ID: 483815
Sample Name:
#PO#PLATINIUMPLATEEQUIPMENT9968686.exe
Cookbook: default.jbs
Time: 14:23:21
Date: 15/09/2021
Version: 33.0.0 White Diamond

Table of Contents

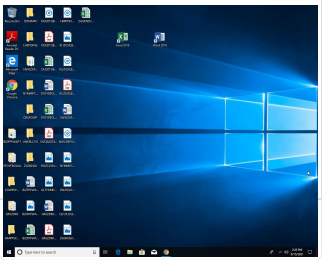
Windows Analysis Report #PO#PLATINIUMPLATEEQUIP…

Overview

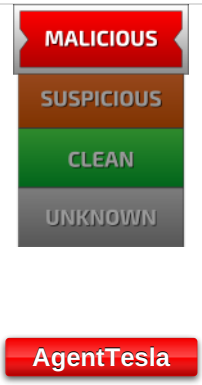
General Information

Sample Name:	#PO#PLATINIUMPLATEEQUIPMENT9968686.exe
Analysis ID:	483815
MD5:	d5ce2c4e604d99..
SHA1:	b6f6bff3e715b6d…
SHA256:	21d1d5c0e8c4cfa..
Tags:	agenttesla exe
Infos:	

Most interesting Screenshot:



Detection



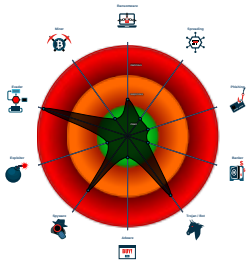
AgentTesla

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

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e.…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Multi AV Scanner detection for dropp…
- Initial sample is a PE file and has a …
- Tries to detect sandboxes and other…
- .NET source code contains potentia…
- Injects a PE file into a foreign proce…
- Queries sensitive video device inform…
- Sigma detected: Powershell Defende…

Classification



Process Tree

- **System is w10x64**
- #PO#PLATINIUMPLATEEQUIPMENT9968686.exe (PID: 4856 cmdline: 'C:\Users\user\Desktop\#PO#PLATINIUMPLATEEQUIPMENT9968686.exe' MD5: D5CE2C4E604D99887C87BBA2C03244FD)
  - powershell.exe (PID: 1092 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\#PO#PLATINIUMPLATEEQUIPMENT9968686.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6080 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 2780 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\cOtSKC' /XML 'C:\Users\user\AppData\Local\Temp\tmpB3A5.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 1276 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - #PO#PLATINIUMPLATEEQUIPMENT9968686.exe (PID: 1064 cmdline: C:\Users\user\Desktop\#PO#PLATINIUMPLATEEQUIPMENT9968686.exe MD5: D5CE2C4E604D99887C87BBA2C03244FD)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "echezona@bonfigliolli.com",
  "Password": "^vccXHY6",
  "Host": "smtp.bonfigliolli.com"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000B.00000002.502821504.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0000000B.00000002.502821504.000000000402000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
00000000.00000002.277208501.0000000003CEC000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000000.00000002.277208501.0000000003CEC000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000000.00000002.276757595.0000000003A89000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 8 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.#PO#PLATINIUMPLATEEQUIPMENT9968686.exe.3b4cd78.2.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.#PO#PLATINIUMPLATEEQUIPMENT9968686.exe.3b4cd78.2.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
11.2.#PO#PLATINIUMPLATEEQUIPMENT9968686.exe.400000.0.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
11.2.#PO#PLATINIUMPLATEEQUIPMENT9968686.exe.400000.0.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.#PO#PLATINIUMPLATEEQUIPMENT9968686.exe.3b4cd78.2.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 1 entries				

Sigma Overview

System Summary:

Sigma detected: Powershell Defender Exclusion

Sigma detected: Non Interactive PowerShell

Sigma detected: T1086 PowerShell Execution

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Networking:

Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)

System Summary:

Initial sample is a PE file and has a suspicious name

.NET source code contains very large strings

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

Moves itself to temp directory

Malware Analysis System Evasion:

Yara detected AntiVM3

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

Queries sensitive video device information (via WMI, Win32_VideoController, often done to detect virtual machines)

Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

Queries sensitive BIOS Information (via WMI, Win32_Bios & Win32_BaseBoard, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Adds a directory exclusion to Windows Defender

Stealing of Sensitive Information:

Yara detected AgentTesla

Tries to steal Mail credentials (via file access)

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

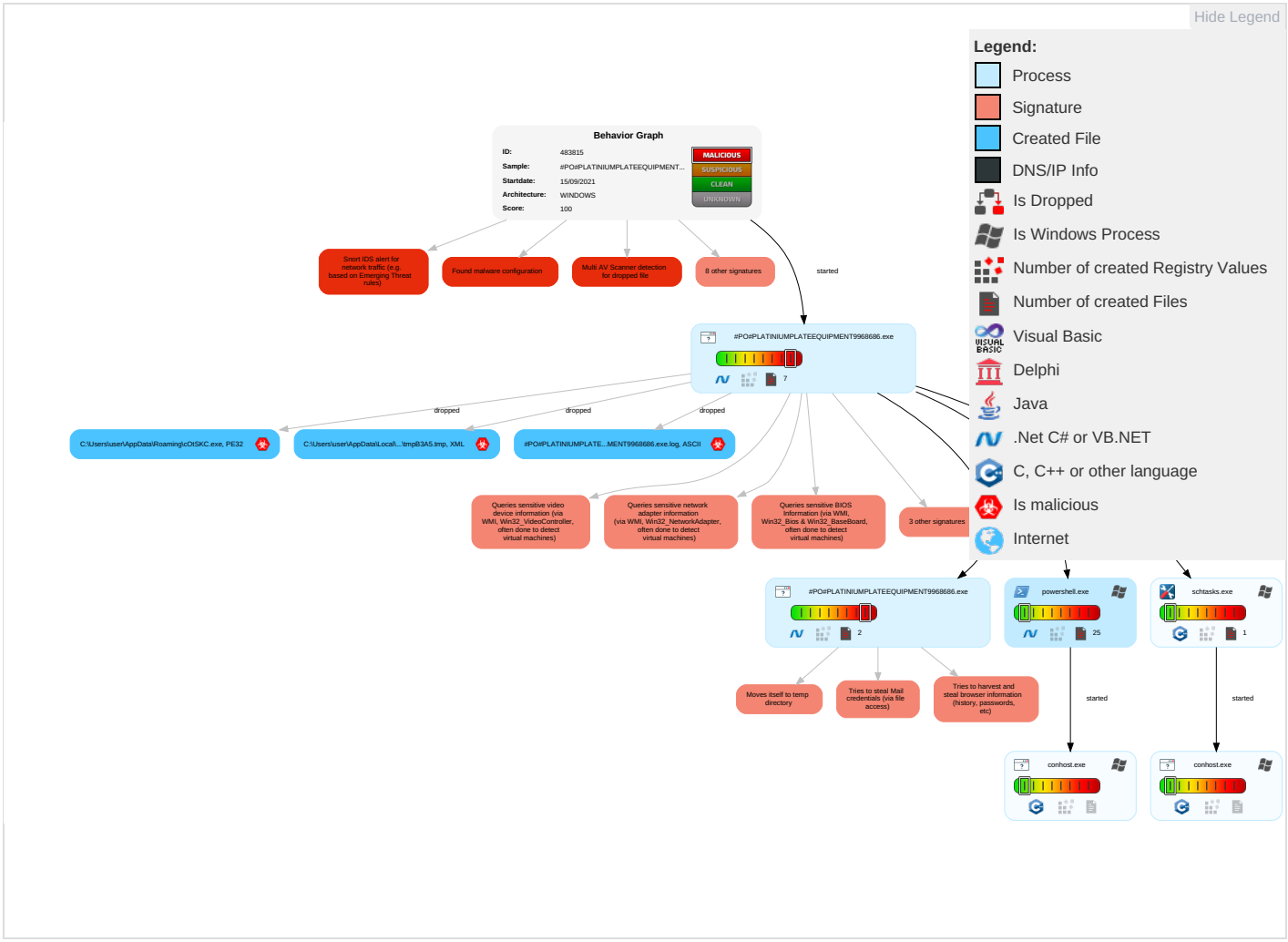
Remote Access Functionality:

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 3 1 1	Scheduled Task/Job 1	Process Injection 1 1 2	Masquerading 1 1	OS Credential Dumping 1	Query Registry 1	Remote Services	Email Collection 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job 1	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1 1	Input Capture 1	Security Software Discovery 4 2 1	Remote Desktop Protocol	Input Capture 1	Exfiltration Over Bluetooth	Junk Data
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Virtualization/Sandbox Evasion 2 4 1	Security Account Manager	Process Discovery 2	SMB/Windows Admin Shares	Archive Collected Data 1 1	Automated Exfiltration	Steganography
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1 2	NTDS	Virtualization/Sandbox Evasion 2 4 1	Distributed Component Object Model	Data from Local System 1	Scheduled Transfer	Protocol Impersonation
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Deobfuscate/Decode Files or Information 1	LSA Secrets	Application Window Discovery 1	SSH	Clipboard Data 1	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Obfuscated Files or Information 2	Cached Domain Credentials	File and Directory Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatior
External Remote Services	Scheduled Task	Startup Items	Startup Items	Software Packing 1 3	DCSync	System Information Discovery 1 1 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

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
#PO#PLATINIUMPLATEEQUIPMENT9968686.exe	25%	Virustotal		Browse
#PO#PLATINIUMPLATEEQUIPMENT9968686.exe	20%	ReversingLabs	ByteCode-MSIL.Trojan.SnakeKeylogger	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\cOtSKC.exe	20%	ReversingLabs	ByteCode-MSIL.Trojan.SnakeKeylogger	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
11.2.#PO#PLATINIUMPLATEEQUIPMENT9968686.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	
http://www.jiyu-kobo.co.jp/va:	0%	Avira URL Cloud	safe	
http://www.fontbureau.comI.TTF	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/ue	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://smtp.bonfigliolli.com	0%	Virustotal		Browse
http://smtp.bonfigliolli.com	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.fontbureau.comtoc	0%	Avira URL Cloud	safe	
http://www.fontbureau.coml1	0%	URL Reputation	safe	
http://www.sajatypeworks.com	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.jiyu-kobo.co.jp/:	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/8	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/3	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
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://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/wa	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.jiyu-kobo.co.jp/P	0%	URL Reputation	safe	
http://uVAudA.com	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/M	0%	URL Reputation	safe	
http://www.fontbureau.com.TTFB	0%	Avira URL Cloud	safe	
http://https://5xKiHIOzRhQXhIdK.net	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/B	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fontbureau.comoitu	0%	URL Reputation	safe	
http://www.galapagosdesign.com/3	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/t	0%	URL Reputation	safe	
http://www.fontbureau.comt	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/k	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.fontbureau.comals	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	483815
Start date:	15.09.2021
Start time:	14:23:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 4s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	#PO#PLATINIUMPLATEEQUIPMENT9968686.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:	32
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@9/8@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:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
14:24:32	API Interceptor	619x Sleep call for process: #PO#PLATINIUMPLATEEQUIPMENT9968686.exe modified
14:24:42	API Interceptor	41x Sleep call for process: powershell.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\#PO#PLATINIUMPLATEEQUIPMENT9968686.exe.log	
Process:	C:\Users\user\Desktop\#PO#PLATINIUMPLATEEQUIPMENT9968686.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1308
Entropy (8bit):	5.345811588615766
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84FsXE8:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzu
MD5:	2E016B886BDB8389D2DD0867BE55F87B
SHA1:	25D28EF2ACBB41764571E06E11BF4C05DD0E2F8B
SHA-256:	1D037CF00A8849E6866603297F85D3DABE09535E72EDD2636FB7D0F6C7DA3427
SHA-512:	C100729153954328AA2A77EECB2A3CBD03CB7E8E23D736000F890B17AAA50BA87745E30FB9E2B0D61E16DCA45694C79B4CE09B9F4475220BEB38CAEA546CFC2A
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..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=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\StartupProfileData-NonInteractive	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	22276
Entropy (8bit):	5.600191675541196
Encrypted:	false
SSDEEP:	384:HtCDLq02eBqnpZAEKUlvMSBKnmZ+b7A9gt/SJ3xeT1MaXZlbAV77ViZBDI+iOE:fewnpVKqvM4KmcHtc8C+fwkVY
MD5:	1401C0135C454F730F063F4164AE8A82
SHA1:	6D8186449CA569E50E7B0191D9354174FAD2B3FB
SHA-256:	DC358D30359360610DAE3A372919C2709BB5483A699EAB005FC18DC46D3519A8
SHA-512:	F4C5951DAC1641AC16709DA96C65E2942E4192169619ACE983757A500C12BD6F398CF75856A1BE378DF1A960AA9499DAD5AC4AEA080C8D84BDD2DB43BCD7F6AB
Malicious:	false
Reputation:	low
Preview:	@...e..........y.....e.................E.........@.........H..............<@.^.L."My...:P..... .Microsoft.PowerShell.ConsoleHostD..............fZve...F.....x.).....System.Management.Automation4.............[...{a.C..%6..h.....System.Core.0.............G-.o...A...4B.........System..4.................Zg5..:O..g..q.........System.Xml..L..............7.....J@.....~.....#.Microsoft.Management.Infrastructure.8.............'....L..}.............System.Numerics.@.................Lo...QN.....<Q........System.DirectoryServices<.................H..QN.Y.f.....System.Management...4.....................].D.E.....#.......System.Data.H.................. ....H..m)aUu.........Microsoft.PowerShell.Security...<.....................~.[L.D.Z.>..m.........System.Transactions.<.....................):gK..G...$.1.q.....System.ConfigurationP.....................C..J..%...].....%.Microsoft.PowerShell.Commands.Utility...D.....................-.D.F.<;.nt.1 ....System.Configuration.Ins

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_45mgaeg2.urh.ps1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_45mgaeg2.urh.ps1	
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_pbpiujfn.0hz.psm1	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	very short file (no magic)
Category:	dropped
Size (bytes):	1
Entropy (8bit):	0.0
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Preview:	1

C:\Users\user\AppData\Local\Temp\tmpB3A5.tmp	
Process:	C:\Users\user\Desktop\#PO#PLATINIUMPLATEEQUIPMENT9968686.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1639
Entropy (8bit):	5.184161769187072
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBUtn:cbh47TlNQ//rydbz9I3YODOLNdq3A
MD5:	D881801981218ED2DB1DFAA2DD185C8B
SHA1:	844F6669003A8F7E3C4B55D88CE39802A4766FD0
SHA-256:	C3DF8E64F808A44023AA56413F20D0698E248AA24E38185975A7431493D1A209
SHA-512:	EDED9315B1B6BCC581ECCD2CD6C305F36393F5AB37CD104DB1CAA345DBD18C64FB4D03AB782193CE9C530069E5FFEB91C1154CB7933865619871F0B8849798 4
Malicious:	**true**
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>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\cOtSKC.exe	
Process:	C:\Users\user\Desktop\#PO#PLATINIUMPLATEEQUIPMENT9968686.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	709632
Entropy (8bit):	7.468928450849731
Encrypted:	false
SSDEEP:	12288:vgWHCM2K4CeI/yzQs2TaIpIRfrjqiKPTYREEZKEgEjJ0h9rqCKyC7uzLja0l:vY3CjMIpIRfrfqYRTKEgVh4CNDI
MD5:	D5CE2C4E604D99887C87BBA2C03244FD
SHA1:	B6F6BFF3E715B6D0093EF2EDA2296F81611362EA
SHA-256:	21D1D5C0E8C4CFA47F08EC502A9D372597731C8FE252A03DB5825C11497AD657
SHA-512:	1137501775EBD9311F459A0C3F12D4A42DC5D8BBEC12D3D967F05AF6BD56364BC2B640E61402DFE66F68BA70810E884CA42EB3DE35B762328EA6BAD4A10B53 A
Malicious:	**true**
Antivirus:	• Antivirus: ReversingLabs, Detection: 20%

C:\Users\user\AppData\Roaming\cOtSKC.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Aa.....0..d...n.....r.... .....@.. .....@..... ..@..... ...O.....k..... ....H.....text...xb... ...d..... ..`.rsrc....k.....l...f.....@..@.reloc..... .....@..B.....T.....H.....x.....Q...x+...V.....0.....}.....(.....(.....r...p.(....(....o.....{.....(....o.....{....r...p.(....(....o.....{.....(....o.....{.....(....o.....{.....(....o.....*...0..._.....(.....(.....o.....,)....t.....o....r-..p(.....,.o.....+..(....o....(.....+...*..0.....(....o....o ...o!....+..*...0..:.....(.....(.....o.....,,r-..p.+....t.... o"....+..*...0..:.....(.....(....

C:\Users\user\AppData\Roaming\cOtSKC.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\#PO#PLATINIUMPLATEEQUIPMENT9968686.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
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20210915\PowerShell_transcript.376483.vpXEvE+r.20210915142441.txt	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	UTF-8 Unicode (with BOM) text, with CRLF line terminators
Category:	dropped
Size (bytes):	5853
Entropy (8bit):	5.458014846517267
Encrypted:	false
SSDEEP:	96:BZLhxNmqDo1Z7ZXhxNmqDo1Z5t3VjZrhxNmqDo1ZLMllnZE:Y
MD5:	7B61C2914C4D6177F15CC19D06DD3E1A
SHA1:	DFDF4D5706B6D7664D9F51956859C93ACDDCE4E4
SHA-256:	DED66ECAA2B2F756070C0B2CFA04D8D303C113F1DAB5E27750F41F87F4492AE9
SHA-512:	C30165B0ABD854D326DFF404DF4E55A9A28011E520740B229D81E2753C128D92C3F09622CE6EB66D75DB7FBAC98E5CEFD85C301A5216D8400B8E85D386C33B
Malicious:	false
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210915142442..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 376483 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\#PO#PLATINIUMPLATEEQUIPMENT9968686.exe..Process ID: 1092..PSVersion: 5.1.17134.1..PSEdition: Desktop..PSCompatibleVersions: 1.0, 2.0, 3.0, 4.0, 5.0, 5.1.17134.1..BuildVersion: 10.0.17134.1..CLRVersion: 4.0.30319.42000..WSManStackVersion: 3.0..PSRemotingProtocolVersion: 2.3..SerializationVersion: 1.1.0.1..**********..**********..Command start time: 20210915142442..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\#PO#PLATINIUMPLATEEQUIPMENT9968686.exe..**********..Windows PowerShell transcript start..Start time: 202109151 42936..Username: computer\user..

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.468928450849731
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% • Win16/32 Executable Delphi generic (2074/23) 0.01% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	#PO#PLATINIUMPLATEEQUIPMENT9968686.exe
File size:	709632
MD5:	d5ce2c4e604d99887c87bba2c03244fd
SHA1:	b6f6bff3e715b6d0093ef2eda2296f81611362ea
SHA256:	21d1d5c0e8c4cfa47f08ec502a9d372597731c8fe252a03db5825c11497ad657

General

SHA512:	1137501775ebd9311f459a0c3f12d4a42dc5d8bbec12d3c967f05af6bd56364bc2b640e61402dfe66f68ba70810e884ca42eb3de35b762328ea6bad4a10b537a
SSDEEP:	12288:vgWHCM2K4CeI/yzQs2TaIpIRfrjqiKPTYREEZKEgEjJ0h9rqCKyC7uzLja0I:vY3CjMIpIRfrfqYRTKEgVh4CNDI
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....Aa.....0..d...n.....r.... .....@.. .....@.....@.....

File Icon

Icon Hash:	f1f0f4d0eecccc71

Static PE Info

General

Entrypoint:	0x4a8272
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:	0x61418FFD [Wed Sep 15 06:17:33 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	0xa6278	0xa6400	False	0.824552102914	data	7.53937303324	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xaa000	0x6ba0	0x6c00	False	0.442853009259	data	5.09551800776	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xb2000	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

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: #PO#PLATINIUMPLATEEQUIPMENT9968686.exe PID: 4856 Parent PID: 6124

General

Start time:	14:24:24
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\#PO#PLATINIUMPLATEEQUIPMENT9968686.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\#PO#PLATINIUMPLATEEQUIPMENT9968686.exe'
Imagebase:	0x6e0000
File size:	709632 bytes
MD5 hash:	D5CE2C4E604D99887C87BBA2C03244FD
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: 00000000.00000002.277208501.0000000003CEC000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.277208501.0000000003CEC000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.276757595.0000000003A89000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.276757595.0000000003A89000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.276209435.0000000002A81000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 1092 Parent PID: 4856

General

Start time:	14:24:39
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\#PO#PLATINIUMPLATEEQUIPMENT9968686.exe'
Imagebase:	0xf30000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: conhost.exe PID: 6080 Parent PID: 1092

General

Start time:	14:24:40
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: schtasks.exe PID: 2780 Parent PID: 4856

General

Start time:	14:24:40
Start date:	15/09/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\cOtSKC' /XML 'C:\Users\user\AppData\Local\Temp\tmpB3A5.tmp'
Imagebase:	0xdf0000
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

Analysis Process: conhost.exe PID: 1276 Parent PID: 2780

General

Start time:	14:24:42
Start date:	15/09/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff6b2800000
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: #PO#PLATINIUMPLATEEQUIPMENT9968686.exe PID: 1064 Parent PID: 4856

General

Start time:	14:24:42
Start date:	15/09/2021
Path:	C:\Users\user\Desktop\#PO#PLATINIUMPLATEEQUIPMENT9968686.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\#PO#PLATINIUMPLATEEQUIPMENT9968686.exe
Imagebase:	0x9e0000
File size:	709632 bytes
MD5 hash:	D5CE2C4E604D99887C87BBA2C03244FD
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: 0000000B.00000002.502821504.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000B.00000002.502821504.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000B.00000002.511511733.0000000002E31000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000B.00000002.511511733.0000000002E31000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities | Show Windows behavior

File Created

File Read

Disassembly

Code Analysis