ID: 458308
Sample Name: RFQ CL-2021 - 0188 ROCKWELL LAND (WEVER).xls.exe
Cookbook: default.jbs
Time: 08:31:37
Date: 03/08/2021
Version: 33.0.0 White Diamond

Table of Contents

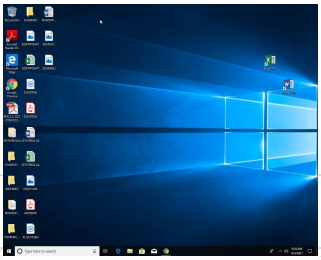
Windows Analysis Report RFQ CL-2021 - 0188 ROCKWE…

Overview

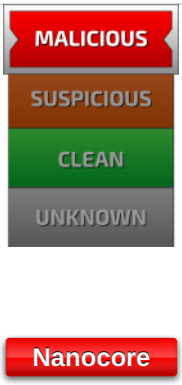
General Information

Sample Name:	RFQ CL-2021 - 0188 ROCKWELL LAND (WEVER).xls.exe
Analysis ID:	458308
MD5:	8c457878cc3c72…
SHA1:	8aad02989c92c4..
SHA256:	94dc3ceb75323f7..
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

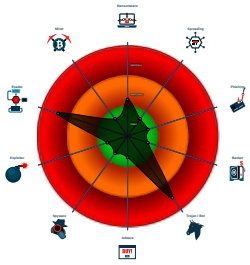


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Detected Nanocore Rat
- Found malware configuration
- Icon mismatch, binary includes an ic…
- Malicious sample detected (through …
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Suspicious Double …
- Yara detected AntiVM3
- Yara detected Nanocore RAT
- C2 URLs / IPs found in malware con…
- Machine Learning detection for dropp…
- Machine Learning detection for samp…

Classification



Process Tree

- **System is w10x64**
- RFQ CL-2021 - 0188 ROCKWELL LAND (WEVER).xls.exe (PID: 4328 cmdline: 'C:\Users\user\Desktop\RFQ CL-2021 - 0188 ROCKWELL LAND (WEVER).xls.exe' MD5: 8C457878CC3C72EA684D3034837101E0)
  - schtasks.exe (PID: 980 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\DCBdvFPc' /XML 'C:\Users\user\AppData\Local\Temp\tmp5F10.tmp' MD5: 838D346D1D28F00783B7A6C6BD03A0DA)
    - conhost.exe (PID: 5600 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - RFQ CL-2021 - 0188 ROCKWELL LAND (WEVER).xls.exe (PID: 3528 cmdline: C:\Users\user\Desktop\RFQ CL-2021 - 0188 ROCKWELL LAND (WEVER).xls.exe MD5: 8C457878CC3C72EA684D3034837101E0)
  - RFQ CL-2021 - 0188 ROCKWELL LAND (WEVER).xls.exe (PID: 248 cmdline: C:\Users\user\Desktop\RFQ CL-2021 - 0188 ROCKWELL LAND (WEVER).xls.exe MD5: 8C457878CC3C72EA684D3034837101E0)
  - RFQ CL-2021 - 0188 ROCKWELL LAND (WEVER).xls.exe (PID: 5612 cmdline: C:\Users\user\Desktop\RFQ CL-2021 - 0188 ROCKWELL LAND (WEVER).xls.exe MD5: 8C457878CC3C72EA684D3034837101E0)
  - RFQ CL-2021 - 0188 ROCKWELL LAND (WEVER).xls.exe (PID: 1704 cmdline: C:\Users\user\Desktop\RFQ CL-2021 - 0188 ROCKWELL LAND (WEVER).xls.exe MD5: 8C457878CC3C72EA684D3034837101E0)
  - RFQ CL-2021 - 0188 ROCKWELL LAND (WEVER).xls.exe (PID: 4724 cmdline: C:\Users\user\Desktop\RFQ CL-2021 - 0188 ROCKWELL LAND (WEVER).xls.exe MD5: 8C457878CC3C72EA684D3034837101E0)
- **cleanup**

Malware Configuration

Threatname: NanoCore

```
{
  "Version": "1.2.2.0",
  "Mutex": "7547b95a-3564-48ed-9de2-e9e7593f",
  "Group": "ikenna",
  "Domain1": "194.5.98.127",
  "Domain2": "127.0.0.1",
  "Port": 54984,
  "KeyboardLogging": "Enable",
  "RunOnStartup": "Enable",
  "RequestElevation": "Disable",
  "BypassUAC": "Enable",
  "ClearZoneIdentifier": "Enable",
  "ClearAccessControl": "Enable",
  "SetCriticalProcess": "Disable",
  "PreventSystemSleep": "Enable",
  "ActivateAwayMode": "Enable",
  "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",
  "BypassUserAccountControlData": "<?xml version=\"1.0\" encoding=\"UTF-16\"?>\r\n<Task version=\"1.2\" xmlns=\"http://schemas.microsoft.com/windows/2004/02/mit/task\">\r\n
<RegistrationInfo />\r\n  <Triggers />\r\n  <Principals>\r\n    <Principal id=\"Author\">\r\n      <LogonType>InteractiveToken</LogonType>\r\n
<RunLevel>HighestAvailable</RunLevel>\r\n    </Principal>\r\n  </Principals>\r\n  <Settings>\r\n    <MultipleInstancesPolicy>Parallel</MultipleInstancesPolicy>\r\n
<DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>\r\n    <StopIfGoingOnBatteries>false</StopIfGoingOnBatteries>\r\n
<AllowHardTerminate>true</AllowHardTerminate>\r\n    <StartWhenAvailable>false</StartWhenAvailable>\r\n    <RunOnlyIfNetworkAvailable>false</RunOnlyIfNetworkAvailable>\r\n
<IdleSettings>\r\n      <StopOnIdleEnd>false</StopOnIdleEnd>\r\n      <RestartOnIdle>false</RestartOnIdle>\r\n    </IdleSettings>\r\n
<AllowStartOnDemand>true</AllowStartOnDemand>\r\n    <Enabled>true</Enabled>\r\n    <Hidden>false</Hidden>\r\n    <RunOnlyIfIdle>false</RunOnlyIfIdle>\r\n
<WakeToRun>false</WakeToRun>\r\n    <ExecutionTimeLimit>PT0S</ExecutionTimeLimit>\r\n    <Priority>4</Priority>\r\n  </Settings>\r\n  <Actions Context=\"Author\">\r\n
<Exec>\r\n      <Command>\"#EXECUTABLEPATH\"</Command>\r\n      <Arguments>$(Arg0)</Arguments>\r\n    </Exec>\r\n  </Actions>\r\n</Task"
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000000.00000002.263221894.000000001304A000.00000004.00000001.sdmp	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x183fbd:$x1: NanoCore.ClientPluginHost • 0x183ffa:$x2: IClientNetworkHost • 0x187b2d:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
00000000.00000002.263221894.000000001304A000.00000004.00000001.sdmp	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
00000000.00000002.263221894.000000001304A000.00000004.00000001.sdmp	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0x183d25:$a: NanoCore • 0x183d35:$a: NanoCore • 0x183f69:$a: NanoCore • 0x183f7d:$a: NanoCore • 0x183fbd:$a: NanoCore • 0x183d84:$b: ClientPlugin • 0x183f86:$b: ClientPlugin • 0x183fc6:$b: ClientPlugin • 0x183eab:$c: ProjectData • 0x2dd371:$c: ProjectData • 0x3d95a9:$c: ProjectData • 0x1848b2:$d: DESCrypto • 0x18c27e:$e: KeepAlive • 0x18a26c:$g: LogClientMessage • 0x186467:$i: get_Connected • 0xb22b6:$j: #=q • 0x184be8:$j: #=q • 0x184c18:$j: #=q • 0x184c34:$j: #=q • 0x184c64:$j: #=q • 0x184c80:$j: #=q
00000000.00000002.260617186.0000000002EC1000.00000004.00000001.sdmp	JoeSecurity_AntiVM_3	Yara detected AntiVM_3	Joe Security	
Process Memory Space: RFQ CL-2021 - 0188 ROCKWELL LAND (WEVER).xls.exe PID: 4328	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x9a19e:$x1: NanoCore.ClientPluginHost • 0x9a1db:$x2: IClientNetworkHost • 0x9d587:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe • 0xa820b:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe

Source	Rule	Description	Author	Strings
Click to see the 3 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
0.2.RFQ CL-2021 - 0188 ROCKWELL LAND (WE VER).xls.exe.131bde30.3.raw.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0x1018d:$x1: NanoCore.ClientPluginHost • 0x101ca:$x2: IClientNetworkHost • 0x13cfd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.2.RFQ CL-2021 - 0188 ROCKWELL LAND (WE VER).xls.exe.131bde30.3.raw.unpack	JoeSecurity_Nanocore	Yara detected Nanocore RAT	Joe Security	
0.2.RFQ CL-2021 - 0188 ROCKWELL LAND (WE VER).xls.exe.131bde30.3.raw.unpack	NanoCore	unknown	Kevin Breen <kevin@techanarchy.net>	• 0xfef5:$a: NanoCore • 0xff05:$a: NanoCore • 0x10139:$a: NanoCore • 0x1014d:$a: NanoCore • 0x1018d:$a: NanoCore • 0xff54:$b: ClientPlugin • 0x10156:$b: ClientPlugin • 0x10196:$b: ClientPlugin • 0x1007b:$c: ProjectData • 0x169541:$c: ProjectData • 0x265779:$c: ProjectData • 0x10a82:$d: DESCrypto • 0x1844e:$e: KeepAlive • 0x1643c:$g: LogClientMessage • 0x12637:$i: get_Connected • 0x10db8:$j: #=q • 0x10de8:$j: #=q • 0x10e04:$j: #=q • 0x10e34:$j: #=q • 0x10e50:$j: #=q • 0x10e6c:$j: #=q
0.2.RFQ CL-2021 - 0188 ROCKWELL LAND (WE VER).xls.exe.131bde30.3.unpack	Nanocore_RAT_Gen_2	Detetcs the Nanocore RAT	Florian Roth	• 0xe38d:$x1: NanoCore.ClientPluginHost • 0xe3ca:$x2: IClientNetworkHost • 0x11efd:$x3: #=qjgz7ljmpp0J7FvL9dmi8ctJILdgtcbw 8JYUc6GC8MeJ9B11Crfg2Djxcf0p8PZGe
0.2.RFQ CL-2021 - 0188 ROCKWELL LAND (WE VER).xls.exe.131bde30.3.unpack	Nanocore_RAT_Feb18_1	Detects Nanocore RAT	Florian Roth	• 0xe105:$x1: NanoCore Client.exe • 0xe38d:$x2: NanoCore.ClientPluginHost • 0xf9c6:$s1: PluginCommand • 0xf9ba:$s2: FileCommand • 0x1086b:$s3: PipeExists • 0x16622:$s4: PipeCreated • 0xe3b7:$s5: IClientLoggingHost
Click to see the 2 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicious Double Extension

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for dropped file

Multi AV Scanner detection for submitted 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)

Boot Survival:

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

Hooking and other Techniques for Hiding and Protection:

Icon mismatch, binary includes an icon from a different legit application in order to fool users

Uses an obfuscated file name to hide its real file extension (double extension)

Malware Analysis System Evasion:

Yara detected AntiVM3

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

Stealing of Sensitive Information:

Yara detected Nanocore RAT

Remote Access Functionality:

Detected Nanocore Rat

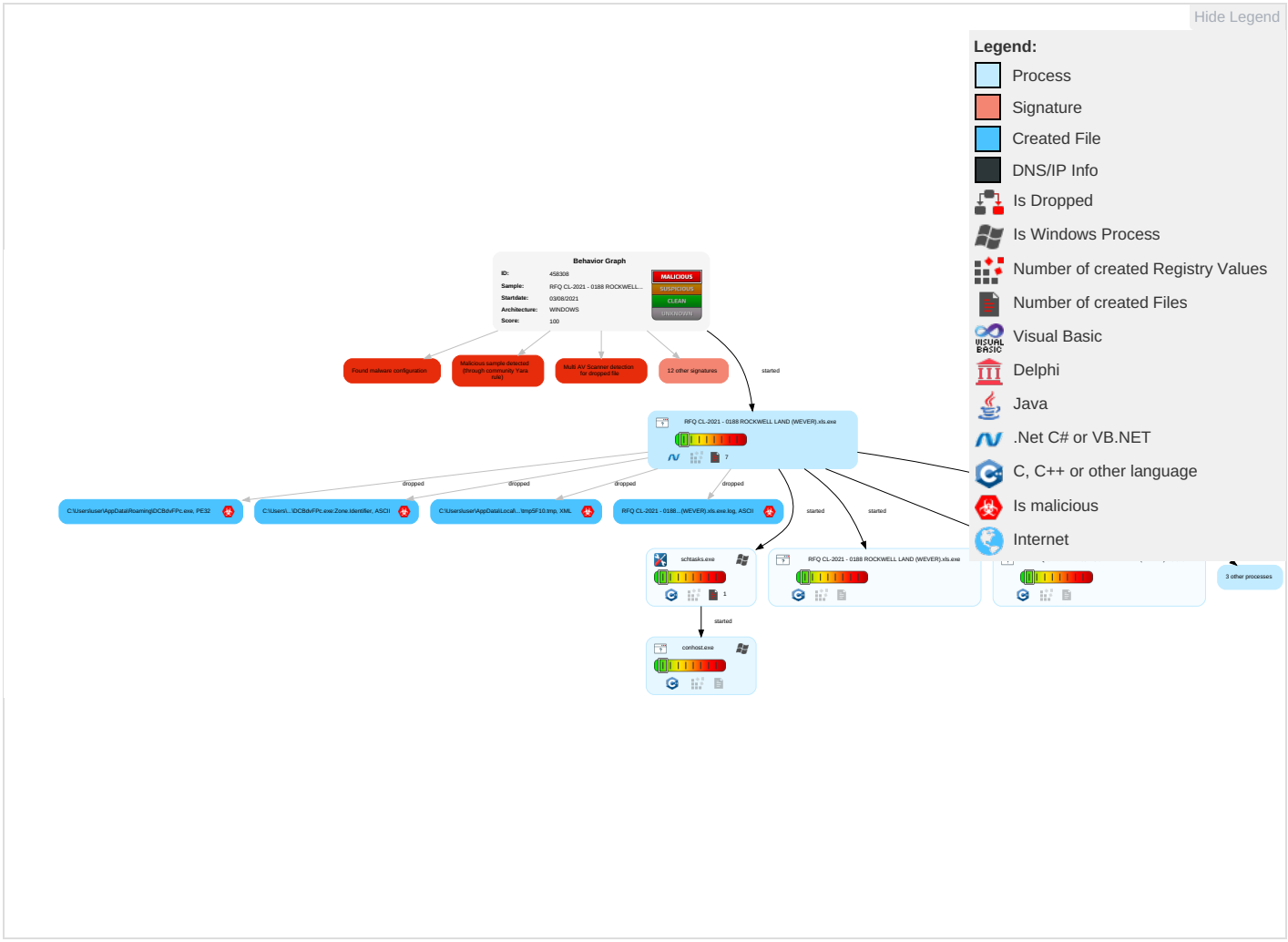
Yara detected Nanocore RAT

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Scheduled Task/Job 1	Scheduled Task/Job 1	Process Injection 1 1	Masquerading 2 1	OS Credential Dumping	Security Software Discovery 2 1	Remote Services	Archive Collected Data 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communication
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Scheduled Task/Job 1	Disable or Modify Tools 1	LSASS Memory	Process Discovery 1	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Bluetooth	Remote Access Software 1	Exploit SS7 to Redirect Phone Calls/SMS
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	Application Layer Protocol 1	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Process Injection 1 1	NTDS	File and Directory Discovery 1	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Obfuscated Files or Information 1 2	LSA Secrets	System Information Discovery 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communication

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Software Packing 2	Cached Domain Credentials	System Owner/User Discovery	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communication	Jamming or Denial of Service

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
RFQ CL-2021 - 0188 ROCKWELL LAND (WEVER).xls.exe	30%	Virustotal		Browse
RFQ CL-2021 - 0188 ROCKWELL LAND (WEVER).xls.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\DCBdvFPc.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\DCBdvFPc.exe	30%	ReversingLabs	ByteCode-MSIL.Trojan.Taskun	

Unpacked PE Files

No Antivirus matches

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
194.5.98.127	0%	Avira URL Cloud	safe	
127.0.0.1	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
194.5.98.127	true	• Avira URL Cloud: safe	unknown
127.0.0.1	true	• Avira URL Cloud: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	458308
Start date:	03.08.2021
Start time:	08:31:37
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 25s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	RFQ CL-2021 - 0188 ROCKWELL LAND (WEVER).xls.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:	25
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@14/4@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 14.1% (good quality ratio 9.5%) • Quality average: 38.2% • Quality standard deviation: 29.2%
HCA Information:	• Successful, ratio: 73% • 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
08:32:29	API Interceptor	1x Sleep call for process: RFQ CL-2021 - 0188 ROCKWELL LAND (WEVER).xls.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v2.0\UsageLogs\RFQ CL-2021 - 0188 ROCKWELL LAND (WEVER).xls.exe.log

Process:	C:\Users\user\Desktop\RFQ CL-2021 - 0188 ROCKWELL LAND (WEVER).xls.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	664
Entropy (8bit):	5.280979230295524
Encrypted:	false
SSDEEP:	12:Q3LaJcP0/9UkB9t0kaHYGLi1B01kKVdisk70OAEaANv:ML2pBLaYgioQxAfA9
MD5:	4F9B2B715AECAC008745D08674616098
SHA1:	C57514C4DD41B45672DA1B05D487E72D46F000AC
SHA-256:	E3A1D0AC3EC711220FADB6166C7C40078134ED136865BCB35DF2034091CB66A9
SHA-512:	4F26878A7FF989DF363B1E55614D856408C44B7F970AA725F1B7C1431D52A7793BFAA22F53897CCF7469E52615550B06FCDBC1A6D51CC5390B2C87FD8559037B
Malicious:	**true**
Reputation:	moderate, very likely benign file
Preview:	1,"fusion","GAC",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_64\System\1201f26cb986c93f55044bb4fa22b294\System.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_64\Microsoft.VisualBas#\76002c3c0a2b9f0c8687ad35e8d9d309\Microsoft.VisualBasic.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Drawing\b12bbcf27f41d96fe44360ae0b566f9b\System.Drawing.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Windows.Forms\454c09ea87bde1d5f545d60232083b79\System.Windows.Forms.ni.dll",0..3,"C:\Windows\assembly\NativeImages_v2.0.50727_64\System.Runtime.Remo#\bc6a0a01a7bd9d05ca132f229184fce6\System.Runtime.Remoting.ni.dll",0..

C:\Users\user\AppData\Local\Temp\tmp5F10.tmp

Process:	C:\Users\user\Desktop\RFQ CL-2021 - 0188 ROCKWELL LAND (WEVER).xls.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1645
Entropy (8bit):	5.170850892375768
Encrypted:	false

C:\Users\user\AppData\Local\Temp\tmp5F10.tmp	
SSDEEP:	24:2dH4+SEqC/a7hTlNMFpH/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB3tn:cbhC7ZlNQF/rydbz9I3YODOLNdq3X
MD5:	D0B8C7DFE85A2E2E892799522AE2047E
SHA1:	575197E95711C9B507A46594C816DB44D9F23D7E
SHA-256:	B078D571D2675B6B56E0529CCB06754785970F3CB225AED532C1987A3034B0B8
SHA-512:	45F535890A75548586ACFA76BBB0DB9DE8C4A49BDAF03772AE234278D997C09C2BC10AA6F43BAB1F0DAF17C3773F3BC243A13CB1869554C133EE8C53FA5341E
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>t

C:\Users\user\AppData\Roaming\DCBdvFPc.exe	
Process:	C:\Users\user\Desktop\RFQ CL-2021 - 0188 ROCKWELL LAND (WEVER).xls.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1203712
Entropy (8bit):	7.695986682629614
Encrypted:	false
SSDEEP:	24576:lrQ9Pmo5Hu99hpsqpBEae4tBI8vNRwiPXToUE1LXBc:hQMo5Hg39DwiPjKJ
MD5:	8C457878CC3C72EA684D3034837101E0
SHA1:	8AAD02989C92C45252B7E41F0C712DB31C0A1574
SHA-256:	94DC3CEB75323F7B1BFF7355DA2D28804D4DF36FA98A1335211101EF94BB2DDA
SHA-512:	2DD8D56814AD511C06A4E331F43B1C4F766C3868F1254B37EFDF173FBCCF1D3887F834A5483936E19431E047505BA8881603D2277203DDE5F0A16A81C467A1C5
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 30%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...z..a....."...P.....N.....z-... ...@....@.. .....@.....(-..O....@...K..... ....H.....text..... ....`.rsrc....K...@...L.....@..@.reloc.....\.....@..B.....\-.....H.....HV.....0.....(....(.....(.....o....*.....(.....(.....(!.....("....(#....*N..(....o....($....*&..(%....*.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\DCBdvFPc.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\RFQ CL-2021 - 0188 ROCKWELL LAND (WEVER).xls.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:	high, very likely benign file
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.695986682629614

General

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:	RFQ CL-2021 - 0188 ROCKWELL LAND (WEVER).xls.exe
File size:	1203712
MD5:	8c457878cc3c72ea684d3034837101e0
SHA1:	8aad02989c92c45252b7e41f0c712db31c0a1574
SHA256:	94dc3ceb75323f7b1bff7355da2d28804d4df36fa98a1335211101ef94bb2dda
SHA512:	2dd8d56814ad511c06a4e331f43b1c4f766c3868f1254b37efdf173fbccf1d3887f834a5483936e19431e047505ba8881603d2277203dde5f0a16a81c467a1c5
SSDEEP:	24576:lrQ9Pmo5Hu99hpsqpBEae4tBI8vNRwiPXToUE1LXBc:hQMo5Hg39DwiPjKJ
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...z..a....."...P.....N.....z-... ...@....@.. .....@.....

File Icon

Icon Hash:	c49a0894909c6494

Static PE Info

General

Entrypoint:	0x522d7a
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x6108AB7A [Tue Aug 3 02:35:38 2021 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	0x120d80	0x120e00	False	0.867353147988	data	7.70845208383	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x124000	0x4bd0	0x4c00	False	0.460166529605	data	6.05100869041	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x12a000	0xc	0x200	False	0.044921875	data	0.101910425663	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Imports

Version Infos

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: RFQ CL-2021 - 0188 ROCKWELL LAND (WEVER).xls.exe PID: 4328
Parent PID: 5552

General

Start time:	08:32:27
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\RFQ CL-2021 - 0188 ROCKWELL LAND (WEVER).xls.exe
Wow64 process (32bit):	false
Commandline:	'C:\Users\user\Desktop\RFQ CL-2021 - 0188 ROCKWELL LAND (WEVER).xls.exe'
Imagebase:	0x750000
File size:	1203712 bytes
MD5 hash:	8C457878CC3C72EA684D3034837101E0
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: 00000000.00000002.263221894.000000001304A000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Nanocore, Description: Yara detected Nanocore RAT, Source: 00000000.00000002.263221894.000000001304A000.00000004.00000001.sdmp, Author: Joe Security • Rule: NanoCore, Description: unknown, Source: 00000000.00000002.263221894.000000001304A000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000000.00000002.260617186.0000000002EC1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities — Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 980 Parent PID: 4328

General

Start time:	08:32:37
Start date:	03/08/2021
Path:	C:\Windows\System32\schtasks.exe
Wow64 process (32bit):	false
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\DCBdvFPc' /XML 'C:\Users\user\AppData\Local\Temp\tmp5F10.tmp'
Imagebase:	0x7ff7d8ce0000
File size:	226816 bytes
MD5 hash:	838D346D1D28F00783B7A6C6BD03A0DA
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	moderate

File Activities Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 5600 Parent PID: 980

General

Start time:	08:32:38
Start date:	03/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7ecfc0000
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: RFQ CL-2021 - 0188 ROCKWELL LAND (WEVER).xls.exe PID: 3528 Parent PID: 4328

General

Start time:	08:32:39
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\RFQ CL-2021 - 0188 ROCKWELL LAND (WEVER).xls.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\RFQ CL-2021 - 0188 ROCKWELL LAND (WEVER).xls.exe
Imagebase:	0x4c0000
File size:	1203712 bytes
MD5 hash:	8C457878CC3C72EA684D3034837101E0
Has elevated privileges:	true

Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: RFQ CL-2021 - 0188 ROCKWELL LAND (WEVER).xls.exe PID: 248 Parent PID: 4328

General

Start time:	08:32:39
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\RFQ CL-2021 - 0188 ROCKWELL LAND (WEVER).xls.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\RFQ CL-2021 - 0188 ROCKWELL LAND (WEVER).xls.exe
Imagebase:	0x5c0000
File size:	1203712 bytes
MD5 hash:	8C457878CC3C72EA684D3034837101E0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: RFQ CL-2021 - 0188 ROCKWELL LAND (WEVER).xls.exe PID: 5612 Parent PID: 4328

General

Start time:	08:32:40
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\RFQ CL-2021 - 0188 ROCKWELL LAND (WEVER).xls.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\RFQ CL-2021 - 0188 ROCKWELL LAND (WEVER).xls.exe
Imagebase:	0xe30000
File size:	1203712 bytes
MD5 hash:	8C457878CC3C72EA684D3034837101E0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: RFQ CL-2021 - 0188 ROCKWELL LAND (WEVER).xls.exe PID: 1704 Parent PID: 4328

General

Start time:	08:32:41
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\RFQ CL-2021 - 0188 ROCKWELL LAND (WEVER).xls.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\RFQ CL-2021 - 0188 ROCKWELL LAND (WEVER).xls.exe
Imagebase:	0xe60000
File size:	1203712 bytes
MD5 hash:	8C457878CC3C72EA684D3034837101E0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: RFQ CL-2021 - 0188 ROCKWELL LAND (WEVER).xls.exe PID: 4724
Parent PID: 4328

General

Start time:	08:32:41
Start date:	03/08/2021
Path:	C:\Users\user\Desktop\RFQ CL-2021 - 0188 ROCKWELL LAND (WEVER).xls.exe
Wow64 process (32bit):	false
Commandline:	C:\Users\user\Desktop\RFQ CL-2021 - 0188 ROCKWELL LAND (WEVER).xls.exe
Imagebase:	0x7ff797770000
File size:	1203712 bytes
MD5 hash:	8C457878CC3C72EA684D3034837101E0
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	low

Disassembly

Code Analysis