
**ID:** 451593
**Sample Name:**
SKGCTMGCarta20210701516374466893343426doc.exe
**Cookbook:** default.jbs
**Time:** 20:52:21
**Date:** 20/07/2021
**Version:** 33.0.0 White Diamond

# Table of Contents

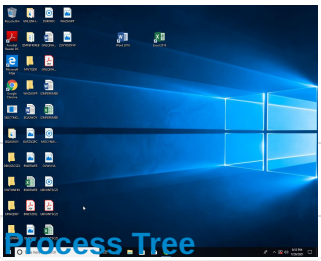
# Windows Analysis Report SKGCTMGCarta20210701516…

## Overview

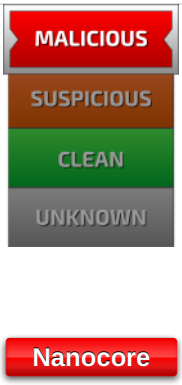
### General Information

| | |
|---|---|
| Sample Name: | SKGCTMGCarta20210701516374466893343426doc.exe |
| Analysis ID: | 451593 |
| MD5: | 0eb0833449cec3.. |
| SHA1: | 63c969feee64e6f.. |
| SHA256: | 945ab6b146dc53.. |
| Tags: | exe NanoCore RAT |
| Infos: | |

Most interesting Screenshot:




### Detection

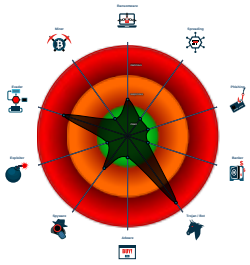



| | |
|---|---|
| Score: | 100 |
| Range: | 0 - 100 |
| Whitelisted: | false |
| Confidence: | 100% |

### Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Sigma detected: NanoCore
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- C2 URLs / IPs found in malware con…
- Injects a PE file into a foreign proce…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…

### Classification



- **System is w10x64**
- SKGCTMGCarta20210701516374466893343426doc.exe (PID: 6916 cmdline: 'C:\Users\user\Desktop\SKGCTMGCarta20210701516374466893343426doc.exe' MD5: 0EB0833449CEC388F8157458FC600691)
  - schtasks.exe (PID: 6772 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\sNIYazJXiEQfkP' /XML 'C:\Users\user\AppData\Local\Temp\tmp1ACF.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6472 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - MSBuild.exe (PID: 6436 cmdline: C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe MD5: D621FD77BD585874F9686D3A76462EF1)
- **cleanup**

## Malware Configuration

### Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "01f9d977-6605-495e-941a-753d3cd6",
  "Group": "4Maticross.",
  "Domain1": "178.170.138.163",
  "Domain2": "",
  "Port": 5626,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Disable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Disable",
  "ClearAccessControl": "Disable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Disable",
  "ActivateAwayMode": "Disable",
  "EnableDebugMode": "Disable",
  "RunDelay": 0,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "8.8.8.8",
  "BackupDNSServer": "8.8.4.4"
}
```


# Yara Overview

## Memory Dumps

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 00000009.00000002.921988297.000000000638 0000.00000004.00000001.sdmp | Nanocore_RAT_Gen_2 | Detetcs the Nanocore RAT | Florian Roth | • 0x39eb:$x1: NanoCore.ClientPluginHost<br>• 0x3a24:$x2: IClientNetworkHost |
| 00000009.00000002.921988297.000000000638 0000.00000004.00000001.sdmp | Nanocore_RAT_Feb18_1 | Detects Nanocore RAT | Florian Roth | • 0x39eb:$x2: NanoCore.ClientPluginHost<br>• 0x3b36:$s4: PipeCreated<br>• 0x3a05:$s5: IClientLoggingHost |
| 00000009.00000002.920719011.000000000534 0000.00000004.00000001.sdmp | Nanocore_RAT_Gen_2 | Detetcs the Nanocore RAT | Florian Roth | • 0x4bbb:$x1: NanoCore.ClientPluginHost<br>• 0x4be5:$x2: IClientNetworkHost |
| 00000009.00000002.920719011.000000000534 0000.00000004.00000001.sdmp | Nanocore_RAT_Feb18_1 | Detects Nanocore RAT | Florian Roth | • 0x4bbb:$x2: NanoCore.ClientPluginHost<br>• 0x6a6b:$s4: PipeCreated |
| 00000009.00000002.922327045.000000000683 0000.00000004.00000001.sdmp | Nanocore_RAT_Gen_2 | Detetcs the Nanocore RAT | Florian Roth | • 0x5fee:$x1: NanoCore.ClientPluginHost<br>• 0x602b:$x2: IClientNetworkHost |
| Click to see the 37 entries | | | | |

## Unpacked PEs

| Source | Rule | Description | Author | Strings |
|---|---|---|---|---|
| 9.2.MSBuild.exe.5270000.20.raw.unpack | Nanocore_RAT_Gen_2 | Detetcs the Nanocore RAT | Florian Roth | • 0xe75:$x1: NanoCore.ClientPluginHost<br>• 0xe8f:$x2: IClientNetworkHost |
| 9.2.MSBuild.exe.5270000.20.raw.unpack | Nanocore_RAT_Feb18_1 | Detects Nanocore RAT | Florian Roth | • 0xe75:$x2: NanoCore.ClientPluginHost<br>• 0x1261:$s3: PipeExists<br>• 0x1136:$s4: PipeCreated<br>• 0xeb0:$s5: IClientLoggingHost |
| 9.2.MSBuild.exe.53b0000.25.unpack | Nanocore_RAT_Gen_2 | Detetcs the Nanocore RAT | Florian Roth | • 0x605:$x1: NanoCore.ClientPluginHost<br>• 0x63e:$x2: IClientNetworkHost |
| 9.2.MSBuild.exe.53b0000.25.unpack | Nanocore_RAT_Feb18_1 | Detects Nanocore RAT | Florian Roth | • 0x605:$x2: NanoCore.ClientPluginHost<br>• 0x720:$s4: PipeCreated<br>• 0x61f:$s5: IClientLoggingHost |
| 9.2.MSBuild.exe.3c5b3e6.14.unpack | Nanocore_RAT_Gen_2 | Detetcs the Nanocore RAT | Florian Roth | • 0x170b:$x1: NanoCore.ClientPluginHost<br>• 0x1725:$x2: IClientNetworkHost |
| Click to see the 121 entries | | | | |

# Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Possible Applocker Bypass

Stealing of Sensitive Information:

Sigma detected: NanoCore

Remote Access Functionality:

Sigma detected: NanoCore

## Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for domain / URL

Multi AV Scanner detection for dropped file

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

C2 URLs / IPs found in malware configuration

E-Banking Fraud:

Yara detected Nanocore RAT

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

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

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Writes to foreign memory regions

## Stealing of Sensitive Information:

Yara detected Nanocore RAT

## Remote Access Functionality:

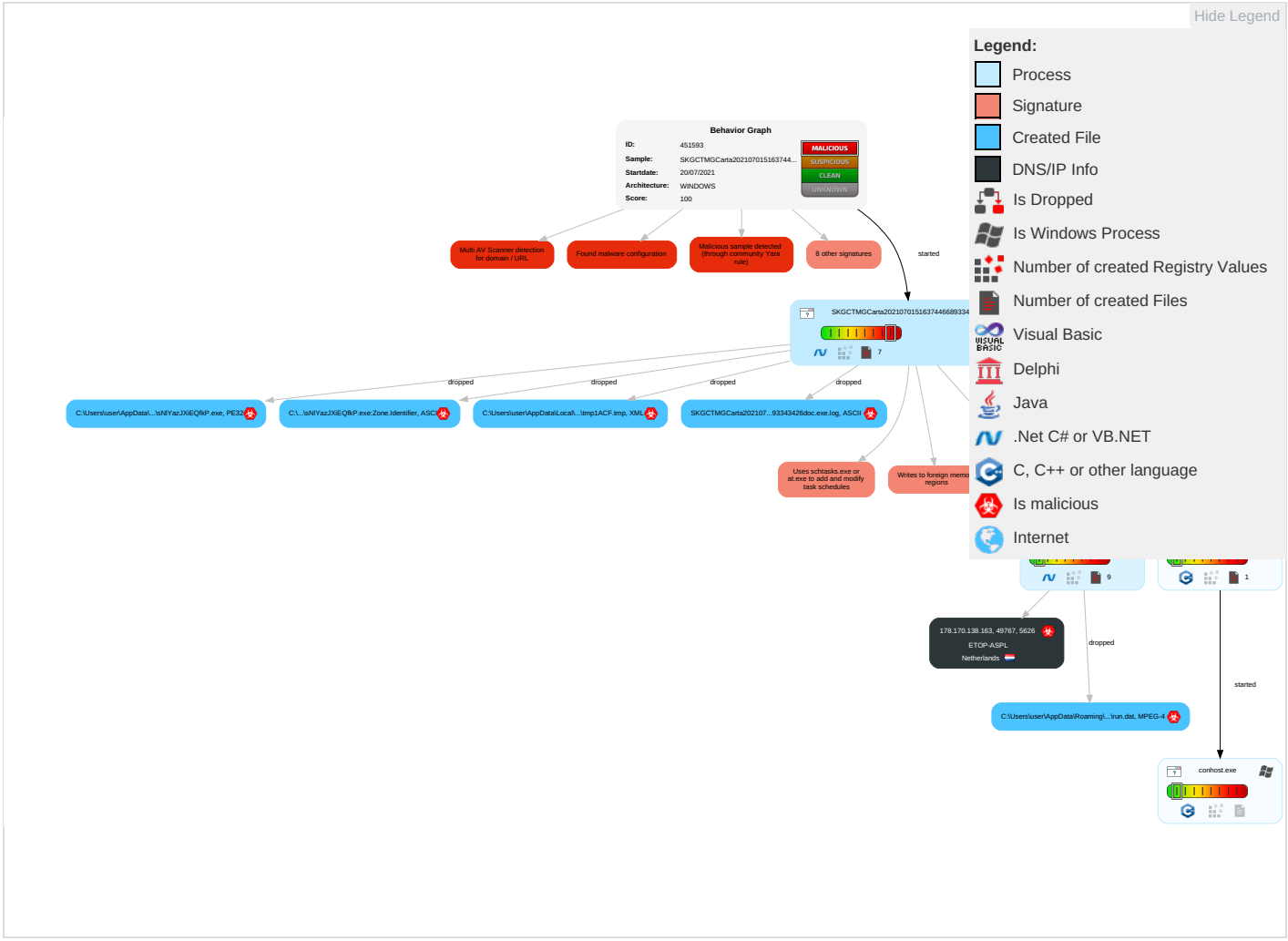
Detected Nanocore Rat

Yara detected Nanocore RAT

## Mitre Att&ck Matrix

| Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Exfiltration | Command and Control | N E |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Valid Accounts | Windows Management Instrumentation 1 | Scheduled Task/Job 1 | Process Injection 2 1 2 | Masquerading 1 | Input Capture 1 1 | Security Software Discovery 1 1 1 | Remote Services | Input Capture 1 1 | Exfiltration Over Other Network Medium | Encrypted Channel 1 2 | E I N C |
| Default Accounts | Scheduled Task/Job 1 | Boot or Logon Initialization Scripts | Scheduled Task/Job 1 | Disable or Modify Tools 1 | LSASS Memory | Process Discovery 2 | Remote Desktop Protocol | Archive Collected Data 1 1 | Exfiltration Over Bluetooth | Non-Standard Port 1 | E F C |
| Domain Accounts | At (Linux) | Logon Script (Windows) | Logon Script (Windows) | Virtualization/Sandbox Evasion 2 1 | Security Account Manager | Virtualization/Sandbox Evasion 2 1 | SMB/Windows Admin Shares | Data from Network Shared Drive | Automated Exfiltration | Remote Access Software 1 | E T L |
| Local Accounts | At (Windows) | Logon Script (Mac) | Logon Script (Mac) | Process Injection 2 1 2 | NTDS | Application Window Discovery 1 | Distributed Component Object Model | Input Capture | Scheduled Transfer | Application Layer Protocol 1 1 | S S |
| Cloud Accounts | Cron | Network Logon Script | Network Logon Script | Deobfuscate/Decode Files or Information 1 | LSA Secrets | File and Directory Discovery 1 | SSH | Keylogging | Data Transfer Size Limits | Fallback Channels | M D C |
| Replication Through Removable Media | Launchd | Rc.common | Rc.common | Obfuscated Files or Information 1 | Cached Domain Credentials | System Information Discovery 1 2 | VNC | GUI Input Capture | Exfiltration Over C2 Channel | Multiband Communication | J D S |
| External Remote Services | Scheduled Task | Startup Items | Startup Items | Software Packing 1 2 | DCSync | Network Sniffing | Windows Remote Management | Web Portal Capture | Exfiltration Over Alternative Protocol | Commonly Used Port | F A |

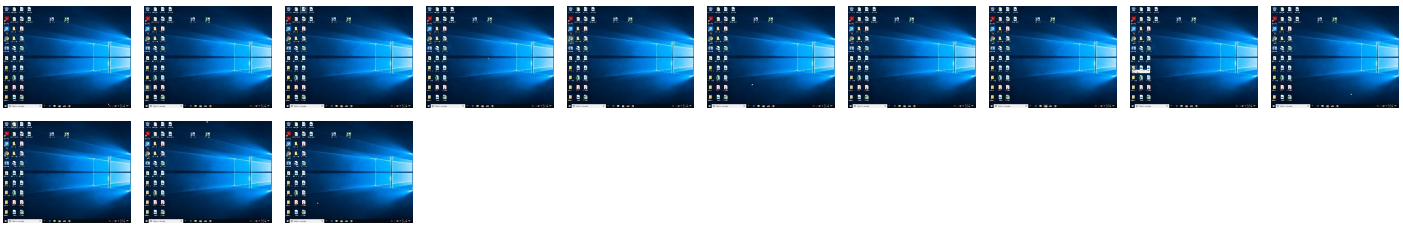
## Behavior Graph




## 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 |
|---|---|---|---|---|
| SKGCTMGCarta20210701516374466893343426doc.exe | 100% | Joe Sandbox ML | | |

## Dropped Files

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| C:\Users\user\AppData\Roaming\sNlYazJXiEQfkP.exe | 100% | Joe Sandbox ML | | |
| C:\Users\user\AppData\Roaming\sNlYazJXiEQfkP.exe | 20% | ReversingLabs | Win32.Trojan.Pwsx | |

## Unpacked PE Files

| Source | Detection | Scanner | Label | Link | Download |
|---|---|---|---|---|---|
| 9.2.MSBuild.exe.53c0000.27.unpack | 100% | Avira | TR/NanoCore.fadte | | Download File |
| 9.2.MSBuild.exe.38f8a10.6.unpack | 100% | Avira | TR/NanoCore.fadte | | Download File |
| 9.2.MSBuild.exe.400000.0.unpack | 100% | Avira | TR/Dropper.MSIL.Gen7 | | Download File |

## Domains

No Antivirus matches

## URLs

| Source | Detection | Scanner | Label | Link |
|---|---|---|---|---|
| 178.170.138.163 | 6% | Virustotal | | Browse |
| 178.170.138.163 | 0% | Avira URL Cloud | safe | |
| | 0% | Avira URL Cloud | safe | |
| http://www.jiyu-kobo.co.jp/str | 0% | Avira URL Cloud | safe | |
| http://www.jiyu-kobo.co.jp/U | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/U | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/U | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/U | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/a-e | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/a-e | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/a-e | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/a-e | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/jp/G | 0% | Avira URL Cloud | safe | |
| http://www.founder.com.cn/cnre | 0% | Avira URL Cloud | safe | |
| http://www.jiyu-kobo.co.jp/G | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/G | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/G | 0% | URL Reputation | 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://tempuri.org/SeguridadDS.xsd | 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://www.jiyu-kobo.co.jp/7 | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/7 | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/7 | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/wdthd | 0% | Avira URL Cloud | safe | |
| http://www.jiyu-kobo.co.jp/Y0o | 0% | Avira URL Cloud | safe | |
| http://www.jiyu-kobo.co.jp/q | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/q | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/q | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp/iv | 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.founder.com.cn/cnt | 0% | URL Reputation | safe | |
| http://www.founder.com.cn/cnt | 0% | URL Reputation | safe | |
| http://www.founder.com.cn/cnt | 0% | URL Reputation | safe | |
| http://www.fonts.comn | 0% | URL Reputation | safe | |
| http://www.fonts.comn | 0% | URL Reputation | safe | |
| http://www.fonts.comn | 0% | URL Reputation | safe | |
| http://www.carterandcone.como. | 0% | URL Reputation | safe | |
| http://www.carterandcone.como. | 0% | URL Reputation | safe | |
| http://www.carterandcone.como. | 0% | URL Reputation | safe | |
| http://www.jiyu-kobo.co.jp//-e | 0% | Avira URL Cloud | safe | |
| http://www.jiyu-kobo.co.jp/fed | 0% | Avira URL Cloud | safe | |

# Domains and IPs

## Contacted Domains

**No contacted domains info**

## Contacted URLs

| Name | Malicious | Antivirus Detection | Reputation |
|---|---|---|---|
| 178.170.138.163 | true | • 6%, Virustotal, Browse<br>• Avira URL Cloud: safe | unknown |
| | true | • Avira URL Cloud: safe | low |

## URLs from Memory and Binaries

## Contacted IPs

### Public

| IP | Domain | Country | Flag | ASN | ASN Name | Malicious |
|---|---|---|---|---|---|---|
| 178.170.138.163 | unknown | Netherlands | | 20853 | ETOP-ASPL | true |

# General Information

| | |
|---|---|
| Joe Sandbox Version: | 33.0.0 White Diamond |
| Analysis ID: | 451593 |
| Start date: | 20.07.2021 |
| Start time: | 20:52:21 |
| Joe Sandbox Product: | CloudBasic |
| Overall analysis duration: | 0h 9m 41s |
| Hypervisor based Inspection enabled: | false |
| Report type: | light |
| Sample file name: | SKGCTMGCarta2021070151637446689334343426doc.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: | 19 |
| 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<br>• EGA enabled<br>• HDC enabled<br>• AMSI enabled |
| Analysis Mode: | default |
| Analysis stop reason: | Timeout |
| Detection: | MAL |
| Classification: | mal100.troj.evad.winEXE@6/8@0/1 |
| EGA Information: | Failed |
| HDC Information: | Failed |
| HCA Information: | • Successful, ratio: 83%<br>• Number of executed functions: 0<br>• Number of non-executed functions: 0 |
| Cookbook Comments: | • Adjust boot time<br>• Enable AMSI<br>• Found application associated with file extension: .exe |
| Warnings: | Show All |

# Simulations

## Behavior and APIs

| Time | Type | Description |
|---|---|---|
| 20:53:39 | API Interceptor | 2x Sleep call for process: SKGCTMGCarta2021070151637446689334343426doc.exe modified |

# Joe Sandbox View / Context

## IPs

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| 178.170.138.163 | SKCTMG_Carta_20210707_16374466893343426doc.exe | Get hash | malicious | Browse | |
| | #U0639#U0631#U0636 #U0627#U0644#U0645#U0646#U062a#U062c Stomanas_SKCGM_63746352021doc.exe | Get hash | malicious | Browse | |
| | Documento de transferencia de Scotiabank7497574730084doc.exe | Get hash | malicious | Browse | |
| | Documento de transferencia de Scotiabank749757473008422doc.exe | Get hash | malicious | Browse | |
| | Documento relativo al carico e alla spedizione del cliente_italy2020.exe | Get hash | malicious | Browse | |
| | Sitech#U4ea7#U54c1#U54a8#U8be2#U89c4#U8303754378y9986456Taiwan2020.exe | Get hash | malicious | Browse | |
| | Detalles de la descripci#U00f3n de la oferta del producto.exe | Get hash | malicious | Browse | |
| | Detalles de la descripci#U00f3n de la oferta del producto.exe | Get hash | malicious | Browse | |
| | Documentos internos de transferencia de dinero Banco Santader.exe | Get hash | malicious | Browse | |
| | Documentos internos de transferencia de dinero Banco Santader.exe | Get hash | malicious | Browse | |
| | Albawardi Group Project offer description 678467463756382020.exe | Get hash | malicious | Browse | |
| | Opis proizvoda prema kvaliteti i modelima2020.exe | Get hash | malicious | Browse | |
| | Opis proizvoda prema kvaliteti i modelima2020.exe | Get hash | malicious | Browse | |
| | Documentos de pago bancario 36587634 Bisa2020.exe | Get hash | malicious | Browse | |
| | Beschrijving van productaanbiedingcWbZN52020.exe | Get hash | malicious | Browse | |
| | Descri#U00e7#U00e3o da oferta do produto 873564635640rden2020.exe | Get hash | malicious | Browse | |
| | Descri#U00e7#U00e3o da oferta do produto 873564635640rden2020.exe | Get hash | malicious | Browse | |
| | BIDAKIS DOO PONUDA PROIZVODA.exe | Get hash | malicious | Browse | |
| | DocumentoNota Cobran#U00e7a IMI (FFPT-2019223912003).exe | Get hash | malicious | Browse | |
| | DocumentoNota Cobran#U00e7a IMI (FFPT-2019223912003).exe | Get hash | malicious | Browse | |

## Domains

No context

## ASN

| Match | Associated Sample Name / URL | SHA 256 | Detection | Link | Context |
|---|---|---|---|---|---|
| ETOP-ASPL | v6clgzEGCb | Get hash | malicious | Browse | • 194.87.61.219 |
| | SKCTMG_Carta_20210707_16374466893343426doc.exe | Get hash | malicious | Browse | • 178.170.138.163 |
| | #U0639#U0631#U0636 #U0627#U0644#U0645#U0646#U062a#U062c Stomanas_SKCGM_63746352021doc.exe | Get hash | malicious | Browse | • 178.170.138.163 |
| | DEBT_06032021_727093524.xlsm | Get hash | malicious | Browse | • 217.147.172.75 |
| | DEBT_06032021_727093524.xlsm | Get hash | malicious | Browse | • 217.147.172.75 |
| | p8Wo6PbOjL.exe | Get hash | malicious | Browse | • 194.87.248.186 |
| | DEBT_06032021_1841965006.xlsm | Get hash | malicious | Browse | • 217.147.172.75 |
| | DEBT_06032021_1841965006.xlsm | Get hash | malicious | Browse | • 217.147.172.75 |
| | 21305177357_05272021.xlsm | Get hash | malicious | Browse | • 217.147.172.75 |
| | 21305177357_05272021.xlsm | Get hash | malicious | Browse | • 217.147.172.75 |
| | 21881755902_05272021.xlsm | Get hash | malicious | Browse | • 217.147.172.75 |
| | 21881755902_05272021.xlsm | Get hash | malicious | Browse | • 217.147.172.75 |
| | SecuriteInfo.com.Downloader-FCEIFE04EE03A3CA.23702.xlsx | Get hash | malicious | Browse | • 217.147.172.65 |
| | SecuriteInfo.com.Downloader-FCEIFE04EE03A3CA.23702.xlsx | Get hash | malicious | Browse | • 217.147.172.65 |
| | SecuriteInfo.com.Heur.18790.xlsx | Get hash | malicious | Browse | • 217.147.172.65 |
| | SecuriteInfo.com.Heur.18790.xlsx | Get hash | malicious | Browse | • 217.147.172.65 |
| | 21975030260_05262021.xlsm | Get hash | malicious | Browse | • 217.147.172.65 |
| | 21975030260_05262021.xlsm | Get hash | malicious | Browse | • 217.147.172.65 |
| | LGZCUIMYwQ.exe | Get hash | malicious | Browse | • 178.170.138.116 |
| | Smart wireless request.xlsb | Get hash | malicious | Browse | • 178.170.138.116 |

## JA3 Fingerprints

**No context**

## Dropped Files

**No context**

# Created / dropped Files

| C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\SKGCTMGCarta2021070151637446689334426doc.exe.log | |
|---|---|
| Process: | C:\Users\user\Desktop\SKGCTMGCarta2021070151637446689334426doc.exe |
| File Type: | ASCII text, with CRLF line terminators |
| Category: | modified |
| Size (bytes): | 1594 |
| Entropy (8bit): | 5.336334182031907 |
| Encrypted: | false |
| SSDEEP: | 48:MgvjHK5HKXE1qHiYHKhQnoPtHoxHhAHKzvFHsAmHK2HKSHKKHKs:lrq5qXEwCYqhQnoPtlxHeqzNM/q2qSqY |
| MD5: | B9E8D9BC061D6715808BB3A28CECBA2B |
| SHA1: | 6F18CD63C12AEC962D089F215658FD5BE1789BC3 |
| SHA-256: | 716E082F23E093EBCA2C8F994745CC7D62457D7359BBE555B75E275CE8EEEDC7 |
| SHA-512: | 6D97D3E34CBCC5C0CCF845E285F98DE1824A825AB1D306D20ED164B0B74270CED9AB694E40831EC796E9F823BB4E369166006E555D7BBD000A33A0FDA601F86 |
| Malicious: | **true** |
| 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\tmp1ACF.tmp | |
|---|---|
| Process: | C:\Users\user\Desktop\SKGCTMGCarta2021070151637446689334426doc.exe |
| File Type: | XML 1.0 document, ASCII text, with CRLF line terminators |
| Category: | dropped |
| Size (bytes): | 1647 |
| Entropy (8bit): | 5.1946234784418746 |
| Encrypted: | false |
| SSDEEP: | 24:2dH4+SEqC/S7hblNMFp//rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBGntn:cbhK79lNQR/rydbz9l3YODOLNdq3i |
| MD5: | 8C8CC3C796621F14169BD093EA6818F4 |
| SHA1: | 3B3888BFFD6FC587368AADF30AB6CCAB6724A306 |
| SHA-256: | CF099569F34DBAFE264CE066E5685D9FF0FB391813DBB88F5460808F0936F01E |
| SHA-512: | 5BC2AB27CAC294C49159A0CE67E8011CA6E0695B51D0B34E9F956C751F4A812F003458499D5EC0AD12551BB2B797CA309A2C5FE127848923E9E94635445BB8B |
| 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\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat | |
|---|---|
| Process: | C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 232 |
| Entropy (8bit): | 7.024371743172393 |
| Encrypted: | false |
| SSDEEP: | 6:X4LDAnybgCFcpJSQwP4d7ZrqJgTFwoaw+9XU4:X4LEnybgCFCtvd7ZrCgpwoaw+Z9 |
| MD5: | 32D0AAE13696FF7F8AF33B2D22451028 |
| SHA1: | EF80C4E0DB2AE8EF288027C9D3518E6950B583A4 |

| C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat | |
|---|---|
| SHA-256: | 5347661365E7AD2C1ACC27AB0D150FFA097D9246BB3626FCA06989E976E8DD29 |
| SHA-512: | 1D77FC13512C0DBC4EFD7A66ACB502481E4EFA0FB73D0C7D0942448A72B9B05BA1EA78DDF0BE966363C2E3122E0B631DB7630D044D08C1E1D32B9FB025C35E A5 |
| Malicious: | false |
| Reputation: | moderate, very likely benign file |
| Preview: | Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.....@.3..{...grv+V...B.....].P...W.4C}uL.....s~..F...}.....E.....E...6E.....{...{.yS...7..".hK.!.x.2..i..zJ... ....f..?._....0. :e[7w{1.!.4.....&. |

| C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat | |
|---|---|
| Process: | C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe |
| File Type: | MPEG-4 LOAS |
| Category: | dropped |
| Size (bytes): | 8 |
| Entropy (8bit): | 3.0 |
| Encrypted: | false |
| SSDEEP: | 3:5P8t:98t |
| MD5: | 884356AE811E6EC35EC71E122ADD3089 |
| SHA1: | 9346B3622B8A7DFCF2A6923688DD29D4D141D23B |
| SHA-256: | 127F0042509D516159135C721EF6096155D1FECB47E0F7804799BBAA20788394 |
| SHA-512: | 5F8386D2FD81492551B6AB9D9813711AD739FF9CEC0037ACD96FFE1BF0E9DEC47EFD29BFA3C871BEECC9D6B9CDF13FB311E806522AD491C18DDAB6D3D6AC 34D |
| Malicious: | **true** |
| Reputation: | low |
| Preview: | V.{..K.H |

| C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin | |
|---|---|
| Process: | C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 40 |
| Entropy (8bit): | 5.153055907333276 |
| Encrypted: | false |
| SSDEEP: | 3:9bzY6oRDT6P2bfVn1:RzWDT621 |
| MD5: | 4E5E92E2369688041CC82EF9650EDED2 |
| SHA1: | 15E44F2F3194EE232B44E9684163B6F66472C862 |
| SHA-256: | F8098A6290118F2944B9E7C842BD014377D45844379F863B00D54515A8A64B48 |
| SHA-512: | 1B368018907A3BC30421FDA2C935B39DC9073B9B1248881E70AD48EDB6CAA256070C1A90B97B0F64BBE61E316DBB8D5B2EC8DBABCD0B0B2999AB50B933671E CB |
| Malicious: | false |
| Preview: | 9iH...}Z.4..f.~a.....~.~.....3.U. |

| C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat | |
|---|---|
| Process: | C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe |
| File Type: | data |
| Category: | dropped |
| Size (bytes): | 327432 |
| Entropy (8bit): | **7.99938831605763** |
| Encrypted: | **true** |
| SSDEEP: | 6144:oX44S90aTiB66x3Pl6nGV4bfD6wXPIZ9iBj0UeprGm2d7Tm:LkjYGsfGUc9iB4UeprKdnm |
| MD5: | 7E8F4A764B981D5B82D1CC49D341E9C6 |
| SHA1: | D9F0685A028FB219E1A6286AEFB7D6FCFC778B85 |
| SHA-256: | 0BD3AAC12623520C4E2031C8B96B4A154702F36F97F643158E91E987D317B480 |
| SHA-512: | 880E46504FCFB4B15B86B9D8087BA88E6C4950E433616EBB637799F42B081ABF6F07508943ECB1F786B2A89E751F5AE62D750BDCFFDDF535D600CF66EC44E92 |
| Malicious: | false |
| Preview: | pT..!..W..G.J..a.).@.i..wpK.so@...5.=.^..Q.oy.=e@9.B...F..09u"3.. 0t..RDn_4d.....E...i.....~...|..fX_...Xf.p^......>a..$...e.6:7d.(a.A...=.)*.....{B.[...y%.*..i.Q.<..xt.X..H.. ..H F7g...I.*3.{.n....L.y;i..s-....(5i...........J.5b7}..fK..HV..,...0.... ....n.w6PMl.......v.'".v.......#..X.a...../...cC...i..l{>5n.._+.e.d'...}...[..../...D.t..GVp.zz.....(...o.....b...+`J.{....hS1G.^*I..v&. jm.#u..1..Mg!.E..U.T.....6.2>...6.l.K.w"o..E..."K%{....z.7....<...,....]t.:.....[.Z.u...3X8.Ql..j_.&..N..q.e.2...6.R.~..9.Bq..A.v.6.G..#y.....O....Z)G...w..E..k(....+..O.........Vg.2xC..... .O...jc.....z..~.P...q../.-.'.h._.cj.=..B.x.Q9.pu.|i4...i...;O...n.?.,. ....v?.5}.OY@.dG|<.._[.69@.2..m..I..oP=...xrK.?.............b..5....i&...l.c\b}..Q..O+.V.mJ.....pz....>F.......H...6$. ..d...|m...N..1.R..B.i.........$....$.......CY}..$....r.....H...8...li.....7 P......?h....R.iF..6...q(.@LI.s..+K.....?m..H....*. l..&<}....`|.B....3.....I..o...u1..8i=.z.W..7 |

| C:\Users\user\AppData\Roaming\sNlYazJXiEQfkP.exe | |
|---|---|
| Process: | C:\Users\user\Desktop\SKGCTMGCarta20210701516374466893343426doc.exe |
| File Type: | PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows |
| Category: | dropped |

### C:\Users\user\AppData\Roaming\sNlYazJXiEQfkP.exe

| | |
|---|---|
| Size (bytes): | 972288 |
| Entropy (8bit): | 7.334276939082949 |
| Encrypted: | false |
| SSDEEP: | 24576:wgpLmQvDB9Ep2nb+B8NJar5e/A82vMfjYOk:XJbTN8r8FOGS |
| MD5: | 0EB0833449CEC388F8157458FC600691 |
| SHA1: | 63C969FEEE64E6FE65D289FBBDF6E2C971F8878B |
| SHA-256: | 945AB6B146DC530E61824B8CCDD396C6C5D84C9537736DB859771B1EE2DD93FE |
| SHA-512: | EE4AE72DEFE8E6E163523FE9175911AF7EEE9FDF2EF086C16F699B51D08D98EBD9104D3FC6310922F7B729850F878C595319D2E89629C4AF798C267DAB28F1C |
| Malicious: | **true** |
| Antivirus: | • Antivirus: Joe Sandbox ML, Detection: 100%<br>• Antivirus: ReversingLabs, Detection: 20% |
| Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P.....v.... .....@.. .....@.....<br>..@.....$...O.....$..... ..... ..H.....text...|.... ..... ..`.rsrc...$.....@..@.reloc.....<br>.....@..B.....X.....H.....(...$.....L....]..... .....0.....(1...(2.....(.....o3....*.....(4.....(5.....(6.....(7.....(8....*N..(....o....(9<br>....*&..(:....*.s;.....s<.....s=.....s>.....s?.....*....0.....~....o@....+..*.0.....~....oA....+..*.0.....~....oB....+..*.0.....~....oC....+..*.0.....~....oD....+..*&..(E....*<br>...0..<.....~.....(F.....,!r...p.....(G...oH...sI.....~..... |

### C:\Users\user\AppData\Roaming\sNlYazJXiEQfkP.exe:Zone.Identifier

| | |
|---|---|
| Process: | C:\Users\user\Desktop\SKGCTMGCarta2021070151637446689334 26doc.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: | **true** |
| Preview: | [ZoneTransfer]....ZoneId=0 |

# Static File Info

## General

| | |
|---|---|
| File type: | PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows |
| Entropy (8bit): | 7.334276939082949 |
| TrID: | • Win32 Executable (generic) Net Framework (10011505/4) 49.80%<br>• Win32 Executable (generic) a (10002005/4) 49.75%<br>• Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36%<br>• Windows Screen Saver (13104/52) 0.07%<br>• Generic Win/DOS Executable (2004/3) 0.01% |
| File name: | SKGCTMGCarta2021070151637446689334 3426doc.exe |
| File size: | 972288 |
| MD5: | 0eb0833449cec388f8157458fc600691 |
| SHA1: | 63c969feee64e6fe65d289fbbdf6e2c971f8878b |
| SHA256: | 945ab6b146dc530e61824b8ccdd396c6c5d84c9537736db859771b1ee2dd93fe |
| SHA512: | ee4ae72defe8e6e163523fe9175911af7eee9fdf2ef086c16f699b51d08d98ebd9104d3fc6310922f7b729850f878c595319d2e89629c4af798c267dab28f1c7 |
| SSDEEP: | 24576:wgpLmQvDB9Ep2nb+B8NJar5e/A82vMfjYOk:XJbTN8r8FOGS |
| File Content Preview: | MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L.....`.....P.....v.... .....@.. .....@.....@..... |

## File Icon

| | |
|---|---|
| Icon Hash: | 00828e8e8686b000 |

## Static PE Info

### General

| | |
|---|---|
| Entrypoint: | 0x4ee876 |
| 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: | 0x60F70F88 [Tue Jul 20 18:01:44 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 | 0xec87c | 0xeca00 | False | 0.651589532158 | data | 7.34236226121 | IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ |
| .rsrc | 0xf0000 | 0x624 | 0x800 | False | 0.3330078125 | data | 3.46462032748 | IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ |
| .reloc | 0xf2000 | 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

# Code Manipulations

# Statistics

## Behavior

Click to jump to process

# System Behavior

## Analysis Process: SKGCTMGCarta2021070151637446689334426doc.exe PID: 6916 Parent PID: 5944

### General

| | |
|---|---|
| Start time: | 20:53:08 |
| Start date: | 20/07/2021 |
| Path: | C:\Users\user\Desktop\SKGCTMGCarta2021070151637446689334426doc.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Users\user\Desktop\SKGCTMGCarta2021070151637446689334426doc.exe' |
| Imagebase: | 0x4a0000 |
| File size: | 972288 bytes |
| MD5 hash: | 0EB0833449CEC388F8157458FC600691 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | .Net C# or VB.NET |
| Reputation: | low |

### File Activities

Show Windows behavior

#### File Created

#### File Deleted

#### File Written

#### File Read

## Analysis Process: schtasks.exe PID: 6772 Parent PID: 6916

### General

| | |
|---|---|
| Start time: | 20:53:41 |
| Start date: | 20/07/2021 |
| Path: | C:\Windows\SysWOW64\schtasks.exe |
| Wow64 process (32bit): | true |
| Commandline: | 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\sNlYazJXiEQfkP' /XML 'C:\Users\user\AppData\Local\Temp\tmp1ACF.tmp' |
| Imagebase: | 0xb30000 |
| 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: 6472 Parent PID: 6772

### General

| | |
|---|---|
| Start time: | 20:53:41 |
| Start date: | 20/07/2021 |
| 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: MSBuild.exe PID: 6436 Parent PID: 6916

### General

| | |
|---|---|
| Start time: | 20:53:42 |
| Start date: | 20/07/2021 |
| Path: | C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe |
| Wow64 process (32bit): | true |
| Commandline: | C:\Windows\Microsoft.NET\Framework\v4.0.30319\MSBuild.exe |
| Imagebase: | 0x570000 |
| File size: | 261728 bytes |
| MD5 hash: | D621FD77BD585874F9686D3A76462EF1 |
| Has elevated privileges: | true |
| Has administrator privileges: | true |
| Programmed in: | .Net C# or VB.NET |
| Yara matches: | • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.921988297.0000000006380000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.921988297.0000000006380000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.920719011.0000000005340000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.920719011.0000000005340000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.922327045.0000000006830000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.922327045.0000000006830000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.922004647.0000000006390000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.922004647.0000000006390000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.920503231.0000000005270000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.920503231.0000000005270000.00000004.00000001.sdmp, Author: Florian Roth<br>• Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.922224537.00000000064B0000.00000004.00000001.sdmp, Author: Florian Roth |

- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.922224537.00000000064B0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: NanoCore, Description: unknown, Source: 00000009.00000002.917951704.00000000039A1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.920917334.00000000053A0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.920917334.00000000053A0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: NanoCore, Description: unknown, Source: 00000009.00000002.918142857.0000000003BC2000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.920788480.0000000005350000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.920788480.0000000005350000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.920890999.0000000005380000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.920890999.0000000005380000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.916279377.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.916279377.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000009.00000002.916279377.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: NanoCore, Description: unknown, Source: 00000009.00000002.917459276.0000000002A0F000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.922204860.00000000064A0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.922204860.00000000064A0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.921932681.0000000006360000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.921932681.0000000006360000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.917875317.0000000003891000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.918281922.0000000003CD3000.00000004.00000001.sdmp, Author: Joe Security
- Rule: NanoCore, Description: unknown, Source: 00000009.00000002.918281922.0000000003CD3000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.920928559.00000000053B0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.920928559.00000000053B0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.920939322.00000000053C0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.920939322.00000000053C0000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000009.00000002.920939322.00000000053C0000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000009.00000002.921968807.0000000006370000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: Nanocore_RAT_Feb18_1, Description: Detects Nanocore RAT, Source: 00000009.00000002.921968807.0000000006370000.00000004.00000001.sdmp, Author: Florian Roth
- Rule: NanoCore, Description: unknown, Source: 00000009.00000002.918165301.0000000003BE8000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

| | |
|---|---|
| Reputation: | moderate |

## File Activities

Show Windows behavior

**File Created**

**File Written**

**File Read**

# Disassembly

## Code Analysis