ID: 458466
Sample Name: Racun.exe
Cookbook: default.jbs
Time: 11:51:37
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

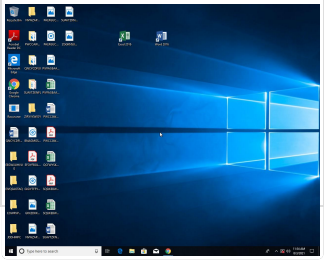
Windows Analysis Report Racun.exe

Overview

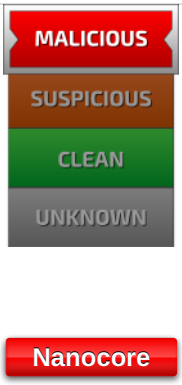
General Information

Sample Name:	Racun.exe
Analysis ID:	458466
MD5:	7f6faba18c6c6e9..
SHA1:	1043aede1c2c61..
SHA256:	8ca455b1943774..
Infos:	

Most interesting Screenshot:



Detection



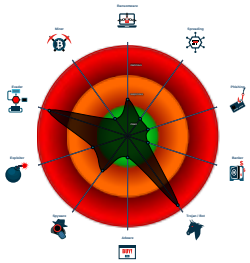
Nanocore

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

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Malicious sample detected (through …
- Sigma detected: NanoCore
- Snort IDS alert for network traffic (e.…
- Yara detected AntiVM3
- Yara detected Nanocore RAT
- .NET source code contains potentia…
- Adds a directory exclusion to Windo…
- C2 URLs / IPs found in malware con…
- Hides that the sample has been dow…
- Injects a PE file into a foreign proce…

Classification



Process Tree

- **System is w10x64**
- Racun.exe (PID: 2432 cmdline: 'C:\Users\user\Desktop\Racun.exe' MD5: 7F6FABA18C6C6E9962A95D02B5B3657C)
  - powershell.exe (PID: 68 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\Desktop\Racun.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 4692 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 4900 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\krPnoRdJhEnEq.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 5980 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6000 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\krPnoRdJhEnEq' /XML 'C:\Users\user\AppData\Local\Temp\tmp502C.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 4160 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 4872 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\krPnoRdJhEnEq.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 2408 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - Racun.exe (PID: 4840 cmdline: C:\Users\user\Desktop\Racun.exe MD5: 7F6FABA18C6C6E9962A95D02B5B3657C)
- dhcpmon.exe (PID: 6472 cmdline: 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: 7F6FABA18C6C6E9962A95D02B5B3657C)
  - powershell.exe (PID: 6888 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 6908 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - schtasks.exe (PID: 6916 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\krPnoRdJhEnEq' /XML 'C:\Users\user\AppData\Local\Temp\tmpA726.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6964 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - powershell.exe (PID: 7092 cmdline: 'C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe' Add-MpPreference -ExclusionPath 'C:\Users\user\AppData\Roaming\krPnoRdJhEnEq.exe' MD5: DBA3E6449E97D4E3DF64527EF7012A10)
    - conhost.exe (PID: 7120 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - dhcpmon.exe (PID: 7112 cmdline: C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe MD5: 7F6FABA18C6C6E9962A95D02B5B3657C)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "b90524a1-4a4b-41de-ac06-59066a86",
  "Group": "Panda",
  "Domain1": "emedoo.ddns.net",
  "Domain2": "127.0.0.1",
  "Port": 5230,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Disable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Enable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Enable",
  "EnableDebugMode": "Disable",
  "RunDelay": 50,
  "ConnectDelay": 4000,
  "RestartDelay": 5000,
  "TimeoutInterval": 5000,
  "KeepAliveTimeout": 30000,
  "MutexTimeout": 5000,
  "LanTimeout": 2500,
  "WanTimeout": 8000,
  "BufferSize": "ffff0000",
  "MaxPacketSize": "0000a000",
  "GCThreshold": "0000a000",
  "UseCustomDNS": "Enable",
  "PrimaryDNSServer": "emedoo.ddns.net",
  "BackupDNSServer": "8.8.4.44"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000D.00000002.468392842.000000000402000.00000040.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xff8d:$x1: NanoCore.ClientPluginHost • 0xffca:$x2: IClientNetworkHost • 0x13afd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0000000D.00000002.468392842.000000000402000.00000040.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0000000D.00000002.468392842.000000000402000.00000040.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfcf5:$a: NanoCore • 0xfd05:$a: NanoCore • 0xff39:$a: NanoCore • 0xff4d:$a: NanoCore • 0xff8d:$a: NanoCore • 0xfd54:$b: ClientPlugin • 0xff56:$b: ClientPlugin • 0xff96:$b: ClientPlugin • 0xfe7b:$c: ProjectData • 0x10882:$d: DESCrypto • 0x1824e:$e: KeepAlive • 0x1623c:$g: LogClientMessage • 0x12437:$i: get_Connected • 0x10bb8:$j: #=q • 0x10be8:$j: #=q • 0x10c04:$j: #=q • 0x10c34:$j: #=q • 0x10c50:$j: #=q • 0x10c6c:$j: #=q • 0x10c9c:$j: #=q • 0x10cb8:$j: #=q
00000018.00000002.330887870.000000000351000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	

Source	Rule	Description	Author	Strings
00000018.00000002.330887870.000000000351 1000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x238a7:$a: NanoCore • 0x23900:$a: NanoCore • 0x2393d:$a: NanoCore • 0x239b6:$a: NanoCore • 0x23909:$b: ClientPlugin • 0x23946:$b: ClientPlugin • 0x24244:$b: ClientPlugin • 0x24251:$b: ClientPlugin • 0x1b0f4:$e: KeepAlive • 0x23d91:$g: LogClientMessage • 0x23d11:$i: get_Connected • 0x158d9:$j: #=q • 0x15909:$j: #=q • 0x15945:$j: #=q • 0x1596d:$j: #=q • 0x1599d:$j: #=q • 0x159cd:$j: #=q • 0x159fd:$j: #=q • 0x15a2d:$j: #=q • 0x15a49:$j: #=q • 0x15a79:$j: #=q
Click to see the 21 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
24.2.dhcpmon.exe.3533ac8.2.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe75:$x1: NanoCore.ClientPluginHost • 0xe8f:$x2: IClientNetworkHost
24.2.dhcpmon.exe.3533ac8.2.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe75:$x2: NanoCore.ClientPluginHost • 0x1261:$s3: PipeExists • 0x1136:$s4: PipeCreated • 0xeb0:$s5: IClientLoggingHost
24.2.dhcpmon.exe.455e434.3.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xf7ad:$x1: NanoCore.ClientPluginHost • 0x28271:$x1: NanoCore.ClientPluginHost • 0xf7da:$x2: IClientNetworkHost • 0x2829e:$x2: IClientNetworkHost
24.2.dhcpmon.exe.455e434.3.raw.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xf7ad:$x2: NanoCore.ClientPluginHost • 0x28271:$x2: NanoCore.ClientPluginHost • 0x10888:$s4: PipeCreated • 0x2934c:$s4: PipeCreated • 0xf7c7:$s5: IClientLoggingHost • 0x2828b:$s5: IClientLoggingHost
24.2.dhcpmon.exe.455e434.3.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
Click to see the 34 entries				

Sigma Overview

AV Detection:

Sigma detected: NanoCore

E-Banking Fraud:

Sigma detected: NanoCore

System Summary:

Sigma detected: Powershell Defender Exclusion

Sigma detected: Non Interactive PowerShell

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

Yara detected Nanocore RAT

Machine Learning detection for dropped file

Machine Learning detection for sample

Networking:

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

C2 URLs / IPs found in malware configuration

Uses dynamic DNS services

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

Hooking and other Techniques for Hiding and Protection:

Hides that the sample has been downloaded from the Internet (zone.identifier)

Malware Analysis System Evasion:

Yara detected AntiVM3

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

HIPS / PFW / Operating System Protection Evasion:

Adds a directory exclusion to Windows Defender

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

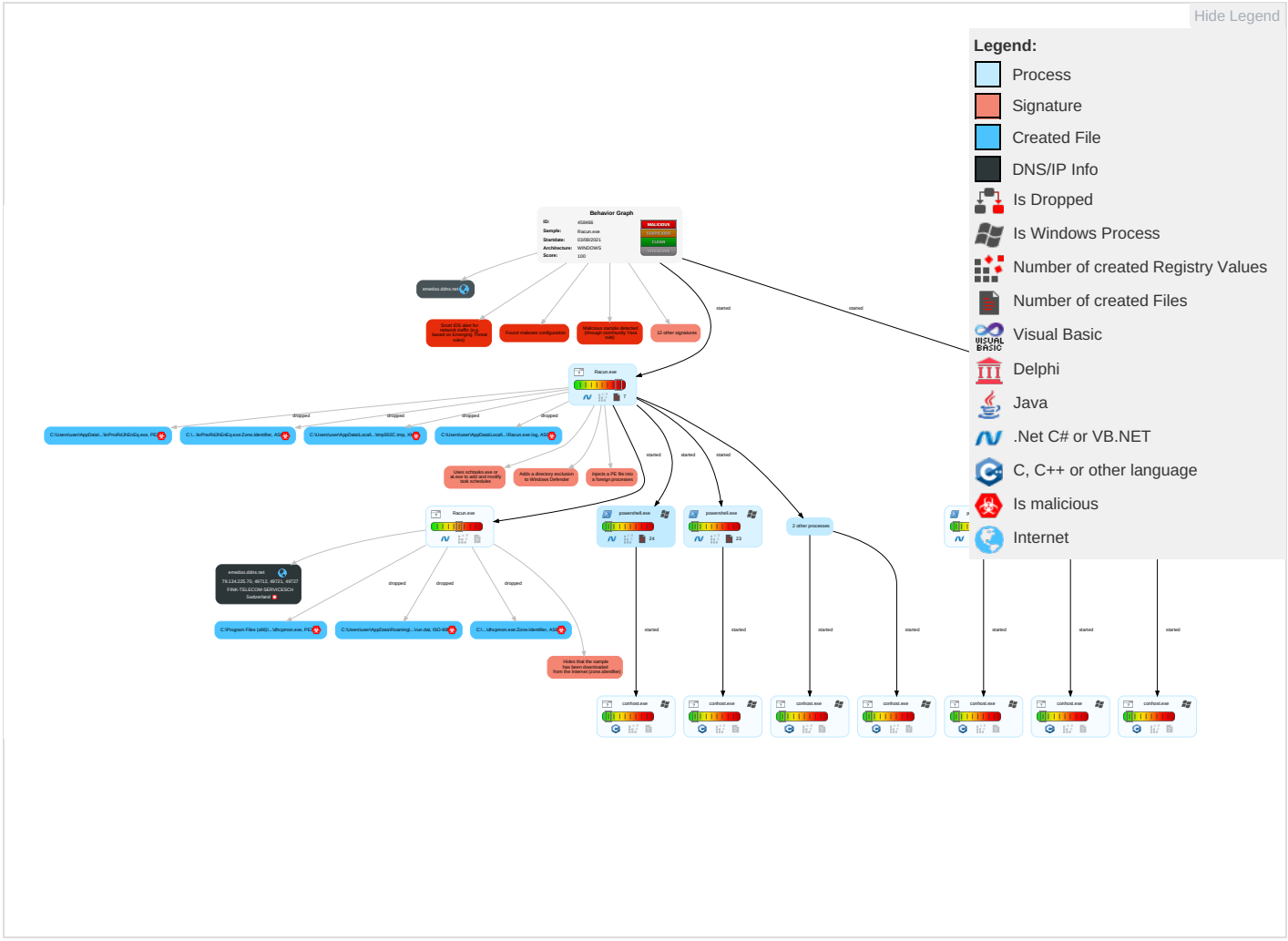
Detected Nanocore Rat

Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	C ar
Valid Accounts	Windows Management Instrumentation 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1 1	Input Capture 2 1	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	E C
Default Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Access Token Manipulation 1	Deobfuscate/Decode Files or Information 1	LSASS Memory	System Information Discovery 1 2	Remote Desktop Protocol	Input Capture 2 1	Exfiltration Over Bluetooth	N P
Domain Accounts	At (Linux)	Logon Script (Windows)	Process Injection 1 1 2	Obfuscated Files or Information 3	Security Account Manager	Query Registry 1	SMB/Windows Admin Shares	Data from Network Shared Drive	Automated Exfiltration	R S
Local Accounts	At (Windows)	Logon Script (Mac)	Scheduled Task/Job 1	Software Packing 1 3	NTDS	Security Software Discovery 1 2 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	N A L P
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Timestomp 1	LSA Secrets	Process Discovery 2	SSH	Keylogging	Data Transfer Size Limits	A L P
Replication Through Removable Media	Launchd	Rc.common	Rc.common	DLL Side-Loading 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	M C
External Remote Services	Scheduled Task	Startup Items	Startup Items	Masquerading 2	DCSync	Application Window Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	C U
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 3 1	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	A L
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Access Token Manipulation 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	W
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Process Injection 1 1 2	Network Sniffing	Process Discovery	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfuscated Non-C2 Protocol	Fi P
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Hidden Files and Directories 1	Input Capture	Permission Groups Discovery	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium	M

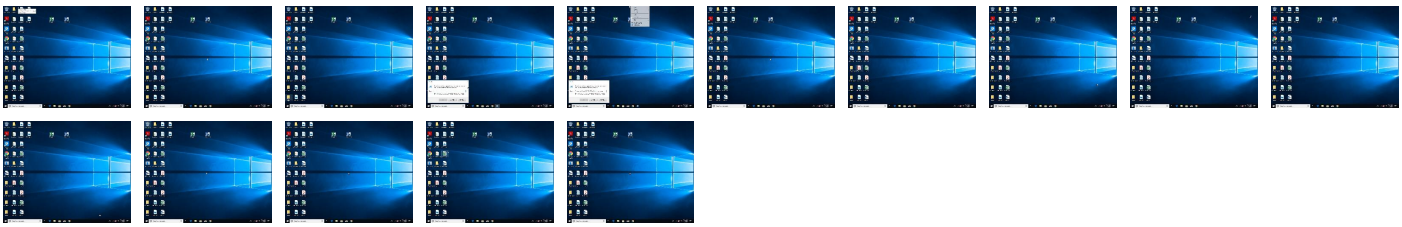
Behavior Graph



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
Racun.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\krPnoRdJhEnEq.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
13.2.Racun.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File
24.2.dhcpmon.exe.400000.0.unpack	100%	Avira	TR/Dropper.MSIL.Gen7		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.carterandcone.com.12	0%	Avira URL Cloud	safe	
http://www.fontbureau.commam	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/G	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://crl._	0%	Avira URL Cloud	safe	
http://www.fontbureau.comessed	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.fontbureau.comL.TTF8	0%	Avira URL Cloud	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.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.zhongyicts.com.cn#	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp//	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.carterandcone.comuct	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://crl.microsoft.cob	0%	Avira URL Cloud	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://crl.mE	0%	Avira URL Cloud	safe	
http://www.carterandcone.comG	0%	Avira URL Cloud	safe	
127.0.0.1	0%	Avira URL Cloud	safe	
http://www.fontbureau.comalsd	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://pesterbdd.com/images/Pester.png	0%	URL Reputation	safe	
http://www.carterandcone.comc	0%	URL Reputation	safe	
http://https://go.micro	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/L	0%	URL Reputation	safe	
http://www.carterandcone.comp	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/G	0%	URL Reputation	safe	
http://www.carterandcone.comItaw	0%	Avira URL Cloud	safe	
http://www.carterandcone.coms	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.fontbureau.comituF	0%	URL Reputation	safe	
http://www.fontbureau.comzanai	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/t	0%	URL Reputation	safe	
http://www.carterandcone.como.)	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/nl-n	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/r	0%	URL Reputation	safe	
http://www.monotype.	0%	URL Reputation	safe	
http://www.fontbureau.comm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/	0%	URL Reputation	safe	
http://www.fontbureau.como	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/i	0%	URL Reputation	safe	
emedoo.ddns.net	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnleaD	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/a	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
emedoo.ddns.net	79.134.225.70	true	false		high

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
127.0.0.1	true	• Avira URL Cloud: safe	unknown
emedoo.ddns.net	true	• Avira URL Cloud: safe	unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
79.134.225.70	emedoo.ddns.net	Switzerland		6775	FINK-TELECOM-SERVICESCH	false

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458466
Start date:	03.08.2021
Start time:	11:51:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 13m 15s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	Racun.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:	41
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.evad.winEXE@27/35@15/1
EGA Information:	• Successful, ratio: 75%
HDC Information:	• Successful, ratio: 0.3% (good quality ratio 0.3%) • Quality average: 74% • Quality standard deviation: 0%
HCA Information:	• Successful, ratio: 99% • 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
11:52:30	API Interceptor	690x Sleep call for process: Racun.exe modified
11:52:37	API Interceptor	222x Sleep call for process: powershell.exe modified
11:52:41	Autostart	Run: HKLM\Software\Microsoft\Windows\CurrentVersion\Run DHCP Monitor C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
11:52:52	API Interceptor	1x Sleep call for process: dhcpmon.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:\Program Files (x86)\DHCP Monitor\dhcpmon.exe

Process:	C:\Users\user\Desktop\Racun.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	852480
Entropy (8bit):	7.459760955959544
Encrypted:	false
SSDEEP:	24576:KYaXL6QVZXprvFE/gc4QZ5lzofB/y9aq1:ymQXRtWg+Z4B/yv
MD5:	7F6FABA18C6C6E9962A95D02B5B3657C
SHA1:	1043AEDE1C2C61575BFD026048A8B2A7E143A68B
SHA-256:	8CA455B1943774DA30A1EE80B2CD11562AF3B69A9D4A0FE00E22294E422DE52E
SHA-512:	EDE8B6D2137BF17BF6AA5394AC5AE7DFAF41C10642A8B5ACB7DD8BC263CCEBF10A6CA1CE1324AB10F115CB124F9750F73CA2BDB3175C072D8D2E9A90ED20576
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....wd.....P..... ... .@.. .....`..... ..@.....H...O.... .....@.....,..... ..... ..H.....text..... ..... ..`.rsrc..... .....@..@.rel oc.....@.....@..B.....\|.....H.....d....8.....0.....(....(.....(.....o.....*.....(.....(.....(!.....("....(#....*N..(....o^... ($....*&..(%....*.s&.....s'.....s(.....s).....s*.....*....0.....~....o+....+..*.0.....~....o,....+..*.0.....~....o-....+..*.0.....~....o.....+..*.0.....~....o/....+..*.0..<.....~.....(0.....,!r...p.....(1...o2...s3.....~.....+..*.0.....

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier

Process:	C:\Users\user\Desktop\Racun.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped

C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe:Zone.Identifier	
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**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\Racun.exe.log	
Process:	C:\Users\user\Desktop\Racun.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	664
Entropy (8bit):	5.288448637977022
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10Ug+9Yz9t0U29hJ5g1B0U2ukyrFk70U2xANlW3ANv:MLF20NaL3z2p29hJ5g522rW2xAi3A9
MD5:	B1DB55991C3DA14E35249AEA1BC357CA
SHA1:	0DD2D91198FDEF296441B12F1A906669B279700C
SHA-256:	34D3E48321D5010AD2BD1F3F0B728077E4F5A7F70D66FA36B57E5209580B6BDC
SHA-512:	BE38A31888C9C2F8047FA9C99672CB985179D325107514B7500DDA9523AE3E1D20B45EACC4E6C8A5D096360D0FBB98A120E63F38FFE324DF8A0559F6890CC80
Malicious:	**true**
Reputation:	unknown
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Runtime.Remo#\35774dc3cd31b4550ab06c3354cf4ba5\System.Runtime.Remoting.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0_32\UsageLogs\dhcpmon.exe.log	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	664
Entropy (8bit):	5.288448637977022
Encrypted:	false
SSDEEP:	12:Q3LaJU20NaL10Ug+9Yz9t0U29hJ5g1B0U2ukyrFk70U2xANlW3ANv:MLF20NaL3z2p29hJ5g522rW2xAi3A9
MD5:	B1DB55991C3DA14E35249AEA1BC357CA
SHA1:	0DD2D91198FDEF296441B12F1A906669B279700C
SHA-256:	34D3E48321D5010AD2BD1F3F0B728077E4F5A7F70D66FA36B57E5209580B6BDC
SHA-512:	BE38A31888C9C2F8047FA9C99672CB985179D325107514B7500DDA9523AE3E1D20B45EACC4E6C8A5D096360D0FBB98A120E63F38FFE324DF8A0559F6890CC80
Malicious:	false
Reputation:	unknown
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System\1ffc437de59fb69ba2b865ffdc98ffd1\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\Microsoft.VisualBas#\cd7c74fce2a0eab72cd25cbe4bb61614\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Drawing\54d944b3ca0ea1188d700fbd8089726b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Windows.Forms\bd8d59c984c9f5f2695f64341115cdf0\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_32\System.Runtime.Remo#\35774dc3cd31b4550ab06c3354cf4ba5\System.Runtime.Remoting.ni.dll",0..

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Process:	C:\Windows\SysWOW64\WindowsPowerShell\v1.0\powershell.exe
File Type:	data
Category:	dropped
Size (bytes):	14734
Entropy (8bit):	4.993014478972177
Encrypted:	false
SSDEEP:	384:cBVoGIpN6KQkj2Wkjh4iUxtaKdROdBLNXp5nYoGib4J:cBV3IpNBQkj2Lh4iUxtaKdROdBLNZBYH
MD5:	8D5E194411E038C060288366D6766D3D
SHA1:	DC1A8229ED0B909042065EA69253E86E86D71C88
SHA-256:	44EEE632DEDFB83A545D8C382887DF3EE7EF551F73DD55FEDCDD8C93D390E31F
SHA-512:	21378D13D42FBFA573DE91C1D4282B03E0AA1317B0C37598110DC53900C6321DB2B9DF27B2816D6EE3B3187E54BF066A96DB9EC1FF47FF86FEA36282AB90636

C:\Users\user\AppData\Local\Microsoft\Windows\PowerShell\ModuleAnalysisCache	
Malicious:	false
Reputation:	unknown
Preview:	PSMODULECACHE.....<.e...Y...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PowerShellGet.psd1.....Uninstall-Module.....inmo..... ..fimo.....Install-Module.....New-ScriptFileInfo.....Publish-Module.....Install-Script.....Update-Script.....Find-Command.....Update-ModuleManifest.....Find- DscResource.....Save-Module.....Save-Script.....upmo.....Uninstall-Script.....Get-InstalledScript.....Update-Module.....Register-PSRepository.....Find-Scri pt.....Unregister-PSRepository.....pumo.....Test-ScriptFileInfo.....Update-ScriptFileInfo.....Set-PSRepository.....Get-PSRepository.....Get-InstalledModule.... ....Find-Module.....Find-RoleCapability.....Publish-Script.....<.e...T...C:\Program Files (x86)\WindowsPowerShell\Modules\PowerShellGet\1.0.0.1\PSModule.psm1*.. .....Install-Script.....Save-Module.....Publish-Module.....Find-Module.....Download-Package.....Update-Module....

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):	5.59678883750819
Encrypted:	false
SSDEEP:	384:btCDYIIXljgEENP4bA0cS0nqultI6DpaeQ99gtXcxm9T1MaPZlbAV7qWDu5ZBDIV:OkEES6Tqult1Fat8FRCOfwcVK
MD5:	C4DB21F11D7AD85EF63B4763FE40D9A4
SHA1:	60D582A45E9E3CEF192315E1F185E0068E75279F
SHA-256:	3B9E47B7AAFEAB6375A4C20809A6C07609691D203902192F0817DFCBB96CCF58
SHA-512:	AFB0833B9614A024345E56F12AFE846E49AAE7A7BC4F0AE771C1A63EC8D629305995213D9D1A991A0BF62E9BBAB312A8B9610462530ED2BAC7A0B4847F0B41B 6
Malicious:	false
Reputation:	unknown
Preview:	@...e.....u.....E.....@.....H.....<@.^.L."My...:<..... .Microsoft.PowerShell.ConsoleHostD.....fZve...F.....x.).....System.Managemen t.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.....Sy stem.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_evqcb1jw.i0j.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
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_h4wv1gl2.dkf.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
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_jmkelw32.rdp.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
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_jsseuiuk.n4q.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
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_kvwwukrm.qm0.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
Reputation:	unknown
Preview:	 1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_nt4syjdt.2h1.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

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_nt4syjdt.2h1.psm1	
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_q3egjga5.vop.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
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_tv0r0wjc.wxj.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
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_v0dzz0y5.dcj.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
Encrypted:	false
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651 A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ya0bad5d.20i.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
Encrypted:	false

C:\Users\user\AppData\Local\Temp__PSScriptPolicyTest_ya0bad5d.20i.ps1	
SSDEEP:	3:U:U
MD5:	C4CA4238A0B923820DCC509A6F75849B
SHA1:	356A192B7913B04C54574D18C28D46E6395428AB
SHA-256:	6B86B273FF34FCE19D6B804EFF5A3F5747ADA4EAA22F1D49C01E52DDB7875B4B
SHA-512:	4DFF4EA340F0A823F15D3F4F01AB62EAE0E5DA579CCB851F8DB9DFE84C58B2B37B89903A740E1EE172DA793A6E79D560E5F7F9BD058A12A280433ED6FA4651(A
Malicious:	false
Reputation:	unknown
Preview:	1

C:\Users\user\AppData\Local\Temp\tmp502C.tmp	
Process:	C:\Users\user\Desktop\Racun.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1646
Entropy (8bit):	5.191525492619861
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBF2tn:cbh47TlNQ//rydbz9I3YODOLNdq3I
MD5:	B62E01A019A73FBAF66E4BD96FA834C5
SHA1:	C38B63C1A277058A0B06648A2B2D9EDC9510C452
SHA-256:	B965418846F43E89EED656199789AD6F8BA768CF432033FD202005922BAF3980
SHA-512:	DC5CA5F0AFEFC48D016227C3195D7CAA1726F76F8DB54A672E3874788A6EE58EAE23146961C576531A4A3D2DF20AC914EC935C27852D3DBB697F1418BB70C3C
Malicious:	**true**
Reputation:	unknown
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\Local\Temp\tmpA726.tmp	
Process:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1646
Entropy (8bit):	5.191525492619861
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKBF2tn:cbh47TlNQ//rydbz9I3YODOLNdq3I
MD5:	B62E01A019A73FBAF66E4BD96FA834C5
SHA1:	C38B63C1A277058A0B06648A2B2D9EDC9510C452
SHA-256:	B965418846F43E89EED656199789AD6F8BA768CF432033FD202005922BAF3980
SHA-512:	DC5CA5F0AFEFC48D016227C3195D7CAA1726F76F8DB54A672E3874788A6EE58EAE23146961C576531A4A3D2DF20AC914EC935C27852D3DBB697F1418BB70C3C
Malicious:	false
Reputation:	unknown
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:\Users\user\Desktop\Racun.exe
File Type:	data
Category:	dropped
Size (bytes):	1624
Entropy (8bit):	7.024371743172393
Encrypted:	false
SSDEEP:	48:Ik/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrwfk/lCrw8:flC0llC0llC0llC0llC0llC08
MD5:	0D79388CEC6619D612C2088173BB6741
SHA1:	8A312E3198009C545D0CF3254572189D29A03EA7
SHA-256:	D7D423B23D932E306F3CCB2F7A984B7036A042C007A43FD655C6B57B960BB8DF

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\catalog.dat	
SHA-512:	53BB3E9263DFD746E7E8159466E220E6EC9D81E9D3F0E1D191E09CD511B7EB93B0BA65D13CE0C97C652ECD0F69BB991E6B1840F961BC65003C4DD7AA93EED 13
Malicious:	false
Reputation:	unknown
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.....&.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.....&.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.....&.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.....&.Gj.h\.3.A...5.x..&...i+..c(1.P..P.cLT...A.b.....4h...t.+..Z\.. .i.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\run.dat	
Process:	C:\Users\user\Desktop\Racun.exe
File Type:	ISO-8859 text, with no line terminators
Category:	dropped
Size (bytes):	8
Entropy (8bit):	3.0
Encrypted:	false
SSDEEP:	3:A4o8t:A4o8t
MD5:	8DD02FB5965ED0552899B0778CF85C0A
SHA1:	808948E10ED0B3D4BCC528A90279F28D4AB7736A
SHA-256:	983C437BAD5CE49741CBA62D37B8E735921A1DC81E3A6087B8918A7A0339AD3B
SHA-512:	B3DB2B4C35C1E8A56087482CACDCDEC5FF2262C3B840A09EF60778326A76F1CDDC941B06B59EE4944556ACD2D9A3B360D38F4492099DDDDCD3B217B8472AF 0F
Malicious:	**true**
Reputation:	unknown
Preview:	.SR.V.H

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bak	
Process:	C:\Users\user\Desktop\Racun.exe
File Type:	data
Category:	modified
Size (bytes):	24
Entropy (8bit):	4.501629167387823
Encrypted:	false
SSDEEP:	3:9bzY6oRDlvYk:RzWDl3
MD5:	ACD3FB4310417DC77FE06F15B0E353E6
SHA1:	80E7002E655EB5765FDEB21114295CB96AD9D5EB
SHA-256:	DC3AE604991C9BB8FF8BC4502AE3D0DB8A3317512C0F432490B103B89C1A4368
SHA-512:	DA46A917DB6276CD4528CFE4AD113292D873CA2EBE53414730F442B83502E5FAF3D1AE87BFA295ADF01E3B44FDBCE239E21A318BFB2CCD1F4753846CB21F6F 97
Malicious:	false
Reputation:	unknown
Preview:	9iH...}Z.4..f..J".C;"a

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\settings.bin	
Process:	C:\Users\user\Desktop\Racun.exe
File Type:	data
Category:	dropped
Size (bytes):	64
Entropy (8bit):	5.320159765557392
Encrypted:	false
SSDEEP:	3:9bzY6oRDlvYVsRLY6oRDT6P2bfVn1:RzWDlfRWDT621
MD5:	BB0F9B9992809E733EFFF8B0E562CFD6
SHA1:	F0BAB3CF73A04F5A689E6AFC764FEE9276992742
SHA-256:	C48F04FE7525AA3A3F9540889883F649726233DE021724823720A59B4F37CEAC
SHA-512:	AE4280AA460DC1C0301D458A3A443F6884A0BE37481737B2ADAFD72C33C55F09BED88ED239C91FE6F19CA137AC3CD7C9B8454C21D3F8E759687F701C8B3C7A 6
Malicious:	false
Reputation:	unknown
Preview:	9iH...}Z.4..f..J".C;"a9iH...}Z.4..f.~a.....~.~.....3.U.

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Process:	C:\Users\user\Desktop\Racun.exe
File Type:	data

C:\Users\user\AppData\Roaming\D06ED635-68F6-4E9A-955C-4899F5F57B9A\storage.dat	
Category:	dropped
Size (bytes):	426840
Entropy (8bit):	**7.999608491116724**
Encrypted:	**true**
SSDEEP:	12288:zKf137EiDsTjevgA4p0V7njXuWSvdVU7V4OC0Rr:+134i2lp67i5d8+OCg
MD5:	963D5E2C9C0008DFF05518B47C367A7F
SHA1:	C183D601FABBC9AC8FBFA0A0937DECC677535E74
SHA-256:	5EACF2974C9BB2C2E24CDC651C4840DD6F4B76A98F0E85E90279F1DBB2E6F3C0
SHA-512:	0C04E1C1A13070D48728D9F7F300D9B26DEC6EC8875D8D3017EAD52B9EE5BDF9B651A7F0FCC537761212831107646ED72B8ED017E7477E600BC0137EF857AE2
Malicious:	false
Reputation:	unknown
Preview:	..g&jo...IPg...GM....R>i...o...I.>.&.r{....8...}...E....v.!7.u3e.. .....db...}.....".t(.xC9.cp.B....7...'.....%.....w.^.._.....B.W%.<..i.0.{9.xS...5...)..w..$..C..?`F..u.5.T.X.w'Si..z.n{...Y!m. ..RA...xg....[7...z..9@.K.-...T..+.ACe....R....enO.....AoNMT.\^....}H&..4I...B.:..@..J...v..rI5..kP.....2j....B..B.~.T..>.c..emW;Rn<9..[.r.o....R[....@=...:...L.g<.....I..%4[.G^.~.I'.....v .p&.....+..S...9d/.{..H.`@.1.....f.\s...X.a.].<.h*...J4*...k.x....%3.....3.c..?%....>.!.}..)(.{...H...3..`].Q.[sN..JX(.%pH....+.....(...v.....H...3..8.a_..J..?4...y.N(..D.*h..g.jD..I...44 Q?..N.....oX.A.....I...n?./.....$.!.;.^9"H.....*...OkF....v.m_.e.v..f...".bq{.....O.-....%R+...-..P.i..t5....2Z# ...#...,L..{..j..heT -=Z.P;...g.m)<owJ].J..../.p..8.u8.&..#.m9...j%..g&... .g.x.I,....u.[....>./W.....*X...b*Z...ex.0..x.}.....Tb...[..H_M._.^N.d&...g._."@4N.pDs].GbT.....&p.....Nw...%$=.....{..J.1....2....<E{..<!G..

C:\Users\user\AppData\Roaming\krPnoRdJhEnEq.exe	
Process:	C:\Users\user\Desktop\Racun.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	852480
Entropy (8bit):	7.459706955959544
Encrypted:	false
SSDEEP:	24576:KYaXL6QVZXprvFE/gc4QZ5lzofB/y9aq1:ymQXRtWg+Z4B/yv
MD5:	7F6FABA18C6C6E9962A95D02B5B3657C
SHA1:	1043AEDE1C2C61575BFD026048A8B2A7E143A68B
SHA-256:	8CA455B1943774DA30A1EE80B2CD11562AF3B69A9D4A0FE00E22294E422DE52E
SHA-512:	EDE8B6D2137BF17BF6AA5394AC5AE7DFAF41C10642A8B5ACB7DD8BC263CCEBF10A6CA1CE1324AB10F115CB124F9750F73CA2BDB3175C072D8D2E9A90ED20 576
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	unknown
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....wd.....P..... ... .@.. .....`..... ..@.....H...O.... .....@..... ..... ..H.....text..... ..... ..`.rsrc..... .....@..@.rel oc.....@.....@..B.....\|.....H.....d....8.....0.....(....(.....(.....o.....*.....(.....(.....(!.....("..... (#....*N..(....o^... ($....*&..(%....*.s&.....s'.....s(.....s).....s*.....*....0.....~....o+....+..*.0.....~....o,....+..*.0.....~....o-....+..*.0.....~....o.....+..*.0.....~....o/....+..*.0..<.....~.....(0.....,!r...p.....(1...o2...s3.....~.....+..*.0.....

C:\Users\user\AppData\Roaming\krPnoRdJhEnEq.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\Racun.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**
Reputation:	unknown
Preview:	[ZoneTransfer]....ZoneId=0

C:\Users\user\Documents\20210803\PowerShell_transcript.585948.Fn2R7YVg.20210803115303.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):	5801
Entropy (8bit):	5.404261003263462
Encrypted:	false
SSDEEP:	96:BZHhTNZqDo1ZEZjhTNZqDo1ZDHBvjZshTNZqDo1Zmu//lZO:+
MD5:	32A1B7CD6A17CF6DE96441F35CBFD0A0

C:\Users\user\Documents\20210803\PowerShell_transcript.585948.Fn2R7YVg.20210803115303.txt	
SHA1:	177212929421F269E731B699267FF399258C3652
SHA-256:	B2CC038DF3CCA22DB5F6C3DBF90C7E0F21C616B7078B34C86C6AA221CE5795F3
SHA-512:	A9412C726321E50F39B76D49921B77FA5EC02926A3DD79D0AD9270F839A0355C9F50628706F42A19F169BE2D4FFBE3DB77F0DE48A6C3BC7E5306804777C857BE
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210803115305..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 585948 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\krPnoRdJhEnEq.exe..Process ID: 7092..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: 20210803115305..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\krPnoRdJhEnEq.exe..**********..Windows PowerShell transcript start..Start time: 20210803115741..Username: computer\user..RunAs User: DESKTOP-716T77

C:\Users\user\Documents\20210803\PowerShell_transcript.585948.Uu720rWo.20210803115233.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):	5647
Entropy (8bit):	5.39228524106385
Encrypted:	false
SSDEEP:	96:BZGhTNsaqDo1ZO1ZRAShTNsaqDo1ZkQN2NINjZlhTNsaqDo1ZfvNYNYNvZo:x9+pmkCOW66g
MD5:	2C80E41ACFEED35A55E0E60911FC4F6B
SHA1:	415C054CAC25B4B4EB99CA83E5FC9F6F6C6C1383
SHA-256:	85A3B82A932536F564579F9BB8960289063DF828FF9820599260BDAC6FFA175A
SHA-512:	E30309118925C70ABE3C40EAA8AE78D13524FA04C52C75AB9DF82704D77A0B4792CF1680849A4BE0D498F4E598A089B6203F7DEFED6BE3599CECCA387EA88F5
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210803115256..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 585948 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\Desktop\Racun.exe..Process ID: 68..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: 20210803115257..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\Desktop\Racun.exe..**********..Windows PowerShell transcript start..Start time: 20210803115927..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Mac

C:\Users\user\Documents\20210803\PowerShell_transcript.585948.bJK7qKO_.20210803115236.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):	5801
Entropy (8bit):	5.406401782940296
Encrypted:	false
SSDEEP:	96:BZVhTNCqDo1ZWZ7ShTNCqDo1ZwHBvjZVhTNCqDo1Zlu//9Zu:RP
MD5:	A92FBFAE984CD659894991413344 8D12
SHA1:	7342017672FBE02985F5DE966FFF7BC63B61C96E
SHA-256:	E76EFC5B5F4A8A572FAF9A95A29EFD74E84BFF6DFD2C02C98B92A6A4292055C0
SHA-512:	9A9F3E287AD54B8A5AB735A0BE81625932BD92508EC98EB642C9A6973C89BDEFD56DEFD92DE7824065852230F072D8DD6B80B21D351A595CB15DCC68E2C224E
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210803115237..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 585948 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\krPnoRdJhEnEq.exe..Process ID: 4872..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: 20210803115237..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\krPnoRdJhEnEq.exe..**********..Windows PowerShell transcript start..Start time: 20210803115627..Username: computer\user..RunAs User: DESKTOP-716T77

C:\Users\user\Documents\20210803\PowerShell_transcript.585948.hfjwuezP.20210803115257.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):	3691
Entropy (8bit):	5.226276031434914
Encrypted:	false
SSDEEP:	96:BZbhTNLqDo1ZwZhhTNLqDo1Z9lzvOzGMzGMzwNZr:8vyGgGgwr
MD5:	CFFCDE7B591A5DF6A3DA74ABD03D8F67

C:\Users\user\Documents\20210803\PowerShell_transcript.585948.hfjwuezP.20210803115257.txt	
SHA1:	520175D582B95BF00FFE4F0D4B02B33423FF0F36
SHA-256:	6F77FDFAC3031D9669D238F8ED662FCBAECD142440C5E2934A9B5AAB34AC0EE5
SHA-512:	E92E4B22F762C070E9C41582369A1DF86A288D101C4216AD02477DD218A22F41CAE7897CAA6833D46F9680D30FA2C371AF0CAED2409A87FA563639B344D7EA3
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210803115301..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 585948 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe..Process ID: 6888..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: 20210803115301..**********..PS>Add-MpPreference -ExclusionPath C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe..**********..Windows PowerShell transcript start..Start time: 20210803115710..Username: computer\user..RunAs User: co mputer\

C:\Users\user\Documents\20210803\PowerShell_transcript.585948.jZDlUhwj.20210803115237.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):	5801
Entropy (8bit):	5.403322387278719
Encrypted:	false
SSDEEP:	96:BZkhTNcqDo1ZyZ2hTNcqDo1ZUHBvjZThTNcqDo1Zwu//hZO:r
MD5:	D36D6A5ABD17FEE7329D7AFF7FB264AA
SHA1:	18D1510106D86CCC2A914D57DCA9FF9191EC177C
SHA-256:	8912FC1FA57B1765B48BD88E59469919ECD2E89BD7D89193B7327F87520A7D3C
SHA-512:	4E4F34F458C883E87B38A7660F09AC636FE37EA27D493F9A7E804DFA728898F82056BCD64D4A3569BA88F4CB94F311C82859BA701C7DEEA580D2ECF152016EC
Malicious:	false
Reputation:	unknown
Preview:	.**********..Windows PowerShell transcript start..Start time: 20210803115302..Username: computer\user..RunAs User: computer\user..Configuration Name: ..Machine: 585948 (Microsoft Windows NT 10.0.17134.0)..Host Application: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe Add-MpPreference -ExclusionPath C:\Users\user\AppData\Roaming\krPnoRdJhEnEq.exe..Process ID: 4900..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: 20210803115303..**********..PS>Add-MpPreference -ExclusionPath C:\Users\user\App Data\Roaming\krPnoRdJhEnEq.exe..**********..Windows PowerShell transcript start..Start time: 20210803115955..Username: computer\user..RunAs User: DE SKTOP-716T77

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assemb ly, for MS Windows
Entropy (8bit):	7.459706955959544
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	Racun.exe
File size:	852480
MD5:	7f6faba18c6c6e9962a95d02b5b3657c
SHA1:	1043aede1c2c61575bfd026048a8b2a7e143a68b
SHA256:	8ca455b1943774da30a1ee80b2cd11562af3b69a9d4a0fe 00e22294e422de52e
SHA512:	ede8b6d2137bf17bf6aa5394ac5ae7dfaf41c10642a8b5a cb7dd8bc263ccebf10a6ca1ce1324ab10f115cb124f9750 f73ca2bdb3175c072d8d2e9a90ed208576
SSDEEP:	24576:KYaXL6QVZXprvFE/gc4QZ5lzofB/y9aq1:ymQX RtWg+Z4B/yv
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....PE..L.... wd.....P..... ... .@.. .....`..... ..@.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4d179a
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:	0xB66477BC [Mon Dec 20 02:26:04 2066 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v2.0.50727
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	0xcf7a0	0xcf800	False	0.793449971762	data	7.46711457835	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0xd2000	0x5cc	0x600	False	0.426432291667	data	4.12264452256	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xd4000	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

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
08/03/21-11:52:44.010631	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49712	5230	192.168.2.3	79.134.225.70
08/03/21-11:52:51.873778	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49721	5230	192.168.2.3	79.134.225.70
08/03/21-11:53:05.361853	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49728	5230	192.168.2.3	79.134.225.70
08/03/21-11:53:18.166590	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49730	5230	192.168.2.3	79.134.225.70
08/03/21-11:53:27.636611	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49731	5230	192.168.2.3	79.134.225.70
08/03/21-11:53:34.430829	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49734	5230	192.168.2.3	79.134.225.70

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
08/03/21-11:53:43.680020	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49741	5230	192.168.2.3	79.134.225.70
08/03/21-11:53:51.207234	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49742	5230	192.168.2.3	79.134.225.70
08/03/21-11:53:58.083149	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49743	5230	192.168.2.3	79.134.225.70
08/03/21-11:54:04.668916	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49745	5230	192.168.2.3	79.134.225.70
08/03/21-11:54:11.157299	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49747	5230	192.168.2.3	79.134.225.70
08/03/21-11:54:17.780323	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49748	5230	192.168.2.3	79.134.225.70
08/03/21-11:54:25.169768	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49749	5230	192.168.2.3	79.134.225.70
08/03/21-11:54:32.964830	TCP	2025019	ET TROJAN Possible NanoCore C2 60B	49750	5230	192.168.2.3	79.134.225.70

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Aug 3, 2021 11:52:43.397562981 CEST	192.168.2.3	8.8.4.4	0x83e	Standard query (0)	emedoo.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 11:52:51.491636038 CEST	192.168.2.3	8.8.4.4	0x5345	Standard query (0)	emedoo.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 11:52:58.823179007 CEST	192.168.2.3	8.8.4.4	0x2035	Standard query (0)	emedoo.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 11:53:05.036528111 CEST	192.168.2.3	8.8.4.4	0x7f8a	Standard query (0)	emedoo.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 11:53:17.450695038 CEST	192.168.2.3	8.8.4.4	0x40c3	Standard query (0)	emedoo.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 11:53:27.358979940 CEST	192.168.2.3	8.8.4.4	0x614e	Standard query (0)	emedoo.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 11:53:34.272722006 CEST	192.168.2.3	8.8.4.4	0xa183	Standard query (0)	emedoo.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 11:53:43.341921091 CEST	192.168.2.3	8.8.4.4	0x793e	Standard query (0)	emedoo.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 11:53:51.031640053 CEST	192.168.2.3	8.8.4.4	0x1c50	Standard query (0)	emedoo.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 11:53:57.847381115 CEST	192.168.2.3	8.8.4.4	0xc870	Standard query (0)	emedoo.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 11:54:04.517573118 CEST	192.168.2.3	8.8.4.4	0x2292	Standard query (0)	emedoo.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 11:54:10.996125937 CEST	192.168.2.3	8.8.4.4	0xd2cd	Standard query (0)	emedoo.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 11:54:17.477345943 CEST	192.168.2.3	8.8.4.4	0x9e77	Standard query (0)	emedoo.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 11:54:24.922684908 CEST	192.168.2.3	8.8.4.4	0xe8d5	Standard query (0)	emedoo.ddns.net	A (IP address)	IN (0x0001)
Aug 3, 2021 11:54:32.802740097 CEST	192.168.2.3	8.8.4.4	0x12bb	Standard query (0)	emedoo.ddns.net	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 11:52:43.436129093 CEST	8.8.4.4	192.168.2.3	0x83e	No error (0)	emedoo.ddns.net		79.134.225.70	A (IP address)	IN (0x0001)
Aug 3, 2021 11:52:51.527358055 CEST	8.8.4.4	192.168.2.3	0x5345	No error (0)	emedoo.ddns.net		79.134.225.70	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Aug 3, 2021 11:52:58.855978012 CEST	8.8.4.4	192.168.2.3	0x2035	No error (0)	emedoo.ddns.net		79.134.225.70	A (IP address)	IN (0x0001)
Aug 3, 2021 11:53:05.061229944 CEST	8.8.4.4	192.168.2.3	0x7f8a	No error (0)	emedoo.ddns.net		79.134.225.70	A (IP address)	IN (0x0001)
Aug 3, 2021 11:53:17.477427959 CEST	8.8.4.4	192.168.2.3	0x40c3	No error (0)	emedoo.ddns.net		79.134.225.70	A (IP address)	IN (0x0001)
Aug 3, 2021 11:53:27.393717051 CEST	8.8.4.4	192.168.2.3	0x614e	No error (0)	emedoo.ddns.net		79.134.225.70	A (IP address)	IN (0x0001)
Aug 3, 2021 11:53:34.308175087 CEST	8.8.4.4	192.168.2.3	0xa183	No error (0)	emedoo.ddns.net		79.134.225.70	A (IP address)	IN (0x0001)
Aug 3, 2021 11:53:43.385349989 CEST	8.8.4.4	192.168.2.3	0x793e	No error (0)	emedoo.ddns.net		79.134.225.70	A (IP address)	IN (0x0001)
Aug 3, 2021 11:53:51.067274094 CEST	8.8.4.4	192.168.2.3	0x1c50	No error (0)	emedoo.ddns.net		79.134.225.70	A (IP address)	IN (0x0001)
Aug 3, 2021 11:53:57.881127119 CEST	8.8.4.4	192.168.2.3	0xc870	No error (0)	emedoo.ddns.net		79.134.225.70	A (IP address)	IN (0x0001)
Aug 3, 2021 11:54:04.546205044 CEST	8.8.4.4	192.168.2.3	0x2292	No error (0)	emedoo.ddns.net		79.134.225.70	A (IP address)	IN (0x0001)
Aug 3, 2021 11:54:11.029992104 CEST	8.8.4.4	192.168.2.3	0xd2cd	No error (0)	emedoo.ddns.net		79.134.225.70	A (IP address)	IN (0x0001)
Aug 3, 2021 11:54:17.510871887 CEST	8.8.4.4	192.168.2.3	0x9e77	No error (0)	emedoo.ddns.net		79.134.225.70	A (IP address)	IN (0x0001)
Aug 3, 2021 11:54:24.959320068 CEST	8.8.4.4	192.168.2.3	0xe8d5	No error (0)	emedoo.ddns.net		79.134.225.70	A (IP address)	IN (0x0001)
Aug 3, 2021 11:54:32.841942072 CEST	8.8.4.4	192.168.2.3	0x12bb	No error (0)	emedoo.ddns.net		79.134.225.70	A (IP address)	IN (0x0001)

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: Racun.exe PID: 2432 Parent PID: 5640

General

Start time:	11:52:25
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\Racun.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\Racun.exe'
Imagebase:	0xc0000

File size:	852480 bytes
MD5 hash:	7F6FABA18C6C6E9962A95D02B5B3657C
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: 00000001.00000002.263923497.0000000009901000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000001.00000002.263923497.0000000009901000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000001.00000002.263923497.0000000009901000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000001.00000002.228985654.0000000002B63000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: powershell.exe PID: 68 Parent PID: 2432

General

Start time:	11:52:31
Start date:	03/08/2021
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\Racun.exe'
Imagebase:	0xa20000
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: 4692 Parent PID: 68

General

Start time:	11:52:32
Start date:	03/08/2021
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: powershell.exe PID: 4900 Parent PID: 2432

General

Start time:	11:52:32
Start date:	03/08/2021
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\AppData\Roaming\krPnoRdJhEnEq.exe'
Imagebase:	0xa20000
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: 5980 Parent PID: 4900

General

Start time:	11:52:32
Start date:	03/08/2021
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: 6000 Parent PID: 2432

General

Start time:	11:52:32
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\krPnoRdJhEnEq' /XML 'C:\Users\user\AppData\Local\Temp\tmp502C.tmp'
Imagebase:	0x330000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: conhost.exe PID: 4160 Parent PID: 6000

General

Start time:	11:52:33
Start date:	03/08/2021
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: powershell.exe PID: 4872 Parent PID: 2432

General

Start time:	11:52:34
Start date:	03/08/2021
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\AppData\Roaming\krPnoRdJhEnEq.exe'
Imagebase:	0xa20000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: conhost.exe PID: 2408 Parent PID: 4872

General

Start time:	11:52:34

Start date:	03/08/2021
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: Racun.exe PID: 4840 Parent PID: 2432

General

Start time:	11:52:34
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\Racun.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\Racun.exe
Imagebase:	0xc00000
File size:	852480 bytes
MD5 hash:	7F6FABA18C6C6E9962A95D02B5B3657C
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: 0000000D.00000002.468392842.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000D.00000002.468392842.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000D.00000002.468392842.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Reputation:	low

Analysis Process: dhcpmon.exe PID: 6472 Parent PID: 3388

General

Start time:	11:52:51
Start date:	03/08/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	'C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0xa10000
File size:	852480 bytes
MD5 hash:	7F6FABA18C6C6E9962A95D02B5B3657C
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: 0000000F.00000002.323593416.00000000035E3000.00000004.00000001.sdmp, Author: Joe Security • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 0000000F.00000002.356240180.0000000009DA1000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 0000000F.00000002.356240180.0000000009DA1000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 0000000F.00000002.356240180.0000000009DA1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
Antivirus matches:	• Detection: 100%, Joe Sandbox ML

Reputation:	low

Analysis Process: powershell.exe PID: 6888 Parent PID: 6472

General

Start time:	11:52:55
Start date:	03/08/2021
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:\Program Files (x86)\DHCP Monitor\dhcpmon.exe'
Imagebase:	0xa20000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Reputation:	high

Analysis Process: conhost.exe PID: 6908 Parent PID: 6888

General

Start time:	11:52:56
Start date:	03/08/2021
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

Analysis Process: schtasks.exe PID: 6916 Parent PID: 6472

General

Start time:	11:52:56
Start date:	03/08/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\krPnoRdJhEnEq' /XML 'C:\Users\user\AppData\Local\Temp\tmpA726.tmp'
Imagebase:	0x330000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language

Analysis Process: conhost.exe PID: 6964 Parent PID: 6916

General

Start time:	11:52:57
Start date:	03/08/2021
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

Analysis Process: powershell.exe PID: 7092 Parent PID: 6472

General

Start time:	11:52:58
Start date:	03/08/2021
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\AppData\Roaming\krPnoRdJhEnEq.exe'
Imagebase:	0xa20000
File size:	430592 bytes
MD5 hash:	DBA3E6449E97D4E3DF64527EF7012A10
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Analysis Process: dhcpmon.exe PID: 7112 Parent PID: 6472

General

Start time:	11:52:59
Start date:	03/08/2021
Path:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Wow64 process (32bit):	true
Commandline:	C:\Program Files (x86)\DHCP Monitor\dhcpmon.exe
Imagebase:	0xd30000
File size:	852480 bytes
MD5 hash:	7F6FABA18C6C6E9962A95D02B5B3657C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000018.00000002.330887870.0000000003511000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000018.00000002.330887870.0000000003511000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000018.00000002.331597779.0000000004511000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000018.00000002.331597779.0000000004511000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: Nanocore_RAT_Gen_2, Description: Detetcs the Nanocore RAT, Source: 00000018.00000002.312029557.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000018.00000002.312029557.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000018.00000002.312029557.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>

Analysis Process: conhost.exe PID: 7120 Parent PID: 7092

General

Start time:	11:52:59
Start date:	03/08/2021
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

Disassembly

Code Analysis