9th.exe (PID: 7048 cmdline: 'C:\Users\user\Desktop\Minutes of meeting June 9th.exe' MD5: EE4B5D2D220B8B925A84755E5AD9FA06)
  - schtasks.exe (PID: 6484 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\RfuYgTevtBVukb' /XML 'C:\Users\user\AppData\Local\Temp\tmp1C49.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 5816 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Minutes of meeting June 9th.exe (PID: 5832 cmdline: C:\Users\user\Desktop\Minutes of meeting June 9th.exe MD5: EE4B5D2D220B8B925A84755E5AD9FA06)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "SMTP Info": "jaime.navarro@crigab.cljaimecrigabmail.crigab.cl"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000005.00000002.909165017.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000002.909165017.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000001.00000002.671554709.000000000830000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
00000005.00000000.668170941.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000005.00000000.668170941.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
Click to see the 8 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
1.2.Minutes of meeting June 9th.exe.3891e68.1.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
1.2.Minutes of meeting June 9th.exe.3891e68.1.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
5.0.Minutes of meeting June 9th.exe.400000.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
5.0.Minutes of meeting June 9th.exe.400000.1.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
1.2.Minutes of meeting June 9th.exe.3891e68.1.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 3 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

System Summary:

.NET source code contains very large array initializations

Boot Survival:

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

Malware Analysis System Evasion:

Yara detected AntiVM3

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)

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

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 Putty / WinSCP information (sessions, passwords, etc)

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:

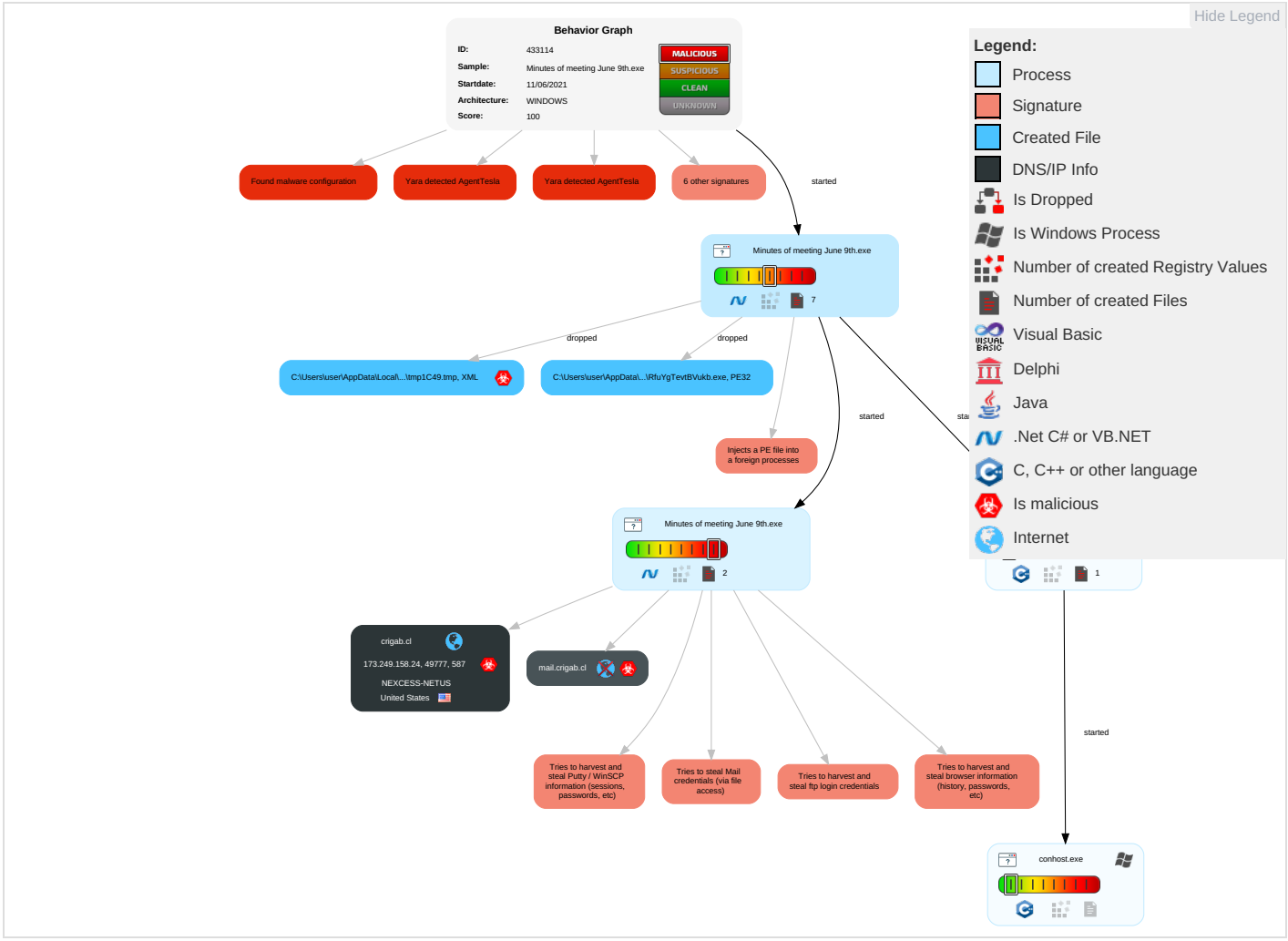
Yara detected AgentTesla

Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Process Injection 1 1 2	Disable or Modify Tools 1	OS Credential Dumping 2	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Deobfuscate/Decode Files or Information 1	Input Capture 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Obfuscated Files or Information 3	Credentials in Registry 1	Query Registry 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 1
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 2	NTDS	Security Software Discovery 2 2 1	Distributed Component Object Model	Input Capture 1	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 4 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 4 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicati
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	Application Layer Protocc

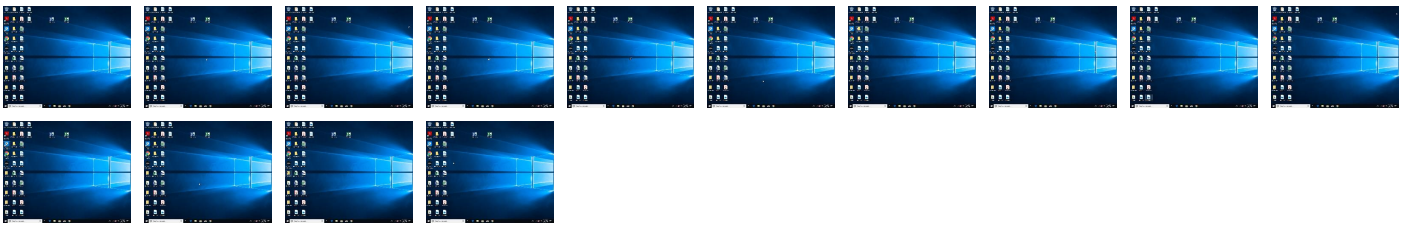
Behavior Graph



Screenshots

Thumbnails

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



Antivirus, Machine Learning and Genetic Malware Detection

Initial Sample

No Antivirus matches

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\RfuYgTevtBVukb.exe	9%	ReversingLabs	ByteCode-MSIL.Trojan.Wacatac	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
5.0.Minutes of meeting June 9th.exe.400000.1.unpack	100%	Avira	TR/Spy.Gen8		Download File
5.2.Minutes of meeting June 9th.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		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	

Source	Detection	Scanner	Label	Link
http://www.fontbureau.comFV	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://wB46twoUXvvh.net	0%	Avira URL Cloud	safe	
http://www.fontbureau.comuef	0%	Avira URL Cloud	safe	
http://www.fontbureau.comgreta2	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnU	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Hb	0%	Avira URL Cloud	safe	
http://www.ascendercorp.com/typedesigners.html=	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/~	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/~	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/~	0%	URL Reputation	safe	
http://www.urwpp.deos	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.fontbureau.comt$	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/2	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/2	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/2	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/-	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/-	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/-	0%	URL Reputation	safe	
http://www.ascendercorp.com/typedesigners.htmlsA	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.fontbureau.comed	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.comoitug	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.urwpp.de	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/V	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.sakkal.com	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://www.fontbureau.comT.TTF~	0%	Avira URL Cloud	safe	
http://www.fontbureau.comlicF	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/W	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/W	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/W	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://HXowME.com	0%	Avira URL Cloud	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/V	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/V	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/V	0%	URL Reputation	safe	
http://www.fontbureau.comico	0%	Avira URL Cloud	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://www.fontbureau.comic	0%	Avira URL Cloud	safe	
http://www.urwpp.deR	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://mail.crigab.cl	0%	Avira URL Cloud	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://www.fontbureau.come.com	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
crigab.cl	173.249.158.24	true	true		unknown
mail.crigab.cl	unknown	unknown	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
173.249.158.24	crigab.cl	United States		36444	NEXCESS-NETUS	true

General Information

Joe Sandbox Version:	32.0.0 Black Diamond
Analysis ID:	433114
Start date:	11.06.2021
Start time:	10:33:15
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 8m 47s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Minutes of meeting June 9th.exe
Cookbook file name:	default.jbs
Analysis system description:	Windows 10 64 bit v1803 with Office Professional Plus 2016, Chrome 85, IE 11, Adobe Reader DC 19, Java 8 Update 211
Number of analysed new started processes analysed:	17
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.evad.winEXE@6/4@2/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.3% (good quality ratio 0.2%) • Quality average: 44.3% • Quality standard deviation: 30.1%
HCA Information:	• Successful, ratio: 91% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
10:34:02	API Interceptor	759x Sleep call for process: Minutes of meeting June 9th.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NEXCESS-NETUS	Miral-Purushotham.verra.htm	Get hash	malicious	Browse	• 173.249.159.98
	BL Draft copy.exe	Get hash	malicious	Browse	• 67.20.61.90
	RFQ Order - Mediform S.A-pdf.exe	Get hash	malicious	Browse	• 209.126.18.3
	http://https://joom.ag/yGUC	Get hash	malicious	Browse	• 67.20.61.14
	http://https://saveunbornlife.org/wp-includes/random_compat/fireweb/login.html#info@americasleading.com	Get hash	malicious	Browse	• 209.87.159.167
	Claim-2020190722-10092020.xls	Get hash	malicious	Browse	• 8.29.130.206
	Claim-2020190722-10092020.xls	Get hash	malicious	Browse	• 8.29.130.206
	http://https://4ac1b1774f.nxcli.net/content/adobe-RD28/index.html	Get hash	malicious	Browse	• 8.29.157.202
	http://https://4ac1b1774f.nxcli.net/content/adobe-RD28/index.html	Get hash	malicious	Browse	• 8.29.157.202
	http://https://u13866594.ct.sendgrid.net/ls/click?upn=zXrfjgsxrhwKJV2JEsds02DTKlA-2FKjP3ouTKap6tb-2BaHzPZGmjljWdY-2B8eIVgUp6FZt5WEBkptcUgYHGhLdiXIOOcl4quBIBQq-2Fl5KivR9ZJcyXiEilPAbFSOTDEzsr8Wg7E9oxBKcFAygB5REMrDA-3D-3DfSmP_JrfdLO9c93xZuhsRHgFhRVDV8bLlln4lYk4aksXNrQT2hmY9LW1-2BwLQhc6eTeTp4EE5NUs8Klx5-2Fha7j5lkjVAbFl1T37-2BhQ2JWSaf7-2FBSF9alW21qJuxs-2B5W9BOyD1t4-2BxoIqaCGgqkyhimaS73eUj7LLB8nO3AAnBWZFTFKyd1HKj5Vs7AylQ6lif5qThylDp9fqArjJYdvxUltYS65reC4G6lXlAEY85yMHqyEg8-3D	Get hash	malicious	Browse	• 173.249.151.38
	http://u8824451.ct.sendgrid.net/ls/click?upn=5fYtplO-2FP4S37YYMUNVFFIYhCASYIhBbksOQ-2FihRkfMagXRLczMdDWyGKLdaZ2fGhDy-2F2d9wvh3PmFD5Sd8YlrIZf9YbBnjsARk2gQWkDh7EtRQeoc6vexcl-2F5xnJda6NJSpa6VgcIL99Z9lzFDK2g-3D-3DJZGb_Zf9noBSXp6zmd8gcAmse0KbOcMdKjdFVksgJt8-2FyUPRtkP4eQAkARHJz9LCsuAXZYmX90WUOo27t0l8tRPd-2BGboZnCD837dyUOzvwZQdq8YyTSBwQz1tmOMo8vOOGjUDn7S-2B-2BvWNHLAYT3doPJ5P9O4MJLNaRyHO39WJVaD-2FaysKv78DQH3AuD-2Br9cP-2Fkv2RSdS4tsTx8jv2duyxUVT2HF-2FSG9MUjWRrKmvZe0PvAPM-3D	Get hash	malicious	Browse	• 209.126.25.245
	Electronic form.doc	Get hash	malicious	Browse	• 173.249.157.230
	Electronic form.doc	Get hash	malicious	Browse	• 173.249.157.230
	Electronic form.doc	Get hash	malicious	Browse	• 173.249.157.230
	http://https://u14688309.ct.sendgrid.net/ls/click?upn=cYiEKVN9lp-2Fx5BNj7S4OzK5I0wmQnNsEyIXHxuR49Y0mFRm5J-2FOvpTZPGVL-2FGaaV1CNEoN1qO2tnUYAsgY7JeZw8g-2FkrIoH7rbEUkNbx58SdDpO0thwug5jJN-2Frup8vaurnMgjuwNweyZIS2CZ3jkA-3D-3DT50W_5fL-2BdZKd8ocMNHc9SFg5eh8Z492W4iYSRnF7u-2BCYs3ycMEdZGjLCvGu2ugUBziXSXaqkh1V-2Fsa99ub68wrh5OdrzEnVOu7TsGbzWwItjPTAUliDykKj-2BrGf-2FnoWP8k64P1CqxPB7O6uti-2BRXKqKaFo62vIKvcgA6010v7qKaYTDacfsNG-2FrdMkVVmeY92oyIYHVAFv40AyUGcaYUyimPMp-2BUSUwNLaX-2B-2FFzXvJQNPfi1wlnZNSvwMO-2FCM-2F5SSLge	Get hash	malicious	Browse	• 209.126.25.245
	http://https://u14688309.ct.sendgrid.net/ls/click?upn=cYiEKVN9lp-2Fx5BNj7S4OzK5I0wmQnNsEyIXHxuR49Y0mFRm5J-2FOvpTZPGVL-2FGaaV1CNEoN1qO2tnUYAsgY7JeZw8g-2FkrIoH7rbEUkNbx58SdDpO0thwug5jJN-2Frup8vaurnMgjuwNweyZIS2CZ3jkA-3D-3DtIcy_5fL-2BdZKd8ocMNHc9SFg5eh8Z492W4iYSRnF7u-2BCYs3ycMEdZGjLCvGu2ugUBziXSXaqkh1V-2Fsa99ub68wrh5OYz6cwOQ7Ot7CgyHJLSBUMG4eMwFRNpKSXwViJxXZcm-2Fun8LUg4JO6z5VtX1zs4YB-2Fft6HB6af-2B0DDiujru0fMifBRcnU9Fi-2FbYW8hlsgmAQC6pODhn8vANdinP-2FA-2FtozTt92M3JpYIKg6Jj-2BLa7t1zJrg6EOnVP-2FGO59JpMZSlp	Get hash	malicious	Browse	• 209.126.25.245
	QW8524983075IS.doc	Get hash	malicious	Browse	• 173.249.157.230
	QW8524983075IS.doc	Get hash	malicious	Browse	• 173.249.157.230
	QW8524983075IS.doc	Get hash	malicious	Browse	• 173.249.157.230

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	mZebTSV5Pp.doc	Get hash	malicious	Browse	• 173.249.15 7.230

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\Minutes of meeting June 9th.exe.log	
Process:	C:\Users\user\Desktop\Minutes of meeting June 9th.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1400
Entropy (8bit):	5.344635889251176
Encrypted:	false
SSDEEP:	24:MLU84jE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4sAmEg:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHV
MD5:	394E646B019FF472CE37EE76A647A27F
SHA1:	BD5872D88EE9CD2299B5F0E462C53D9E7040D6DA
SHA-256:	2295A0B1F6ACD75FB5D038ADE65725EDF3DDF076107AEA93E4A864E35974AE2A
SHA-512:	7E95510C85262998AECC9A06A73A5BF6352304AF6EE143EC7E48A17473773F33A96A2F4146446444789B8BCC9B83372A227DC89C3D326A2E142BCA1E1A9B4809
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmp1C49.tmp	
Process:	C:\Users\user\Desktop\Minutes of meeting June 9th.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1647
Entropy (8bit):	5.184913133325714
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGQ9tn:cbhK79lNQR/rydbz9l3YODOLNdq31
MD5:	51A0296D50D19C44A767FB7256285438
SHA1:	F5D712FADFAF2975F12F55E357FDBF9DB6CC3772
SHA-256:	1E8EED0B81F03036E346C7C79FCBE10E68D152162903F4282BB12841F64399AA
SHA-512:	E1AFA3981131BB90DD0CC03808DBD1FC7E891D99DAA8EC8719669599A0B84B95F0B2F4C1AEE733F759A9616D2894579543DD40939D446C0F765D65475E6CBC7
Malicious:	**true**
Reputation:	low
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>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\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

C:\Users\user\AppData\Roaming\RfuYgTevtBVukb.exe	
Process:	C:\Users\user\Desktop\Minutes of meeting June 9th.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1552896
Entropy (8bit):	7.307230517877139
Encrypted:	false
SSDEEP:	24576:5ONeBUdtwsEgwsoe/z8YEoqSg5LlJfH6zMIDsxTt8nUhqF+39k6aq0+imRlyY/r:EwBUwsEgwsoe5U/BldO/jFyHaq0lyIye

C:\Users\user\AppData\Roaming\RfuYgTevtBVukb.exe	
MD5:	EE4B5D2D220B8B925A84755E5AD9FA06
SHA1:	4BFA8D3ABF280CCA85905CE083FE4446AC1D4862
SHA-256:	31E702DD0FC8AE15E8CA4991263C135709A1D64CDA293A4896F89ED3B3699B77
SHA-512:	101B8FEC687AAA86F558188832C3A0C77264EDE18A962772E68C678C24D6FFBEA135188B53D291641A472A27E4241A152180960B45428435CA359E20AD214F2A
Malicious:	false
Antivirus:	• Antivirus: ReversingLabs, Detection: 9%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P..*.....I... ...`....@.. ....@.....H..O....`.....G..... ..... ..H.....text...4)... ...*..... ..`.rsrc.....`.....,.....@..@.rel oc.....@..B.....I.....H.....D.....0.....(....(.....(.....o.....*.....(.....(!.....("......(#.....($....*N..(....o....(% ....*&..(&....*.s'.....s(.....s).....s*.....s+.....*....0.....~....o,....+..*.0.....~....o-....+..*.0.....~....o.....+..*.0.....~....o/....+..*.0.....~....o0....+..*&..(1....*...0..<... .....~.....(2.....,lr...p.....(3...o4...s5.....~.....

C:\Users\user\AppData\Roaming\RfuYgTevtBVukb.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Minutes of meeting June 9th.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	false
Reputation:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.307230517877139
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	Minutes of meeting June 9th.exe
File size:	1552896
MD5:	ee4b5d2d220b8b925a84755e5ad9fa06
SHA1:	4bfa8d3abf280cca85905ce083fe4446ac1d4862
SHA256:	31e702dd0fc8ae15e8ca4991263c135709a1d64cda293a4896f89ed3b3699b77
SHA512:	101b8fec687aaa86f558188832c3a0c77264ede18a962772e68c678c24d6ffbea135188b53d291641a472a27e4241a152180960b45428435ca359e20ad214f2a
SSDEEP:	24576:5ONeBUdtwsEgwsoe/z8YEoqSg5LlJfH6zMIDsxTt8nUhqF+39k6aq0+imRlyY/r:EwBUwsEgwsoe5U/BldO/jFyHaq0lyIye
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P..*.....I... ...`....@.. .... @.....

File Icon

Icon Hash:	e0c6a169f4bed870

Static PE Info

General

Entrypoint:	0x55492e
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x60C3140B [Fri Jun 11 07:43:07 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
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:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x152934	0x152a00	False	0.699034901024	data	7.39720072133	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x156000	0x2838c	0x28400	False	0.599845933618	data	6.35335609293	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x180000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Jun 11, 2021 10:35:52.829802990 CEST	192.168.2.4	8.8.8.8	0x4e11	Standard query (0)	mail.crigab.cl	A (IP address)	IN (0x0001)
Jun 11, 2021 10:35:53.043632030 CEST	192.168.2.4	8.8.8.8	0x3c1f	Standard query (0)	mail.crigab.cl	A (IP address)	IN (0x0001)

DNS Answers

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Jun 11, 2021 10:35:53.027034044 CEST	8.8.8.8	192.168.2.4	0x4e11	No error (0)	mail.crigab.cl	crigab.cl		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 10:35:53.027034044 CEST	8.8.8.8	192.168.2.4	0x4e11	No error (0)	crigab.cl		173.249.158.24	A (IP address)	IN (0x0001)
Jun 11, 2021 10:35:53.216770887 CEST	8.8.8.8	192.168.2.4	0x3c1f	No error (0)	mail.crigab.cl	crigab.cl		CNAME (Canonical name)	IN (0x0001)
Jun 11, 2021 10:35:53.216770887 CEST	8.8.8.8	192.168.2.4	0x3c1f	No error (0)	crigab.cl		173.249.158.24	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Jun 11, 2021 10:35:53.879920959 CEST	587	49777	173.249.158.24	192.168.2.4	220-ww1.hechile.com ESMTP Exim 4.94.2 #2 Fri, 11 Jun 2021 04:35:53 -0400 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Jun 11, 2021 10:35:53.880697012 CEST	49777	587	192.168.2.4	173.249.158.24	EHLO 494126
Jun 11, 2021 10:35:54.419498920 CEST	587	49777	173.249.158.24	192.168.2.4	250-ww1.hechile.com Hello 494126 [84.17.52.18] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-STARTTLS 250 HELP
Jun 11, 2021 10:35:54.420450926 CEST	49777	587	192.168.2.4	173.249.158.24	MAIL FROM:<jaime.navarro@crigab.cl>
Jun 11, 2021 10:35:54.575196028 CEST	587	49777	173.249.158.24	192.168.2.4	550 Access denied - Invalid HELO name (See RFC2821 4.1.1.1)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Minutes of meeting June 9th.exe PID: 7048 Parent PID: 5988

General

Start time:	10:34:00
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\Minutes of meeting June 9th.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Minutes of meeting June 9th.exe'
Imagebase:	0x250000
File size:	1552896 bytes
MD5 hash:	EE4B5D2D220B8B925A84755E5AD9FA06
Has elevated privileges:	true
Has administrator privileges:	true

Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.671554709.0000000002830000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000001.00000002.671900306.00000000037E1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000001.00000002.671900306.00000000037E1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 6484 Parent PID: 7048

General

Start time:	10:34:10
Start date:	11/06/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\RfuYgTevtBVukb' /XML 'C:\Users\user\AppData\Local\Temp\tmp1C49.tmp'
Imagebase:	0x2d0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
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: conhost.exe PID: 5816 Parent PID: 6484

General

Start time:	10:34:10
Start date:	11/06/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff724c50000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: Minutes of meeting June 9th.exe PID: 5832 Parent PID: 7048

General

Start time:	10:34:11
Start date:	11/06/2021
Path:	C:\Users\user\Desktop\Minutes of meeting June 9th.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Minutes of meeting June 9th.exe
Imagebase:	0x960000
File size:	1552896 bytes
MD5 hash:	EE4B5D2D220B8B925A84755E5AD9FA06
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: 00000005.00000002.909165017.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000002.909165017.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000000.668170941.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000005.00000000.668170941.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000005.00000002.910886849.00000000030B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000005.00000002.910886849.00000000030B1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Read

Disassembly

Code Analysis