ID: 528509
Sample Name: balance payment.exe
Cookbook: default.jbs
Time: 11:55:13
Date: 25/11/2021
Version: 34.0.0 Boulder Opal

Table of Contents

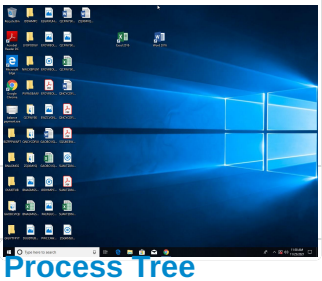
Windows Analysis Report balance payment.exe

Overview

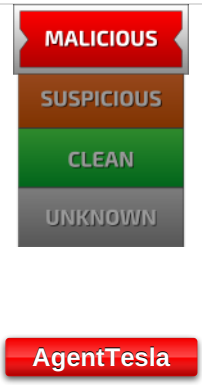
General Information

Sample Name:	balance payment.exe
Analysis ID:	528509
MD5:	8749faaa0cd99cc..
SHA1:	aa20d9562fba4be.
SHA256:	f7e55c2a4643804.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection

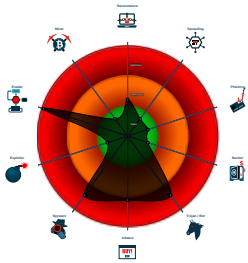


Score:	100
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Found malware configuration
- Snort IDS alert for network traffic (e…
- Multi AV Scanner detection for subm…
- Yara detected AgentTesla
- Yara detected AntiVM3
- Multi AV Scanner detection for dropp…
- Tries to steal Mail credentials (via fil…
- Initial sample is a PE file and has a …
- Tries to harvest and steal Putty / Wi…
- Tries to harvest and steal ftp login c…
- Modifies the hosts file
- Tries to detect sandboxes and other…

Classification



Process Tree

- **System is w10x64**
- balance payment.exe (PID: 2316 cmdline: "C:\Users\user\Desktop\balance payment.exe" MD5: 8749FAAA0CD99CC1C11849AC401736E2)
  - schtasks.exe (PID: 3132 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\mbYOWdeph" /XML "C:\Users\user\AppData\Local\Temp\tmp6392.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6484 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - balance payment.exe (PID: 6492 cmdline: {path} MD5: 8749FAAA0CD99CC1C11849AC401736E2)
- tKZVPq.exe (PID: 1244 cmdline: "C:\Users\user\AppData\Roaming\tKZVPq\tKZVPq.exe" MD5: 8749FAAA0CD99CC1C11849AC401736E2)
  - schtasks.exe (PID: 5048 cmdline: C:\Windows\System32\schtasks.exe" /Create /TN "Updates\mbYOWdeph" /XML "C:\Users\user\AppData\Local\Temp\tmp5CD.tmp MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 1140 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - tKZVPq.exe (PID: 7112 cmdline: {path} MD5: 8749FAAA0CD99CC1C11849AC401736E2)
  - tKZVPq.exe (PID: 5572 cmdline: {path} MD5: 8749FAAA0CD99CC1C11849AC401736E2)
- tKZVPq.exe (PID: 3016 cmdline: "C:\Users\user\AppData\Roaming\tKZVPq\tKZVPq.exe" MD5: 8749FAAA0CD99CC1C11849AC401736E2)
- **cleanup**

Malware Configuration

Threatname: Agenttesla

```
{
  "Exfil Mode": "SMTP",
  "Username": "admin@nktech.com.sg",
  "Password": "Nktech@64",
  "Host": "mail.nktech.com.sg"
}
```

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
0000000E.00000002.406918222.000000000407 9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	

Source	Rule	Description	Author	Strings
0000000E.00000002.406918222.000000000407 9000.00000004.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000016.00000000.397724944.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
00000016.00000000.397724944.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
00000016.00000000.399409697.000000000040 2000.00000040.00000001.sdmp	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 38 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
22.0.tKZVPq.exe.400000.10.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
22.0.tKZVPq.exe.400000.10.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
0.2.balance payment.exe.373a2d8.1.raw.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
0.2.balance payment.exe.373a2d8.1.raw.unpack	JoeSecurity_AgentTesla_2	Yara detected AgentTesla	Joe Security	
10.0.balance payment.exe.400000.4.unpack	JoeSecurity_AgentTesla_1	Yara detected AgentTesla	Joe Security	
Click to see the 37 entries				

Sigma Overview

System Summary:

Sigma detected: Suspicius Add Task From User AppData Temp

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Found malware configuration

Multi AV Scanner detection for submitted file

Multi AV Scanner detection for dropped file

Machine Learning detection for sample

Machine Learning detection for dropped file

Networking:

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

Spam, unwanted Advertisements and Ransom Demands:

Modifies the hosts file

System Summary:

Initial sample is a PE file and has a suspicious name

.NET source code contains very large array initializations

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)

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

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

HIPS / PFW / Operating System Protection Evasion:

Modifies the hosts file

Injects a PE file into a foreign processes

Lowering of HIPS / PFW / Operating System Security Settings:

Modifies the hosts file

Stealing of Sensitive Information:

Yara detected AgentTesla

Tries to steal Mail credentials (via file / registry access)

Tries to harvest and steal Putty / WinSCP information (sessions, passwords, etc)

Tries to harvest and steal ftp login credentials

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

Remote Access Functionality:

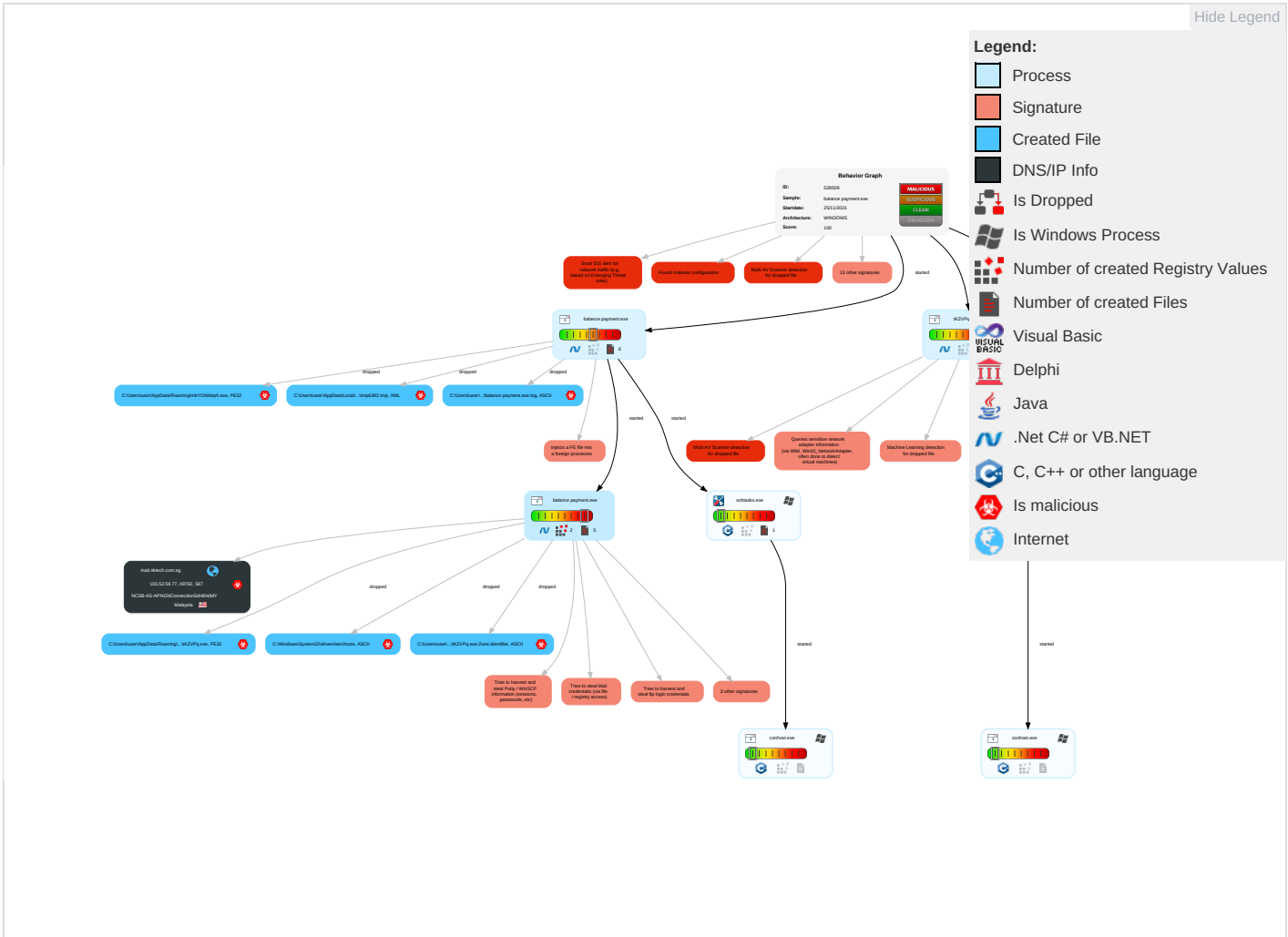
Yara detected AgentTesla

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 2 1 1	Scheduled Task/Job 1	Process Injection 1 1 2	File and Directory Permissions Modification 1	OS Credential Dumping 2	File and Directory Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Scheduled Task/Job 1	Registry Run Keys / Startup Folder 1	Scheduled Task/Job 1	Disable or Modify Tools 1	Input Capture 1	System Information Discovery 1 1 4	Remote Desktop Protocol	Data from Local System 2	Exfiltration Over Bluetooth	Non-Standard Port 1
Domain Accounts	At (Linux)	Logon Script (Windows)	Registry Run Keys / Startup Folder 1	Deobfuscate/Decode Files or Information 1	Credentials in Registry 1	Security Software Discovery 3 1 1	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Non-Application Layer Protocol 1

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	Process Discovery 2	Distributed Component Object Model	Input Capture 1	Scheduled Transfer	Application Layer Protocol 1 1
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1 3	LSA Secrets	Virtualization/Sandbox Evasion 1 3 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Application Window Discovery 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicatic
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 1 3 1	DCSync	Remote System Discovery 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 1 1 2	Proc Filesystem	Network Service Scanning	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protocc
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Hidden Files and Directories 1	/etc/passwd and /etc/shadow	System Network Connections Discovery	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encrypted Non-C2 Protocol	Web Protocol

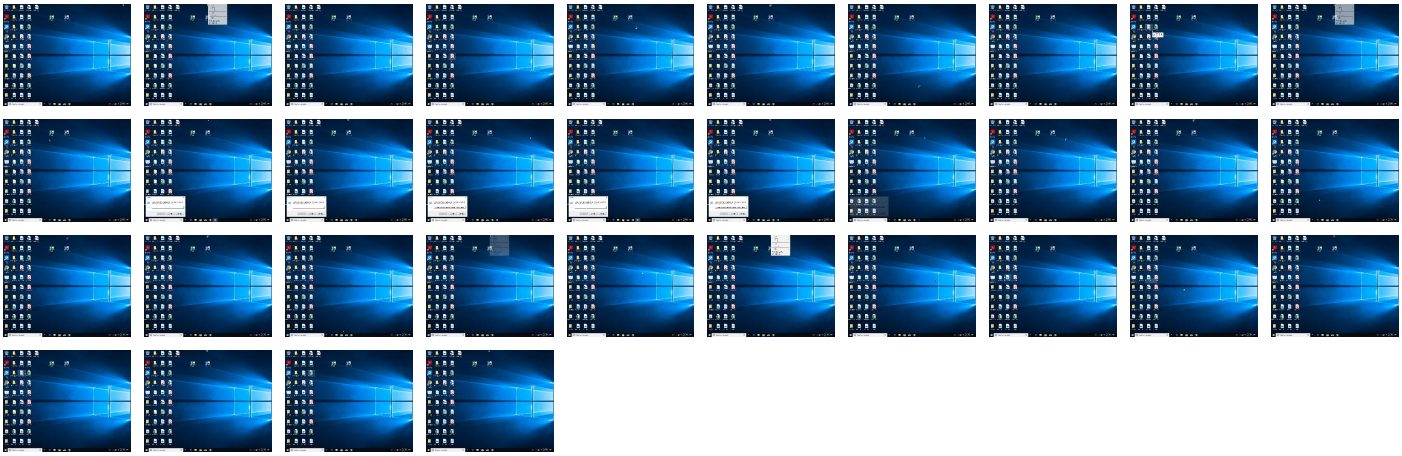
Behavior Graph



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
balance payment.exe	45%	Virustotal		Browse
balance payment.exe	36%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
balance payment.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\mbYOWdeph.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\tKZVPq\tKZVPq.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\mbYOWdeph.exe	40%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	
C:\Users\user\AppData\Roaming\tKZVPq\tKZVPq.exe	40%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
22.0.tKZVPq.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
10.0.balance payment.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
10.0.balance payment.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
22.2.tKZVPq.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File
10.0.balance payment.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
22.0.tKZVPq.exe.400000.12.unpack	100%	Avira	TR/Spy.Gen8		Download File
22.0.tKZVPq.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
10.0.balance payment.exe.400000.10.unpack	100%	Avira	TR/Spy.Gen8		Download File
22.0.tKZVPq.exe.400000.4.unpack	100%	Avira	TR/Spy.Gen8		Download File
22.0.tKZVPq.exe.400000.6.unpack	100%	Avira	TR/Spy.Gen8		Download File
10.0.balance payment.exe.400000.8.unpack	100%	Avira	TR/Spy.Gen8		Download File
10.2.balance payment.exe.400000.0.unpack	100%	Avira	TR/Spy.Gen8		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://127.0.0.1:HTTP/1.1	0%	Avira URL Cloud	safe	
http://DynDns.comDynDNS	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip%tordir%%ha	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://mail.nktech.com.sg	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://en.w	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://nOoUXb.com	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.sandoll.co.kr	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://904oyGsO0QBTV.com1-5-21-3853321935-2125563209-4053062332-1002_Classes	0%	Avira URL Cloud	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://https://www.theonionrouter.com/dist.torproject.org/torbrowser/9.5.3/tor-win32-0.4.3.6.zip	0%	URL Reputation	safe	
http://904oyGsO0QBTV.com	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
mail.nktech.com.sg	103.52.59.77	true	true		unknown

URLs from Memory and Binaries

Contacted IPs

Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
103.52.59.77	mail.nktech.com.sg	Malaysia		134088	NCSB-AS-APNGNConnectionSdnBhdMY	true

General Information

Joe Sandbox Version:	34.0.0 Boulder Opal
Analysis ID:	528509
Start date:	25.11.2021
Start time:	11:55:13
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 33s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	balance payment.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:	30
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.adwa.spyw.evad.winEXE@15/9@1/1
EGA Information:	Failed
HDC Information:	• Successful, ratio: 0.3% (good quality ratio 0.2%) • Quality average: 50.5% • Quality standard deviation: 30.5%
HCA Information:	• Successful, ratio: 96% • 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
11:56:08	API Interceptor	742x Sleep call for process: balance payment.exe modified
11:56:38	Autostart	Run: HKCU\Software\Microsoft\Windows\CurrentVersion\Run tKZVPq C:\Users\user\AppData\Roaming\tKZVPq\tKZVPq.exe
11:56:46	Autostart	Run: HKCU64\Software\Microsoft\Windows\CurrentVersion\Run tKZVPq C:\Users\user\AppData\Roaming\tKZVPq\tKZVPq.exe
11:56:49	API Interceptor	422x Sleep call for process: tKZVPq.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
mail.nktech.com.sg	SOA.exe	Get hash	malicious	Browse	• 103.52.59.50
	SOA.exe	Get hash	malicious	Browse	• 103.52.59.50
	statement of account.exe	Get hash	malicious	Browse	• 103.52.59.77

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
NCSB-AS-APNGNConnectionSdnBhdMY	SOA.exe	Get hash	malicious	Browse	• 103.52.59.50
	SOA.exe	Get hash	malicious	Browse	• 103.52.59.39
	SOA 5 NOV.exe	Get hash	malicious	Browse	• 103.52.59.39

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\balance payment.exe.log

Process:	C:\Users\user\Desktop\balance payment.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F8
Malicious:	**true**
Reputation:	high, very likely benign file

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\balance payment.exe.log	
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\tKZVPq.exe.log	
Process:	C:\Users\user\AppData\Roaming\tKZVPq\tKZVPq.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4x84qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4j:MIHK5HKXE1qHxviYHKhQnoPtHoxHhAHY
MD5:	69206D3AF7D6EFD08F4B4726998856D3
SHA1:	E778D4BF781F7712163CF5E2F5E7C15953E484CF
SHA-256:	A937AD22F9C3E667A062BA0E116672960CD93522F6997C77C00370755929BA87
SHA-512:	CD270C3DF75E548C9B0727F13F44F45262BD474336E89AAEBE56FABFE8076CD4638F88D3C0837B67C2EB3C54055679B07E4212FB3FEDBF88C015EB5DBBCD7F8
Malicious:	false
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..2,"Microsoft.VisualBasic, Version=10.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a

C:\Users\user\AppData\Local\Temp\tmp2BD3.tmp	
Process:	C:\Users\user\AppData\Roaming\tKZVPq\tKZVPq.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.188663948232156
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB2tn:cbh47TlNQ//rydbz9l3YODOLNdq36
MD5:	10DB0B216285C1DA4AF14425DD70EC81
SHA1:	5A1C4C14FBC5D0F731748A3430B6A86E4D76BF2B
SHA-256:	E3E25AE6161A01398BCCDFBFA3BCAA26D25F37F5493A5719DDB4B2A64911006F
SHA-512:	D93448AFE7FF9D827A1AE6D6458DE04A5A361D13579D54D1AD89851F9BA8CA8DBAD8DE0D7D6F22A8CA0965A1BD2EDA723032869A608A08C9606AEA55C9FBDFD
Malicious:	false
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Local\Temp\tmp5CD.tmp	
Process:	C:\Users\user\AppData\Roaming\tKZVPq\tKZVPq.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.188663948232156
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB2tn:cbh47TlNQ//rydbz9l3YODOLNdq36
MD5:	10DB0B216285C1DA4AF14425DD70EC81
SHA1:	5A1C4C14FBC5D0F731748A3430B6A86E4D76BF2B
SHA-256:	E3E25AE6161A01398BCCDFBFA3BCAA26D25F37F5493A5719DDB4B2A64911006F
SHA-512:	D93448AFE7FF9D827A1AE6D6458DE04A5A361D13579D54D1AD89851F9BA8CA8DBAD8DE0D7D6F22A8CA0965A1BD2EDA723032869A608A08C9606AEA55C9FBDFD
Malicious:	false
Reputation:	low

C:\Users\user\AppData\Local\Temp\tmp5CD.tmp	
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\tmp6392.tmp	
Process:	C:\Users\user\Desktop\balance payment.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1642
Entropy (8bit):	5.188663948232156
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/Q7hxlNMFp1/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB2tn:cbh47TlNQ//rydbz9l3YODOLNdq36
MD5:	10DB0B216285C1DA4AF14425DD70EC81
SHA1:	5A1C4C14FBC5D0F731748A3430B6A86E4D76BF2B
SHA-256:	E3E25AE6161A01398BCCDFBFA3BCAA26D25F37F5493A5719DDB4B2A64911006F
SHA-512:	D93448AFE7FF9D827A1AE6D6458DE04A5A361D13579D54D1AD89851F9BA8CA8DBAD8DE0D7D6F22A8CA0965A1BD2EDA723032869A608A08C9606AEA55C9FBDFD
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvailable>true

C:\Users\user\AppData\Roaming\mbYOWdeph.exe	
Process:	C:\Users\user\Desktop\balance payment.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	625664
Entropy (8bit):	7.583832724842121
Encrypted:	false
SSDEEP:	12288:1h7R5iVjIiMqAx7K5Twn1dGCT6R7siYZEHfdQVYJUEKl75jQWmc:nDiOvRgwn1sCTymkf2VYJUEKlCW
MD5:	8749FAAA0CD99CC1C11849AC401736E2
SHA1:	AA20D9562FBA4BE847ABAA8D3FB3C5335DD9ECF4
SHA-256:	F7E55C2A4643804D04C3BE2A535F480BD1AFDBB3D627769DDDFFE96B93546B0A
SHA-512:	CBC355E2BADFE761F03B094AD8CCE1F02697FFBF16DEC9ED515940D6D637883280ABF7AA2FEDC41E6E4F33CBF1BE64EC0E7287A9B579D9DCE06577F66DAAAE53
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 40%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...A..a.....B...H.....2a... .....@.. ....@.....`..W.....E..... ..... ..H.....text...8A... ...B..... ..`.rsrc....E.....F...D.....@..@.rel oc.....@..B.....a.....H.....&...:.....j...pQ..T.....z.(.....}.....(....o....}....*..0.....{.....3.....(....*.....0.....{.....,....f.... .....}.....}.....}.....s....o....}.....}....8.....{....o....}.....{....}.....}.....}.....{.....Y}.....{....-...+H.{.....{....X.{....X .;.|.{....Xa}.....}.....{....o....q....(....+..(.....}.....(.....*.....n ..}.....{.....,..{....oh...*..{....*.s .

C:\Users\user\AppData\Roaming\tKZVPq\tKZVPq.exe	
Process:	C:\Users\user\Desktop\balance payment.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	625664
Entropy (8bit):	7.583832724842121
Encrypted:	false
SSDEEP:	12288:1h7R5iVjIiMqAx7K5Twn1dGCT6R7siYZEHfdQVYJUEKl75jQWmc:nDiOvRgwn1sCTymkf2VYJUEKlCW
MD5:	8749FAAA0CD99CC1C11849AC401736E2
SHA1:	AA20D9562FBA4BE847ABAA8D3FB3C5335DD9ECF4
SHA-256:	F7E55C2A4643804D04C3BE2A535F480BD1AFDBB3D627769DDDFFE96B93546B0A
SHA-512:	CBC355E2BADFE761F03B094AD8CCE1F02697FFBF16DEC9ED515940D6D637883280ABF7AA2FEDC41E6E4F33CBF1BE64EC0E7287A9B579D9DCE06577F66DAAAE53
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 40%

C:\Users\user\AppData\Roaming\tKZVPq\tKZVPq.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...A..a.....B...H.....2a... .....@.. ....@.....`..W.....E..... ..... ..H.....text...8A... ...B..... ..`.rsrc....E.....F...D.....@..@.rel oc.....@..B.....a.....H.....&...:.....j...pQ..T.....z.(.....}.....(....o....}....*..0.....{.....3.....(....*.....0.....{.....,...f.... .....}.....}.....}.....s....o....}.....}....8.....{....o....}.....{....}.....}.....}.....{.....Y}.....{....-...+H.{.....{....X.{....X .;.|.{....Xa}.....}.....{....o....:q....(....+..(.....}.....(.....*.....n ..}.....{.....,.{....oh...*..{....*.s .

C:\Users\user\AppData\Roaming\tKZVPq\tKZVPq.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\balance payment.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	**true**
Preview:	[ZoneTransfer]....ZoneId=0

C:\Windows\System32\drivers\etc\hosts	
Process:	C:\Users\user\Desktop\balance payment.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	835
Entropy (8bit):	4.694294591169137
Encrypted:	false
SSDEEP:	24:QWDZh+ragzMZfuMMs1L/JU5fFCkK8T1rTt8:vDZhyoZWM9rU5fFcP
MD5:	6EB47C1CF858E25486E42440074917F2
SHA1:	6A63F93A95E1AE831C393A97158C526A4FA0FAAE
SHA-256:	9B13A3EA948A1071A81787AAC1930B89E30DF22CE13F8FF751F31B5D83E79FFB
SHA-512:	08437AB32E7E905EB11335E670CDD5D999803390710ED39CBC31A2D3F05868D5D0E5D051CCD7B06A85BB466932F99A220463D27FAC29116D241E8ADAC495FA2
Malicious:	**true**
Preview:	# Copyright (c) 1993-2009 Microsoft Corp...#..# This is a sample HOSTS file used by Microsoft TCP/IP for Windows...#..# This file contains the mappings of IP addresses to host names. Each..# entry should be kept on an individual line. The IP address should..# be placed in the first column followed by the corresponding host name...# The IP address and the host name should be separated by at least one..# space...#..# Additionally, comments (such as these) may be inserted on individual..# lines or following the machine name denoted by a '#' symbol...#..# For example:..#..# 102.54.94.97 rhino.acme.com # source server..# 38.25.63.10 x.acme.com # x client host....# localhost name resolution is handled within DNS itself...#.127.0.0.1 localhost..#.::1 localhost....127.0.0.1

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.583832724842121
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.83% • Win32 Executable (generic) a (10002005/4) 49.78% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Generic Win/DOS Executable (2004/3) 0.01% • DOS Executable Generic (2002/1) 0.01%
File name:	balance payment.exe
File size:	625664
MD5:	8749faaa0cd99cc1c11849ac401736e2
SHA1:	aa20d9562fba4be847abaa8d3fb3c5335dd9ecf4
SHA256:	f7e55c2a4643804d04c3be2a535f480bd1afdbb3d627769dddffe96b93546b0a
SHA512:	cbc355e2badfe761f03b094ad8cce1f02697ffbf16dec9ed515940d6d637883280abf7aa2fedc41e6e4f33cbf1be64ec0e7287a9b579d9dce06577f66daaae53

General

SSDEEP:	12288:1h7R5iVjliMqAx7K5Twn1dGCT6R7siYZEHfdQVYJUEKl75jQWmc:nDiOvRgwn1sCTymkf2VYJUEKlCW
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L...A..a.....B...H.....2a... .....@.. .....@.....

File Icon

Icon Hash:	04fcf0b0d4a6e46c

Static PE Info

General

Entrypoint:	0x466132
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED
DLL Characteristics:	NO_SEH, TERMINAL_SERVER_AWARE, DYNAMIC_BASE, NX_COMPAT
Time Stamp:	0x619EF841 [Thu Nov 25 02:43:13 2021 UTC]
TLS Callbacks:	
CLR (.Net) Version:	v4.0.30319
OS Version Major:	4
OS Version Minor:	0
File Version Major:	4
File Version Minor:	0
Subsystem Version Major:	4
Subsystem Version Minor:	0
Import Hash:	f34d5f2d4577ed6d9ceec516c1f5a744

Entrypoint Preview

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x2000	0x64138	0x64200	False	0.965726435705	data	7.96739096894	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rsrc	0x68000	0x345ac	0x34600	False	0.444967556683	data	6.26468611955	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0x9e000	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

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/25/21-11:57:57.302473	TCP	2030171	ET TROJAN AgentTesla Exfil Via SMTP	49782	587	192.168.2.3	103.52.59.77

Network Port Distribution

TCP Packets

UDP Packets

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 25, 2021 11:57:54.618191004 CET	192.168.2.3	8.8.8.8	0x633b	Standard query (0)	mail.nktech.com.sg	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 25, 2021 11:57:55.471035004 CET	8.8.8.8	192.168.2.3	0x633b	No error (0)	mail.nktech.com.sg		103.52.59.77	A (IP address)	IN (0x0001)
Nov 25, 2021 11:57:55.471035004 CET	8.8.8.8	192.168.2.3	0x633b	No error (0)	mail.nktech.com.sg		103.52.59.50	A (IP address)	IN (0x0001)

SMTP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 25, 2021 11:57:56.057274103 CET	587	49782	103.52.59.77	192.168.2.3	220 ns50.isodium.net ESMTP Exim 4.94.2 Thu, 25 Nov 2021 18:57:55 +0800
Nov 25, 2021 11:57:56.058543921 CET	49782	587	192.168.2.3	103.52.59.77	EHLO 123991
Nov 25, 2021 11:57:56.263880968 CET	587	49782	103.52.59.77	192.168.2.3	250-ns50.isodium.net Hello 123991 [84.17.52.63] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-PIPE_CONNECT 250-AUTH PLAIN LOGIN 250-STARTTLS 250 HELP
Nov 25, 2021 11:57:56.264570951 CET	49782	587	192.168.2.3	103.52.59.77	AUTH login YWRtaW5Abmt0ZWNoLmNvbS5zZw==
Nov 25, 2021 11:57:56.468581915 CET	587	49782	103.52.59.77	192.168.2.3	334 UGFzc3dvcmQ6
Nov 25, 2021 11:57:56.685695887 CET	587	49782	103.52.59.77	192.168.2.3	235 Authentication succeeded
Nov 25, 2021 11:57:56.686741114 CET	49782	587	192.168.2.3	103.52.59.77	MAIL FROM:<admin@nktech.com.sg>
Nov 25, 2021 11:57:56.892146111 CET	587	49782	103.52.59.77	192.168.2.3	250 OK
Nov 25, 2021 11:57:56.892642975 CET	49782	587	192.168.2.3	103.52.59.77	RCPT TO:<admin@nktech.com.sg>
Nov 25, 2021 11:57:57.097042084 CET	587	49782	103.52.59.77	192.168.2.3	250 Accepted
Nov 25, 2021 11:57:57.097614050 CET	49782	587	192.168.2.3	103.52.59.77	DATA
Nov 25, 2021 11:57:57.300781012 CET	587	49782	103.52.59.77	192.168.2.3	354 Enter message, ending with "." on a line by itself
Nov 25, 2021 11:57:57.303690910 CET	49782	587	192.168.2.3	103.52.59.77	.
Nov 25, 2021 11:57:57.521567106 CET	587	49782	103.52.59.77	192.168.2.3	250 OK id=1mqCRc-0003E7-6R

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: balance payment.exe PID: 2316 Parent PID: 2364

General

Start time:	11:56:02
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\balance payment.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\Desktop\balance payment.exe"
Imagebase:	0x2a0000
File size:	625664 bytes
MD5 hash:	8749FAAA0CD99CC1C11849AC401736E2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.305613107.00000000037F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.305613107.00000000037F1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000000.00000002.303631045.00000000035A9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000000.00000002.303631045.00000000035A9000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 3132 Parent PID: 2316

General

Start time:	11:56:11
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\mbYOWdeph" /XML "C:\Users\user\AppData\Local\Temp\tmp6392.tmp
Imagebase:	0xe0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 6484 Parent PID: 3132

General

Start time:	11:56:12
Start date:	25/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
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: balance payment.exe PID: 6492 Parent PID: 2316

General

Start time:	11:56:12
Start date:	25/11/2021
Path:	C:\Users\user\Desktop\balance payment.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xa30000
File size:	625664 bytes
MD5 hash:	8749FAAA0CD99CC1C11849AC401736E2
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000A.00000000.298455303.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000A.00000000.298455303.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000A.00000002.546690574.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000A.00000002.546690574.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000A.00000000.298892992.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000A.00000000.298892992.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000A.00000000.298033202.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000A.00000000.298033202.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000A.00000002.553285330.0000000002F21000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 0000000A.00000002.553285330.0000000002F21000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000A.00000000.299544596.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000A.00000000.299544596.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Written

File Read

Registry Activities

Show Windows behavior

Key Value Created

Analysis Process: tKZVPq.exe PID: 1244 Parent PID: 3352

General

Start time:	11:56:46
Start date:	25/11/2021
Path:	C:\Users\user\AppData\Roaming\tKZVPq\tKZVPq.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\tKZVPq\tKZVPq.exe"
Imagebase:	0xd80000
File size:	625664 bytes
MD5 hash:	8749FAAA0CD99CC1C11849AC401736E2
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 0000000E.00000002.406918222.0000000004079000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 0000000E.00000002.406918222.0000000004079000.00000004.00000001.sdmp, Author: Joe Security

Antivirus matches:	• Detection: 100%, Joe Sandbox ML • Detection: 40%, ReversingLabs
Reputation:	low

File Activities Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 5048 Parent PID: 1244

General

Start time:	11:56:53
Start date:	25/11/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\System32\schtasks.exe" /Create /TN "Updates\mbYOWdeph" /XML "C:\Users\user\AppData\Local\Temp\tmp5CD.tmp
Imagebase:	0xe0000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

File Activities Show Windows behavior

File Read

Analysis Process: conhost.exe PID: 1140 Parent PID: 5048

General

Start time:	11:56:54
Start date:	25/11/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff7f20f0000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: tKZVPq.exe PID: 3016 Parent PID: 3352

General

Start time:	11:56:54
Start date:	25/11/2021
Path:	C:\Users\user\AppData\Roaming\tKZVPq\tKZVPq.exe
Wow64 process (32bit):	true
Commandline:	"C:\Users\user\AppData\Roaming\tKZVPq\tKZVPq.exe"
Imagebase:	0x310000
File size:	625664 bytes
MD5 hash:	8749FAAA0CD99CC1C11849AC401736E2
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000014.00000002.409260613.00000000036E9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000014.00000002.409260613.00000000036E9000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000014.00000002.407021911.00000000026E1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Analysis Process: tKZVPq.exe PID: 7112 Parent PID: 1244

General

Start time:	11:56:57
Start date:	25/11/2021
Path:	C:\Users\user\AppData\Roaming\tKZVPq\tKZVPq.exe
Wow64 process (32bit):	false
Commandline:	{path}
Imagebase:	0x130000
File size:	625664 bytes
MD5 hash:	8749FAAA0CD99CC1C11849AC401736E2
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	C, C++ or other language
Reputation:	low

Analysis Process: tKZVPq.exe PID: 5572 Parent PID: 1244

General

Start time:	11:56:59
Start date:	25/11/2021
Path:	C:\Users\user\AppData\Roaming\tKZVPq\tKZVPq.exe
Wow64 process (32bit):	true
Commandline:	{path}
Imagebase:	0xb40000
File size:	625664 bytes
MD5 hash:	8749FAAA0CD99CC1C11849AC401736E2
Has elevated privileges:	false
Has administrator privileges:	false
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000016.00000000.397724944.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000016.00000000.397724944.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000016.00000000.399409697.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000016.00000000.399409697.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000016.00000000.398550040.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000016.00000000.398550040.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000016.00000000.400184100.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000016.00000000.400184100.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000016.00000002.546602894.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_2, Description: Yara detected AgentTesla, Source: 00000016.00000002.546602894.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AgentTesla_1, Description: Yara detected AgentTesla, Source: 00000016.00000002.551451589.0000000002EC1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_CredentialStealer, Description: Yara detected Credential Stealer, Source: 00000016.00000002.551451589.0000000002EC1000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Read

Disassembly

Code Analysis