ID: 320625
Sample Name: BANK-STATMENT _xlsx.exe
Cookbook: default.jbs
Time: 16:01:48
Date: 19/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

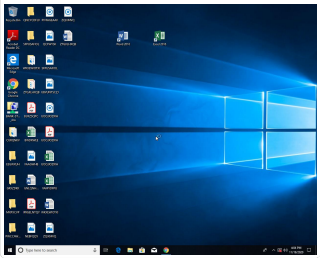
Analysis Report BANK-STATMENT _xlsx.exe

Overview

General Information

Sample Name:	BANK-STATMENT _xlsx.exe
Analysis ID:	320625
MD5:	debe564cd4c27c...
SHA1:	1b55fba242460cc...
SHA256:	edafe7e62738e18...
Tags:	exe HawkEye

Most interesting Screenshot:



Detection

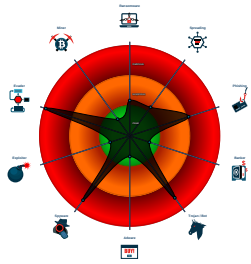
HawkEye
MailPassView

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

Signatures

- Detected HawkEye Rat
- Detected unpacking (changes PE se…
- Detected unpacking (creates a PE fi…
- Detected unpacking (overwrites its o…
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for subm…
- Snort IDS alert for network traffic (e.…
- Yara detected HawkEye Keylogger
- Yara detected MailPassView
- .NET source code contains potentia…
- .NET source code references suspic…
- Allocates memory in foreign process

Classification



Startup

- **System is w10x64**
- BANK-STATMENT _xlsx.exe (PID: 1496 cmdline: 'C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe' MD5: DEBE564CD4C27C02D23C828DF27FE27F)
  - BANK-STATMENT _xlsx.exe (PID: 4500 cmdline: 'C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe' MD5: DEBE564CD4C27C02D23C828DF27FE27F)
    - dw20.exe (PID: 5996 cmdline: dw20.exe -x -s 2264 MD5: 8D10DA8A3E11747E51F23C882C22BBC3)
    - vbc.exe (PID: 6920 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holdermail.txt' MD5: C63ED21D5706A527419C9FBD730FFB2E)
    - vbc.exe (PID: 7044 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holderwb.txt' MD5: C63ED21D5706A527419C9FBD730FFB2E)
  - BANK-STATMENT _xlsx.exe (PID: 3984 cmdline: 'C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe' 2 4500 5715437 MD5: DEBE564CD4C27C02D23C828DF27FE27F)
    - BANK-STATMENT _xlsx.exe (PID: 1900 cmdline: C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe MD5: DEBE564CD4C27C02D23C828DF27FE27F)
      - BANK-STATMENT _xlsx.exe (PID: 4240 cmdline: C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe MD5: DEBE564CD4C27C02D23C828DF27FE27F)
        - dw20.exe (PID: 5456 cmdline: dw20.exe -x -s 2304 MD5: 8D10DA8A3E11747E51F23C882C22BBC3)
      - BANK-STATMENT _xlsx.exe (PID: 6452 cmdline: 'C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe' 2 4240 5772140 MD5: DEBE564CD4C27C02D23C828DF27FE27F)
        - BANK-STATMENT _xlsx.exe (PID: 3028 cmdline: C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe MD5: DEBE564CD4C27C02D23C828DF27FE27F)
          - BANK-STATMENT _xlsx.exe (PID: 1548 cmdline: C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe MD5: DEBE564CD4C27C02D23C828DF27FE27F)
            - dw20.exe (PID: 5992 cmdline: dw20.exe -x -s 2288 MD5: 8D10DA8A3E11747E51F23C882C22BBC3)
            - vbc.exe (PID: 5676 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holdermail.txt' MD5: C63ED21D5706A527419C9FBD730FFB2E)
            - vbc.exe (PID: 6708 cmdline: C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holderwb.txt' MD5: C63ED21D5706A527419C9FBD730FFB2E)
          - BANK-STATMENT _xlsx.exe (PID: 2240 cmdline: 'C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe' 2 1548 5785125 MD5: DEBE564CD4C27C02D23C828DF27FE27F)
            - BANK-STATMENT _xlsx.exe (PID: 6984 cmdline: C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe MD5: DEBE564CD4C27C02D23C828DF27FE27F)
              - BANK-STATMENT _xlsx.exe (PID: 6180 cmdline: C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe MD5: DEBE564CD4C27C02D23C828DF27FE27F)
                - dw20.exe (PID: 5484 cmdline: dw20.exe -x -s 2264 MD5: 8D10DA8A3E11747E51F23C882C22BBC3)
              - BANK-STATMENT _xlsx.exe (PID: 6188 cmdline: 'C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe' 2 6180 5810484 MD5: DEBE564CD4C27C02D23C828DF27FE27F)
                - BANK-STATMENT _xlsx.exe (PID: 5540 cmdline: C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe MD5: DEBE564CD4C27C02D23C828DF27FE27F)
                  - BANK-STATMENT _xlsx.exe (PID: 5580 cmdline: C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe MD5: DEBE564CD4C27C02D23C828DF27FE27F)
                    - dw20.exe (PID: 6904 cmdline: dw20.exe -x -s 2324 MD5: 8D10DA8A3E11747E51F23C882C22BBC3)
                  - BANK-STATMENT _xlsx.exe (PID: 5588 cmdline: 'C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe' 2 5580 5822718 MD5: DEBE564CD4C27C02D23C828DF27FE27F)
                    - BANK-STATMENT _xlsx.exe (PID: 6176 cmdline: C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe MD5: DEBE564CD4C27C02D23C828DF27FE27F)
                      - BANK-STATMENT _xlsx.exe (PID: 2864 cmdline: C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe MD5: DEBE564CD4C27C02D23C828DF27FE27F)
                      - BANK-STATMENT _xlsx.exe (PID: 4608 cmdline: 'C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe' 2 2864 5836578 MD5: DEBE564CD4C27C02D23C828DF27FE27F)
- **cleanup**

Malware Configuration

Threatname: HawkEye


```
{
  "Modules": [
    "Mail PassView",
    "mailpv"
  ],
  "Version": ""
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000022.00000002.915921004.000000000303 2000.00000004.00000001.sdmp	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
00000022.00000002.915921004.000000000303 2000.00000004.00000001.sdmp	Hawkeye	detect HawkEye in memory	JPCERT/CC Incident Response Group	• 0x2674:$hawkstr1: HawkEye Keylogger • 0x20ec:$hawkstr2: Dear HawkEye Customers! • 0x221e:$hawkstr3: HawkEye Logger Details:

Source	Rule	Description	Author	Strings
00000025.00000002.926331050.000000000285 7000.00000040.00000001.sdmp	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x7b984:$key: HawkEyeKeylogger • 0x7dbb4:$salt: 099u787978786 • 0x7bfc5:$string1: HawkEye_Keylogger • 0x7ce04:$string1: HawkEye_Keylogger • 0x7db14:$string1: HawkEye_Keylogger • 0x7c39a:$string2: holdermail.txt • 0x7c3ba:$string2: holdermail.txt • 0x7c2dc:$string3: wallet.dat • 0x7c2f4:$string3: wallet.dat • 0x7c30a:$string3: wallet.dat • 0x7d6d8:$string4: Keylog Records • 0x7d9f0:$string4: Keylog Records • 0x7dc0c:$string5: do not script --> • 0x7b96c:$string6: \pidloc.txt • 0x7b9fa:$string7: BSPLIT • 0x7ba0a:$string7: BSPLIT
00000025.00000002.926331050.000000000285 7000.00000040.00000001.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
00000025.00000002.926331050.000000000285 7000.00000040.00000001.sdmp	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
Click to see the 280 entries				

Unpacked PEs

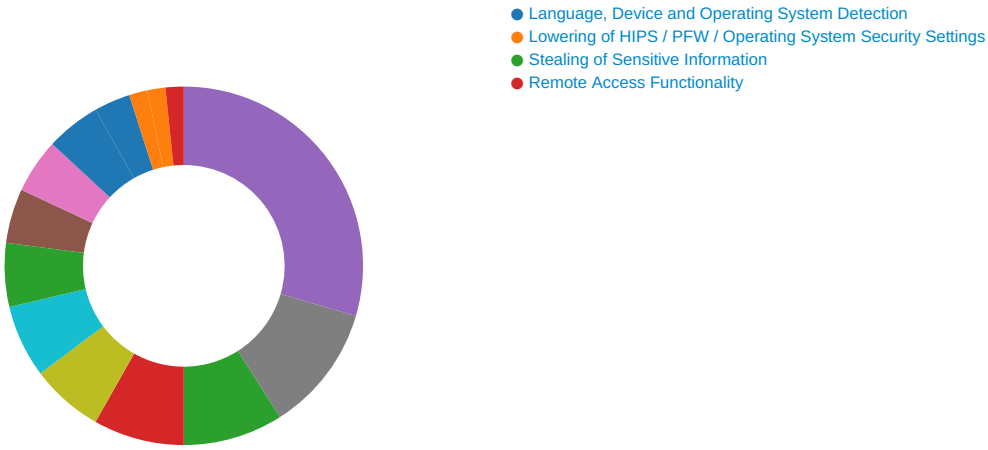
Source	Rule	Description	Author	Strings
25.2.vbc.exe.400000.0.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
7.2.vbc.exe.400000.0.unpack	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
1.2.BANK-STATMENT _xlsx.exe.23b0000.3.unpack	RAT_HawkEye	Detects HawkEye RAT	Kevin Breen <kevin@techanarchy.net>	• 0x7b89c:$key: HawkEyeKeylogger • 0x7dacc:$salt: 099u787978786 • 0x7bedd:$string1: HawkEye_Keylogger • 0x7cd1c:$string1: HawkEye_Keylogger • 0x7da2c:$string1: HawkEye_Keylogger • 0x7c2b2:$string2: holdermail.txt • 0x7c2d2:$string2: holdermail.txt • 0x7c1f4:$string3: wallet.dat • 0x7c20c:$string3: wallet.dat • 0x7c222:$string3: wallet.dat • 0x7d5f0:$string4: Keylog Records • 0x7d908:$string4: Keylog Records • 0x7db24:$string5: do not script --> • 0x7b884:$string6: \pidloc.txt • 0x7b912:$string7: BSPLIT • 0x7b922:$string7: BSPLIT
1.2.BANK-STATMENT _xlsx.exe.23b0000.3.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
1.2.BANK-STATMENT _xlsx.exe.23b0000.3.unpack	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
Click to see the 216 entries				

Sigma Overview

No Sigma rule has matched

Signature Overview

- AV Detection
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Hooking and other Techniques for Hiding and Protection
- Malware Analysis System Evasion
- Anti Debugging
- HIPS / PFW / Operating System Protection Evasion



Click to jump to signature section

AV Detection:

- Found malware configuration
- Multi AV Scanner detection for submitted file
- Machine Learning detection for sample

Networking:

- Snort IDS alert for network traffic (e.g. based on Emerging Threat rules)
- May check the online IP address of the machine

Key, Mouse, Clipboard, Microphone and Screen Capturing:

- Yara detected HawkEye Keylogger
- Contains functionality to log keystrokes (.Net Source)
- Installs a global keyboard hook

System Summary:

- Malicious sample detected (through community Yara rule)

Data Obfuscation:

- Detected unpacking (changes PE section rights)
- Detected unpacking (creates a PE file in dynamic memory)
- Detected unpacking (overwrites its own PE header)
- .NET source code contains potential unpacker

Hooking and other Techniques for Hiding and Protection:

- Changes the view of files in windows explorer (hidden files and folders)

Malware Analysis System Evasion:

- Contains functionality to detect sleep reduction / modifications

HIPS / PFW / Operating System Protection Evasion:

.NET source code references suspicious native API functions

Allocates memory in foreign processes

Injects a PE file into a foreign processes

Maps a DLL or memory area into another process

Sample uses process hollowing technique

Writes to foreign memory regions

Stealing of Sensitive Information:

Yara detected HawkEye Keylogger

Yara detected MailPassView

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

Tries to steal Instant Messenger accounts or passwords

Tries to steal Mail credentials (via file access)

Tries to steal Mail credentials (via file registry)

Yara detected WebBrowserPassView password recovery tool

Remote Access Functionality:

Detected HawkEye Rat

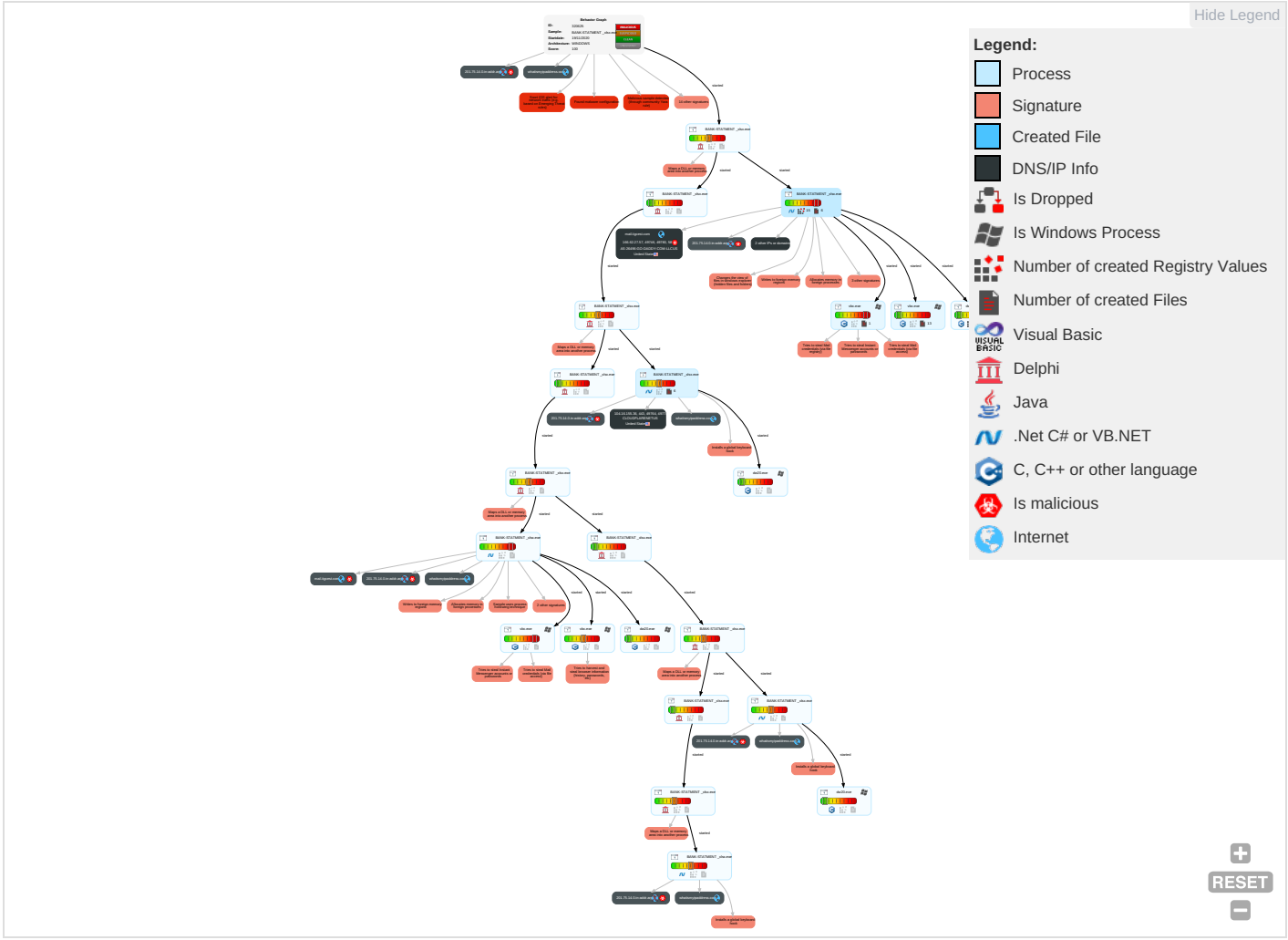
Yara detected HawkEye Keylogger

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Replication Through Removable Media 1	Windows Management Instrumentation 2 1	DLL Side-Loading 1	DLL Side-Loading 1	Disable or Modify Tools 1	OS Credential Dumping 1	System Time Discovery 1 1	Replication Through Removable Media 1	Archive Collected Data 1 1	Exfiltration Over C Network Medium
Default Accounts	Native API 1 1	Application Shimming 1	Application Shimming 1	Deobfuscate/Decode Files or Information 1 1	Input Capture 2 2 1	Peripheral Device Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth
Domain Accounts	Shared Modules 1	Logon Script (Windows)	Process Injection 5 1 2	Obfuscated Files or Information 2 1	Credentials in Registry 2	Account Discovery 1	SMB/Windows Admin Shares	Screen Capture 1	Automated Exfiltra
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Software Packing 4 1	Credentials In Files 1	File and Directory Discovery 1	Distributed Component Object Model	Email Collection 1	Scheduled Transfe
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	DLL Side-Loading 1	LSA Secrets	System Information Discovery 3 9	SSH	Input Capture 2 2 1	Data Transfer Size Limits
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Query Registry 1	VNC	Clipboard Data 3	Exfiltration Over C Channel
External Remote Services	Scheduled Task	Startup Items	Startup Items	Modify Registry 1	DCSync	Security Software Discovery 1 10 1	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protoc
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Virtualization/Sandbox Evasion 6	Proc Filesystem	Virtualization/Sandbox Evasion 6	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encryp Non-C2 Protocol
Exploit Public-Facing Application	PowerShell	At (Linux)	At (Linux)	Process Injection 5 1 2	/etc/passwd and /etc/shadow	Process Discovery 4	Software Deployment Tools	Data Staged	Exfiltration Over Asymmetric Encry Non-C2 Protocol
Supply Chain Compromise	AppleScript	At (Windows)	At (Windows)	Hidden Files and Directories 1	Network Sniffing	Application Window Discovery 1 1	Taint Shared Content	Local Data Staging	Exfiltration Over Unencrypted/Obfu Non-C2 Protocol

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration
Compromise Software Dependencies and Development Tools	Windows Command Shell	Cron	Cron	Right-to-Left Override	Input Capture	System Owner/User Discovery 1	Replication Through Removable Media	Remote Data Staging	Exfiltration Over Physical Medium
Compromise Software Supply Chain	Unix Shell	Launchd	Launchd	Rename System Utilities	Keylogging	Remote System Discovery 1	Component Object Model and Distributed COM	Screen Capture	Exfiltration over U
Compromise Hardware Supply Chain	Visual Basic	Scheduled Task	Scheduled Task	Masquerade Task or Service	GUI Input Capture	System Network Configuration Discovery 1	Exploitation of Remote Services	Email Collection	Commonly Used P

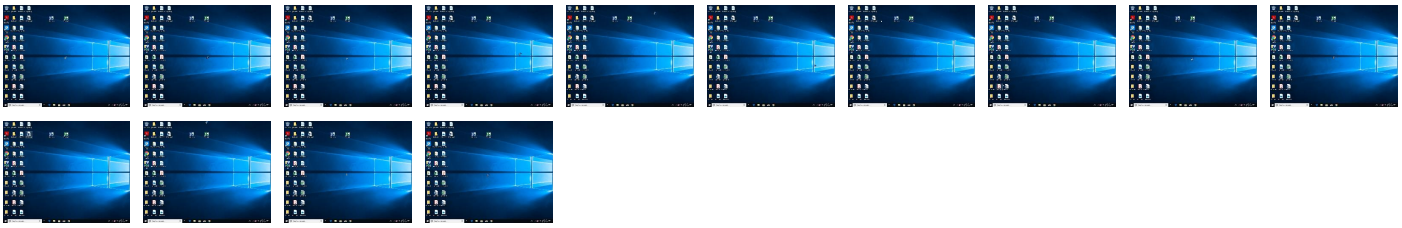
Behavior Graph



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
BANK-STATMENT _xlsx.exe	40%	Virustotal		Browse
BANK-STATMENT _xlsx.exe	42%	ReversingLabs	Win32.Trojan.LokiBot	
BANK-STATMENT _xlsx.exe	100%	Joe Sandbox ML		

Dropped Files

No Antivirus matches

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
29.2.BANK-STATMENT _xlsx.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File

Source	Detection	Scanner	Label	Link	Download
29.2.BANK-STATMENT _xlsx.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
33.2.BANK-STATMENT _xlsx.exe.25e0000.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
37.2.BANK-STATMENT _xlsx.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
14.2.BANK-STATMENT _xlsx.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
21.2.BANK-STATMENT _xlsx.exe.21e0000.2.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
21.2.BANK-STATMENT _xlsx.exe.21e0000.2.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
1.2.BANK-STATMENT _xlsx.exe.23b0000.3.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
1.2.BANK-STATMENT _xlsx.exe.23b0000.3.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
16.2.BANK-STATMENT _xlsx.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
7.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
2.2.BANK-STATMENT _xlsx.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
34.2.BANK-STATMENT _xlsx.exe.2400000.3.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
34.2.BANK-STATMENT _xlsx.exe.2400000.3.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
1.2.BANK-STATMENT _xlsx.exe.2290000.2.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
1.2.BANK-STATMENT _xlsx.exe.2290000.2.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
28.2.BANK-STATMENT _xlsx.exe.27a0000.3.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
28.2.BANK-STATMENT _xlsx.exe.27a0000.3.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
29.1.BANK-STATMENT _xlsx.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
38.2.BANK-STATMENT _xlsx.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
38.2.BANK-STATMENT _xlsx.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
15.2.BANK-STATMENT _xlsx.exe.2310000.3.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
15.2.BANK-STATMENT _xlsx.exe.2310000.3.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
0.2.BANK-STATMENT _xlsx.exe.2780000.3.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
0.2.BANK-STATMENT _xlsx.exe.2780000.3.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
15.2.BANK-STATMENT _xlsx.exe.2250000.2.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
15.2.BANK-STATMENT _xlsx.exe.2250000.2.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
28.2.BANK-STATMENT _xlsx.exe.2750000.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
1.1.BANK-STATMENT _xlsx.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
21.2.BANK-STATMENT _xlsx.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
21.2.BANK-STATMENT _xlsx.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
15.2.BANK-STATMENT _xlsx.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
15.2.BANK-STATMENT _xlsx.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
29.2.BANK-STATMENT _xlsx.exe.23d0000.2.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
29.2.BANK-STATMENT _xlsx.exe.23d0000.2.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
20.2.BANK-STATMENT _xlsx.exe.26b0000.3.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
20.2.BANK-STATMENT _xlsx.exe.26b0000.3.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
31.2.BANK-STATMENT _xlsx.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
29.2.BANK-STATMENT _xlsx.exe.ad0000.1.unpack	100%	Avira	TR/Inject.vcoldi		Download File
20.2.BANK-STATMENT _xlsx.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
1.2.BANK-STATMENT _xlsx.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
1.2.BANK-STATMENT _xlsx.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
14.2.BANK-STATMENT _xlsx.exe.25e0000.2.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
35.2.BANK-STATMENT _xlsx.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
28.2.BANK-STATMENT _xlsx.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
34.1.BANK-STATMENT _xlsx.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
0.2.BANK-STATMENT _xlsx.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
38.1.BANK-STATMENT _xlsx.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
33.2.BANK-STATMENT _xlsx.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
26.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
23.2.BANK-STATMENT _xlsx.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
34.2.BANK-STATMENT _xlsx.exe.22d0000.1.unpack	100%	Avira	TR/Inject.vcoldi		Download File
21.2.BANK-STATMENT _xlsx.exe.22c0000.3.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File

Source	Detection	Scanner	Label	Link	Download
21.2.BANK-STATMENT _xlsx.exe.22c0000.3.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
39.2.BANK-STATMENT _xlsx.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1131223		Download File
21.1.BANK-STATMENT _xlsx.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File
15.2.BANK-STATMENT _xlsx.exe.810000.1.unpack	100%	Avira	TR/Inject.vcoldi		Download File
38.2.BANK-STATMENT _xlsx.exe.2350000.3.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
38.2.BANK-STATMENT _xlsx.exe.2350000.3.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
21.2.BANK-STATMENT _xlsx.exe.2150000.1.unpack	100%	Avira	TR/Inject.vcoldi		Download File
29.2.BANK-STATMENT _xlsx.exe.2460000.3.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
29.2.BANK-STATMENT _xlsx.exe.2460000.3.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
37.2.BANK-STATMENT _xlsx.exe.27c0000.3.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
37.2.BANK-STATMENT _xlsx.exe.27c0000.3.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
33.2.BANK-STATMENT _xlsx.exe.2640000.3.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
33.2.BANK-STATMENT _xlsx.exe.2640000.3.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
34.2.BANK-STATMENT _xlsx.exe.400000.0.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
34.2.BANK-STATMENT _xlsx.exe.400000.0.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
14.2.BANK-STATMENT _xlsx.exe.2640000.3.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
14.2.BANK-STATMENT _xlsx.exe.2640000.3.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
38.2.BANK-STATMENT _xlsx.exe.2230000.1.unpack	100%	Avira	TR/Inject.vcoldi		Download File
34.2.BANK-STATMENT _xlsx.exe.2360000.2.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
34.2.BANK-STATMENT _xlsx.exe.2360000.2.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
1.2.BANK-STATMENT _xlsx.exe.9d0000.1.unpack	100%	Avira	TR/Inject.vcoldi		Download File
38.2.BANK-STATMENT _xlsx.exe.22c0000.2.unpack	100%	Avira	TR/AD.MExecute.lzrac		Download File
38.2.BANK-STATMENT _xlsx.exe.22c0000.2.unpack	100%	Avira	SPR/Tool.MailPassView.473		Download File
15.1.BANK-STATMENT _xlsx.exe.400000.0.unpack	100%	Avira	TR/Crypt.XPACK.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://www.carterandcone.comsig	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.carterandcone.com#	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/://w7	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/typo	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnrb	0%	Avira URL Cloud	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0s	0%	Avira URL Cloud	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.carterandcone.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/alny	0%	Avira URL Cloud	safe	
http://whatismyipaddress.comx&	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cnD	0%	Avira URL Cloud	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	
http://www.typography.netD	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.typography.netD	0%	URL Reputation	safe	
http://www.fontbureau.com)	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	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://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.galapagosdesign.com/staff/dennis.htm	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/7	0%	Avira URL Cloud	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://fontfabrik.com	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/font	0%	Avira URL Cloud	safe	
http://www.fontbureau.comcom	0%	URL Reputation	safe	
http://www.fontbureau.comcom	0%	URL Reputation	safe	
http://www.fontbureau.comcom	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/)	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/N	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/Norm	0%	Avira URL Cloud	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.sandoll.co.kr	0%	URL Reputation	safe	
http://www.founder.com.cn/cnZ	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.sakkal.com	0%	URL Reputation	safe	
http://www.fontbureau.comueed	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.galapagosdesign.com/	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.fontbureau.comF	0%	URL Reputation	safe	
http://www.galapagosdesign.com/S	0%	Avira URL Cloud	safe	
http://www.carterandcone.comc	0%	Avira URL Cloud	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.carterandcone.comTC	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/N	0%	Avira URL Cloud	safe	
http://https://whatismyipaddress.comx&	0%	Avira URL Cloud	safe	
http://go.microsoft.	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/E	0%	Avira URL Cloud	safe	
http://go.microsoft.LinkId=42127	0%	Avira URL Cloud	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/jp/	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.coma	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.fontbureau.comd	0%	URL Reputation	safe	
http://www.carterandcone.comg	0%	Avira URL Cloud	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	

Source	Detection	Scanner	Label	Link
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.jiyu-kobo.co.jp/Y0nt	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.founder.com.cn/cn	0%	URL Reputation	safe	
http://www.fontbureau.come	0%	Avira URL Cloud	safe	
http://www.fontbureau.comoitu	0%	URL Reputation	safe	

Domains and IPs

Contacted Domains

Name	IP	Active	Malicious	Antivirus Detection	Reputation
whatismyipaddress.com	104.16.154.36	true	false		high
mail.iigcest.com	166.62.27.57	true	true		unknown
201.75.14.0.in-addr.arpa	unknown	unknown	true		unknown

Contacted URLs

Name	Malicious	Antivirus Detection	Reputation
http://whatismyipaddress.com/	false		high

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comsig	BANK-STATMENT _xlsx.exe, 00000001.00000003.670678801.0000000005126000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersG	BANK-STATMENT _xlsx.exe, 00000001.00000002.773771914.0000000005260000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000000F.00000002.804652091.00000000050E0000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000015.00000002.858940820.00000000050E0000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000001D.00000002.887749942.0000000005220000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000022.00000002.917199610.0000000005250000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com/designers/?	BANK-STATMENT _xlsx.exe, 00000001.00000002.773771914.0000000005260000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000000F.00000002.804652091.00000000050E0000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000015.00000002.858940820.00000000050E0000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000001D.00000002.887749942.0000000005220000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000022.00000002.917199610.0000000005250000.00000002.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn/bThe	BANK-STATMENT _xlsx.exe, 00000001.00000002.773771914.0000000005260000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000000F.00000002.804652091.00000050E0000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000015.00000002.858940820.00000000050E0000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000001D.00000002.887749942.0000000005220000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000022.00000002.917199610.0000000005250000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com#	BANK-STATMENT _xlsx.exe, 00000001.00000003.671131128.0000000005127000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/://w7	BANK-STATMENT _xlsx.exe, 00000001.00000003.671578581.00000000050F4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers?	BANK-STATMENT _xlsx.exe, 00000001.00000002.773771914.0000000005260000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000000F.00000002.804652091.00000050E0000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000015.00000002.858940820.00000000050E0000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000001D.00000002.887749942.0000000005220000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000022.00000002.917199610.0000000005250000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/typo	BANK-STATMENT _xlsx.exe, 00000001.00000003.672478858.00000000050FA000.00000004.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000001.00000003.672193622.00000050FB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cnrb	BANK-STATMENT _xlsx.exe, 00000001.00000003.668963519.0000000000510A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.tiro.com	BANK-STATMENT _xlsx.exe, 00000022.00000002.917199610.0000000005250000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/Y0s	BANK-STATMENT _xlsx.exe, 00000001.00000003.672478858.00000000050FA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers	BANK-STATMENT _xlsx.exe, 00000022.00000002.917199610.0000000005250000.00000002.00000001.sdmp	false		high
http://www.goodfont.co.kr	BANK-STATMENT _xlsx.exe, 00000001.00000002.773771914.0000000005260000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000000F.00000002.804652091.00000050E0000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000015.00000002.858940820.00000000050E0000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000001D.00000002.887749942.0000000005220000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000022.00000002.917199610.0000000005250000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.com	BANK-STATMENT _xlsx.exe, 00000001.00000003.670678801.0000000005126000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/alny	BANK-STATMENT _xlsx.exe, 00000001.00000003.672193622.00000000050FB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designersS	BANK-STATMENT _xlsx.exe, 00000001.00000003.676434970.0000000005128000.00000004.00000001.sdmp	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://whatismyipaddress.comx&	BANK-STATMENT _xlsx.exe, 00000 00F.00000002.801748838.0000000 002B0E000.00000004.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0 000001D.00000002.884820790.000 0000002B4E000.00000004.0000000 1.sdmp, BANK-STATMENT _xlsx.exe, 00000022.00000002.915036172 .0000000002C3E000.00000004.000 00001.sdmp	false	• Avira URL Cloud: safe	low
http://www.founder.com.cn/cnD	BANK-STATMENT _xlsx.exe, 00000 001.00000003.669162564.0000000 005122000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sajatypeworks.com	BANK-STATMENT _xlsx.exe, 00000 001.00000002.773771914.0000000 005260000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0 000000F.00000002.804652091.000 00000050E0000.00000002.0000000 1.sdmp, BANK-STATMENT _xlsx.exe, 00000015.00000002.858940820 .00000000050E0000.00000002.000 00001.sdmp, BANK-STATMENT _xls x.exe, 0000001D.00000002.88774 9942.0000000005220000.00000002 .00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000022.00000002.9 17199610.0000000005250000.0000 0002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.typography.netD	BANK-STATMENT _xlsx.exe, 00000 001.00000002.773771914.0000000 005260000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0 000000F.00000002.804652091.000 00000050E0000.00000002.0000000 1.sdmp, BANK-STATMENT _xlsx.exe, 00000015.00000002.858940820 .00000000050E0000.00000002.000 00001.sdmp, BANK-STATMENT _xls x.exe, 0000001D.00000002.88774 9942.0000000005220000.00000002 .00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000022.00000002.9 17199610.0000000005250000.0000 0002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com)	BANK-STATMENT _xlsx.exe, 00000 001.00000002.773005820.0000000 005100000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	low
http://www.founder.com.cn/cn/cThe	BANK-STATMENT _xlsx.exe, 00000 001.00000002.773771914.0000000 005260000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0 000000F.00000002.804652091.000 00000050E0000.00000002.0000000 1.sdmp, BANK-STATMENT _xlsx.exe, 00000015.00000002.858940820 .00000000050E0000.00000002.000 00001.sdmp, BANK-STATMENT _xls x.exe, 0000001D.00000002.88774 9942.0000000005220000.00000002 .00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000022.00000002.9 17199610.0000000005250000.0000 0002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/staff/dennis.htm	BANK-STATMENT _xlsx.exe, 00000 001.00000002.773771914.0000000 005260000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0 000000F.00000002.804652091.000 00000050E0000.00000002.0000000 1.sdmp, BANK-STATMENT _xlsx.exe, 00000015.00000002.858940820 .00000000050E0000.00000002.000 00001.sdmp, BANK-STATMENT _xls x.exe, 0000001D.00000002.88774 9942.0000000005220000.00000002 .00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000022.00000002.9 17199610.0000000005250000.0000 0002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/7	BANK-STATMENT _xlsx.exe, 00000 001.00000003.672478858.0000000 0050FA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://fontfabrik.com	BANK-STATMENT _xlsx.exe, 00000001.00000002.773771914.0000000005260000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000000F.00000002.804652091.00000000050E0000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000015.00000002.858940820.00000000050E0000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000001D.00000002.887749942.0000000005220000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000022.00000002.917199610.0000000005250000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/font	BANK-STATMENT _xlsx.exe, 00000001.00000003.671578581.0000000050F4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.msn.com/de-ch/?ocid=iehpHLMEMh	vbc.exe, 0000001A.00000002.838373686.0000000000758000.00000004.00000020.sdmp	false		high
http://www.fontbureau.comcom	BANK-STATMENT _xlsx.exe, 00000001.00000003.676664424.0000000050FF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designersd	BANK-STATMENT _xlsx.exe, 00000001.00000003.676177368.0000000005121000.00000004.00000001.sdmp	false		high
http://whatismyipaddress.com/-	BANK-STATMENT _xlsx.exe, 00000000.00000002.666309079.0000000002817000.00000040.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000001.00000002.765706717.0000000497000.00000040.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000000E.00000002.788401031.0000000002642000.00000040.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000000F.00000002.799181132.0000000002312000.00000040.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000014.00000002.826494513.0000000002747000.00000040.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000015.00000002.852456722.0000000000402000.00000040.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000001C.00000002.870010845.00000000027A2000.00000040.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000001D.00000002.883042234.0000000000AD0000.00000004.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000021.00000002.903399921.0000000002642000.00000040.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000022.00000002.912614884.0000000002362000.00000004.00000001.sdmp	false		high
http://www.galapagosdesign.com/DPlease	BANK-STATMENT _xlsx.exe, 00000001.00000002.773771914.0000000005260000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000000F.00000002.804652091.00000000050E0000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000015.00000002.858940820.00000000050E0000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000001D.00000002.887749942.0000000005220000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000022.00000002.917199610.0000000005250000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/)	BANK-STATMENT _xlsx.exe, 00000001.00000003.672478858.0000000050FA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/jp/N	BANK-STATMENT _xlsx.exe, 00000001.00000003.672193622.0000000050FB000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://login.yahoo.com/config/login	BANK-STATMENT _xlsx.exe, vbc.exe	false		high

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.fonts.com	BANK-STATMENT _xlsx.exe, 00000001.00000002.773771914.0000000005260000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000000F.00000002.804652091.00000000050E0000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000015.00000002.858940820.00000000050E0000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000001D.00000002.887749942.0000000005220000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000022.00000002.917199610.0000000005250000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/Norm	BANK-STATMENT _xlsx.exe, 00000001.00000003.671578581.00000000050F4000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.sandoll.co.kr	BANK-STATMENT _xlsx.exe, 00000001.00000002.773771914.0000000005260000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000000F.00000002.804652091.00000000050E0000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000015.00000002.858940820.00000000050E0000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000001D.00000002.887749942.0000000005220000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000022.00000002.917199610.0000000005250000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.site.com/logs.php	BANK-STATMENT _xlsx.exe, 00000022.00000002.915036172.000000002C3E000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cnZ	BANK-STATMENT _xlsx.exe, 00000001.00000003.669162564.0000000005122000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.urwpp.deDPlease	BANK-STATMENT _xlsx.exe, 00000001.00000002.773771914.0000000005260000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000000F.00000002.804652091.00000000050E0000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000015.00000002.858940820.00000000050E0000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000001D.00000002.887749942.0000000005220000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000022.00000002.917199610.0000000005250000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.nirsoft.net/	BANK-STATMENT _xlsx.exe, 00000022.00000002.912614884.0000000002362000.00000004.00000001.sdmp	false		high
http://www.zhongyicts.com.cn	BANK-STATMENT _xlsx.exe, 00000001.00000002.773771914.0000000005260000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000000F.00000002.804652091.00000000050E0000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000015.00000002.858940820.00000000050E0000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000001D.00000002.887749942.0000000005220000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000022.00000002.917199610.0000000005250000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

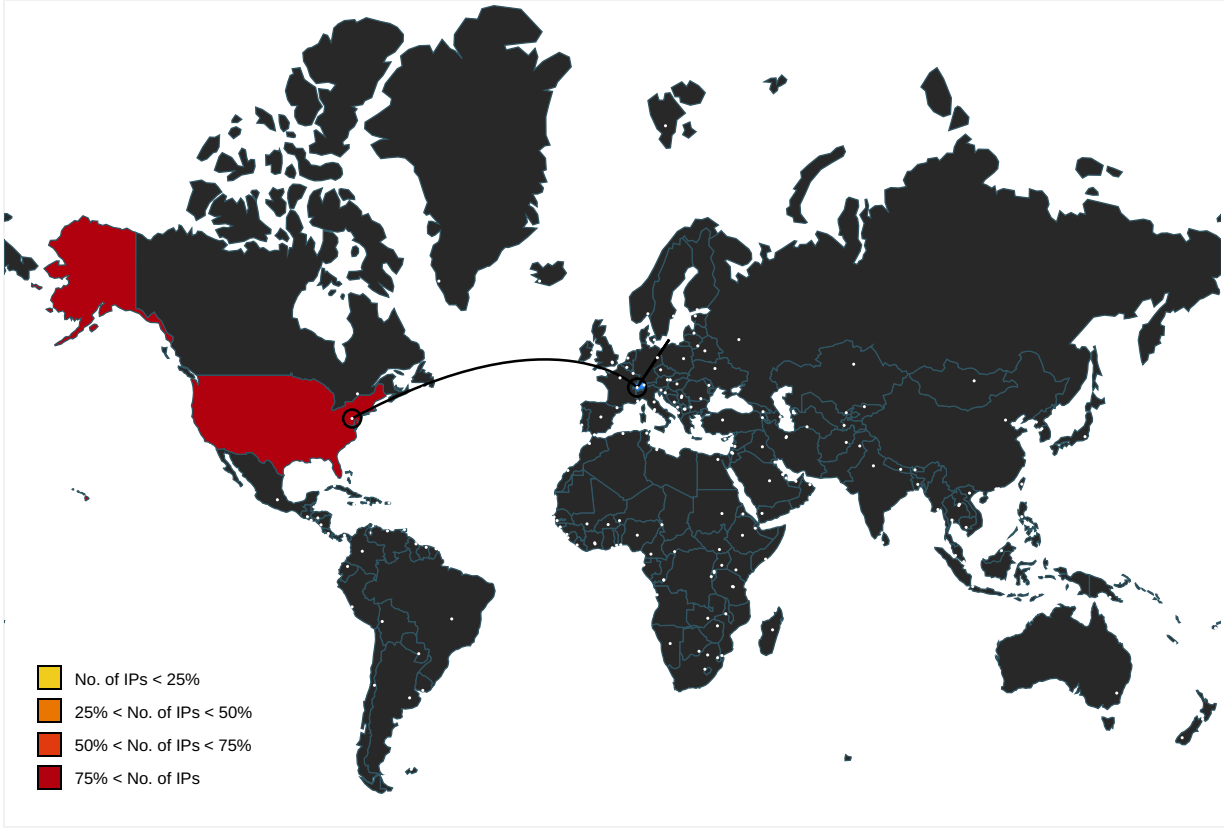
Name	Source	Malicious	Antivirus Detection	Reputation
http://www.sakkal.com	BANK-STATMENT _xlsx.exe, 00000001.00000002.773771914.0000000005260000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000000F.00000002.804652091.00000050E0000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000015.00000002.858940820.00000000050E0000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000001D.00000002.887749942.0000000005220000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000022.00000002.917199610.0000000005250000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comueed	BANK-STATMENT _xlsx.exe, 00000001.00000003.676664424.00000000050FF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designerst	BANK-STATMENT _xlsx.exe, 00000001.00000003.674765089.0000000005121000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cnd	BANK-STATMENT _xlsx.exe, 00000001.00000003.669404161.0000000005123000.00000004.00000001.sdmp	false		unknown
http://https://whatismyipaddress.com/	BANK-STATMENT _xlsx.exe, 0000001D.00000002.885555940.0000000002F14000.00000004.00000001.sdmp	false		high
http://www.apache.org/licenses/LICENSE-2.0	BANK-STATMENT _xlsx.exe, 00000001.00000003.670079069.0000000005123000.00000004.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000000F.00000002.804652091.00000050E0000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000015.00000002.858940820.00000000050E0000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000001D.00000002.887749942.0000000005220000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000022.00000002.917199610.0000000005250000.00000002.00000001.sdmp	false		high
http://www.fontbureau.com	BANK-STATMENT _xlsx.exe, 00000001.00000002.773771914.0000000005260000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000000F.00000002.804652091.00000050E0000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000015.00000002.858940820.00000000050E0000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000001D.00000002.887749942.0000000005220000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000022.00000002.917199610.0000000005250000.00000002.00000001.sdmp	false		high
http://www.galapagosdesign.com/	BANK-STATMENT _xlsx.exe, 00000001.00000003.678233333.00000000050FF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://whatismyipaddress.com	BANK-STATMENT _xlsx.exe, 00000001.00000002.770219917.0000000002AF1000.00000004.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000000F.00000002.803423064.0000000002ED4000.00000004.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000015.00000002.855941175.0000000002A31000.00000004.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000001D.00000002.885555940.0000000002F14000.00000004.00000001.sdmp	false		high
http://www.fontbureau.comF	BANK-STATMENT _xlsx.exe, 00000001.00000003.675782658.00000000050FF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.galapagosdesign.com/S	BANK-STATMENT _xlsx.exe, 00000001.00000003.678233333.00000000050FF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.carterandcone.comc	BANK-STATMENT _xlsx.exe, 00000001.00000003.670925242.0000000 0050FC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.comTC	BANK-STATMENT _xlsx.exe, 00000001.00000003.671889636.0000000 0050FB000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.jiyu-kobo.co.jp/N	BANK-STATMENT _xlsx.exe, 00000001.00000003.672478858.0000000 0050FA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://whatismyipaddress.comx&	BANK-STATMENT _xlsx.exe, 00000 00F.00000002.803423064.0000000 002ED4000.00000004.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0 000001D.00000002.885555940.000 0000002F14000.00000004.0000000 1.sdmp	false	• Avira URL Cloud: safe	low
http://go.microsoft.	BANK-STATMENT _xlsx.exe, 00000 01D.00000002.882848976.0000000 0007BD000.00000004.00000020.sdmp, BANK-STATMENT _xlsx.exe, 0 0000022.00000002.912205260.000 000000077B000.00000004.0000002 0.sdmp	false	• Avira URL Cloud: safe	unknown
http://whatismyipaddress.com	BANK-STATMENT _xlsx.exe, 00000001.00000002.770219917.0000000 002AF1000.00000004.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0 000000F.00000002.801748838.000 0000002B0E000.00000004.0000000 1.sdmp, BANK-STATMENT _xlsx.exe, 00000015.00000002.855941175 .0000000002A31000.00000004.000 00001.sdmp, BANK-STATMENT _xls x.exe, 0000001D.00000002.88482 0790.0000000002B4E000.00000004 .00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000022.00000002.9 15036172.0000000002C3E000.0000 0004.00000001.sdmp	false		high
http://www.fontbureau.com/designersno	BANK-STATMENT _xlsx.exe, 00000001.00000003.682397058.0000000 005121000.00000004.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/E	BANK-STATMENT _xlsx.exe, 00000001.00000003.672478858.0000000 0050FA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contextual.media.net/	vbc.exe, 0000001A.00000002.838 399630.000000000076E000.000000 04.00000020.sdmp	false		high
http://go.microsoft.LinkId=42127	BANK-STATMENT _xlsx.exe, 00000 01D.00000002.882848976.0000000 0007BD000.00000004.00000020.sdmp, BANK-STATMENT _xlsx.exe, 0 0000022.00000002.912205260.000 000000077B000.00000004.0000002 0.sdmp	false	• Avira URL Cloud: safe	low
http://www.jiyu-kobo.co.jp/jp/	BANK-STATMENT _xlsx.exe, 00000001.00000003.672478858.0000000 0050FA000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.coma	BANK-STATMENT _xlsx.exe, 00000001.00000003.676664424.0000000 0050FF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.comd	BANK-STATMENT _xlsx.exe, 00000001.00000003.676664424.0000000 0050FF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comg	BANK-STATMENT _xlsx.exe, 00000001.00000003.670678801.0000000 005126000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.carterandcone.coml	BANK-STATMENT _xlsx.exe, 00000001.00000002.773771914.0000000 005260000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0 000000F.00000002.804652091.000 00000050E0000.00000002.0000000 1.sdmp, BANK-STATMENT _xlsx.exe, 00000015.00000002.858940820 .00000000050E0000.00000002.000 00001.sdmp, BANK-STATMENT _xls x.exe, 0000001D.00000002.88774 9942.0000000005220000.00000002 .00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000022.00000002.9 17199610.0000000005250000.0000 0002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.jiyu-kobo.co.jp/Y0nt	BANK-STATMENT _xlsx.exe, 00000001.00000003.672478858.00000000050FA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.founder.com.cn/cn/	BANK-STATMENT _xlsx.exe, 00000001.00000003.669521206.00000000005105000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/cabarga.htmlN	BANK-STATMENT _xlsx.exe, 00000001.00000002.773771914.00000000005260000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000000F.00000002.804652091.00000000050E0000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000015.00000002.858940820.00000000050E0000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000001D.00000002.887749942.0000000005220000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000022.00000002.917199610.0000000005250000.00000002.00000001.sdmp	false		high
http://www.founder.com.cn/cn	BANK-STATMENT _xlsx.exe, 00000001.00000002.773771914.00000000005260000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000001.00000003.669103284.00000000005122000.00000004.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000000F.00000002.804652091.00000000050E0000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000015.00000002.858940820.00000000050E0000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000001D.00000002.887749942.0000000005220000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000022.00000002.917199610.0000000005250000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.fontbureau.com/designers/frere-user.html	BANK-STATMENT _xlsx.exe, 00000001.00000002.773771914.00000000005260000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000000F.00000002.804652091.00000000050E0000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000015.00000002.858940820.00000000050E0000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000001D.00000002.887749942.0000000005220000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000022.00000002.917199610.0000000005250000.00000002.00000001.sdmp	false		high
http://www.fontbureau.come	BANK-STATMENT _xlsx.exe, 00000001.00000002.773005820.00000000005100000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comoitu	BANK-STATMENT _xlsx.exe, 00000001.00000003.675782658.00000000050FF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.carterandcone.comz	BANK-STATMENT _xlsx.exe, 00000001.00000003.670800155.00000000005106000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.com/designers/cabarga.html	BANK-STATMENT _xlsx.exe, 00000001.00000003.675887823.00000000512B000.00000004.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000001.00000003.675857787.000000000512A000.00000004.00000001.sdmp	false		high
http://www.founder.com.cn/cn7	BANK-STATMENT _xlsx.exe, 00000001.00000003.668963519.00000000510A000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://static-global-s-msn-com.ak	vbc.exe, 0000001A.00000002.838399630.000000000076E000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.fontbureau.comcomF	BANK-STATMENT _xlsx.exe, 00000001.00000003.676664424.00000000050FF000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://www.founder.com.cn/cn8	BANK-STATMENT _xlsx.exe, 00000001.00000003.669162564.00000000005122000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.jiyu-kobo.co.jp/	BANK-STATMENT _xlsx.exe, 00000001.00000002.773771914.0000000005260000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000000.00000003.672193622.00000000050FB000.00000004.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000001.00000003.671578581.00000000050F4000.00000004.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000000F.00000002.804652091.00000000050E0000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000015.00000002.858940820.00000000050E0000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000001D.00000002.887749942.0000000005220000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000022.00000002.917199610.0000000005250000.00000002.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://https://contextual.media.net/checksync.php?&vsSyn	vbc.exe, 0000001A.00000002.838399630.000000000076E000.00000004.00000020.sdmp	false		high
http://www.fontbureau.com/designers8	BANK-STATMENT _xlsx.exe, 00000001.00000002.773771914.0000000005260000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000000F.00000002.804652091.00000000050E0000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000015.00000002.858940820.00000000050E0000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 0000001D.00000002.887749942.0000000005220000.00000002.00000001.sdmp, BANK-STATMENT _xlsx.exe, 00000022.00000002.917199610.0000000005250000.00000002.00000001.sdmp	false		high
http://www.jiyu-kobo.co.jp/j	BANK-STATMENT _xlsx.exe, 00000001.00000003.672478858.00000000050FA000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown
http://www.msn.com/?ocid=iehpEM3LMEM	vbc.exe, 0000001A.00000002.838373686.0000000000758000.00000004.00000020.sdmp	false		high
http://www.fontbureau.comalic	BANK-STATMENT _xlsx.exe, 00000001.00000003.676664424.00000000050FF000.00000004.00000001.sdmp	false	• URL Reputation: safe • URL Reputation: safe • URL Reputation: safe	unknown
http://www.tiro.comic	BANK-STATMENT _xlsx.exe, 00000001.00000003.670925242.00000000050FC000.00000004.00000001.sdmp	false	• Avira URL Cloud: safe	unknown

Contacted IPs



Public

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
104.16.154.36	unknown	United States		13335	CLOUDFLARENETUS	false
104.16.155.36	unknown	United States		13335	CLOUDFLARENETUS	false
166.62.27.57	unknown	United States		26496	AS-26496-GO-DADDY-COM-LLCUS	true

Private

IP
192.168.2.1

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	320625
Start date:	19.11.2020
Start time:	16:01:48
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 14m 44s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	BANK-STATMENT _xlsx.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:	40
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.phis.troj.spyw.evad.winEXE@53/29@20/4
EGA Information:	Failed
HDC Information:	• Successful, ratio: 80.4% (good quality ratio 78.5%) • Quality average: 85.2% • Quality standard deviation: 24%
HCA Information:	• Successful, ratio: 87% • 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 • Exclude process from analysis (whitelisted): BackgroundTransferHost.exe, backgroundTaskHost.exe, svchost.exe, wuapihost.exe • TCP Packets have been reduced to 100 • Excluded IPs from analysis (whitelisted): 52.255.188.83, 40.88.32.150, 51.104.144.132, 2.20.142.210, 2.20.142.209, 52.155.217.156, 20.54.26.129, 92.122.213.194, 92.122.213.247, 52.147.198.201 • Excluded domains from analysis (whitelisted): au.download.windowsupdate.com.edgesuite.net, displaycatalog-europeeap.md.mp.microsoft.com.akadns.net, arc.msn.com.nsatc.net, displaycatalog.md.mp.microsoft.com.akadns.net, ris-prod.trafficmanager.net, ctldl.windowsupdate.com, a767.dscg3.akamai.net, a1449.dscg2.akamai.net, arc.msn.com, db5eap.displaycatalog.md.mp.microsoft.com.akadns.net, ris.api.iris.microsoft.com, skypedataprdcoleus16.cloudapp.net, skypedataprdcoleus15.cloudapp.net, umwatsonrouting.trafficmanager.net, skypedataprdcoleus17.cloudapp.net, audownload.windowsupdate.nsatc.net, displaycatalog.mp.microsoft.com, watson.telemetry.microsoft.com, img-prod-cms-rt-microsoft-com.akamaized.net, au-bg-shim.trafficmanager.net • Report creation exceeded maximum time and may have missing disassembly code information. • Report size exceeded maximum capacity and may have missing behavior information. • Report size exceeded maximum capacity and may have missing disassembly code. • Report size getting too big, too many NtAllocateVirtualMemory calls found. • Report size getting too big, too many NtDeviceIoControlFile calls found. • Report size getting too big, too many NtOpenKeyEx calls found. • Report size getting too big, too many NtProtectVirtualMemory calls found. • Report size getting too big, too many NtQueryValueKey calls found.

Simulations

Behavior and APIs

Time	Type	Description
16:02:55	API Interceptor	63x Sleep call for process: BANK-STATMENT _xlsx.exe modified
16:03:31	API Interceptor	5x Sleep call for process: dw20.exe modified

Joe Sandbox View / Context

IPs

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
104.16.154.36	INQUIRY.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	c9o0CtTIYT.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	6JLHKYvboo.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	khJdbt0clZ.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	ZMOKwXqVHO.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	5Av43Q5IXd.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	8oaZfXDstn.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	9vdouqRTh3.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	M9RhKQ1G91.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	0CyK3Y7XBs.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	pwYhlZGMa6.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	Vll6ZcOkEQ.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	oLHQIQAI3N.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	YrHUxpftPs.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	WuGzF7ZJ7P.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	cj9weNQmT2.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	lk5M5Q97c3.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	2v7Vtqfo81.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	Enquiry_pdf.exe	Get hash	malicious	Browse	• whatismyipaddress.com/
	KM4ukzS8ER.exe	Get hash	malicious	Browse	• whatismyipaddress.com/

Domains

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
whatismyipaddress.com	INQUIRY.exe	Get hash	malicious	Browse	• 104.16.154.36
	Prueba de pago.exe	Get hash	malicious	Browse	• 104.16.155.36
	879mgDuqEE.jar	Get hash	malicious	Browse	• 66.171.248.178
	remittance1111.jar	Get hash	malicious	Browse	• 66.171.248.178
	879mgDuqEE.jar	Get hash	malicious	Browse	• 66.171.248.178
	remittance1111.jar	Get hash	malicious	Browse	• 66.171.248.178
	http://https://my-alliances.co.uk/	Get hash	malicious	Browse	• 66.171.248.178
	c9o0CtTIYT.exe	Get hash	malicious	Browse	• 104.16.154.36
	mR3CdUkyLL.exe	Get hash	malicious	Browse	• 104.16.155.36
	6JLHKYvboo.exe	Get hash	malicious	Browse	• 104.16.155.36
	jSMd8npgmU.exe	Get hash	malicious	Browse	• 104.16.155.36
	khJdbt0clZ.exe	Get hash	malicious	Browse	• 104.16.154.36
	ZMOKwXqVHO.exe	Get hash	malicious	Browse	• 104.16.154.36
	5Av43Q5IXd.exe	Get hash	malicious	Browse	• 104.16.154.36
	8oaZfXDstn.exe	Get hash	malicious	Browse	• 104.16.154.36
	RXk6PjNTN8.exe	Get hash	malicious	Browse	• 104.16.155.36
	9vdouqRTh3.exe	Get hash	malicious	Browse	• 104.16.154.36
	5pB35gGfZ5.exe	Get hash	malicious	Browse	• 104.16.155.36
	M9RhKQ1G91.exe	Get hash	malicious	Browse	• 104.16.154.36

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	0CyK3Y7XBs.exe	Get hash	malicious	Browse	• 104.16.154.36
mail.iigcest.com	INQUIRY.exe	Get hash	malicious	Browse	• 166.62.27.57
	Vll6ZcOkEQ.exe	Get hash	malicious	Browse	• 166.62.27.57
	x2rzwu7CQ3.exe	Get hash	malicious	Browse	• 166.62.27.57
	X62RG9z7kY.exe	Get hash	malicious	Browse	• 166.62.27.57
	SWIFT100892220-PDF.exe	Get hash	malicious	Browse	• 166.62.27.57
	SWIFT0079111-pdf.exe	Get hash	malicious	Browse	• 166.62.27.57
	AD1-2001328L_pdf.exe	Get hash	malicious	Browse	• 166.62.27.57

ASN

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
CLOUDFLARENETUS	http://https://my.freshbooks.com/#/link/eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJzeXN0ZW1pZCI6OTQ3OTM1LCJ1c2VyaWQiOjYzNDYyNywidHlwZSI6Imludm9pY2UiLCJvYmplY3RpZCI6Mjg4MjQ0OSwiZXhwIjoxNjM3MjY5MTgxLCJsZXZlbCI6MH0.DGVcXxdiwtgxTUka4TzPi_o6GS8zH-kvvTnFJZxapLg?companyName=Amanda&invoiceNumber=00007767&ownerEmail=avigilante%40maxburst.com&type=primary	Get hash	malicious	Browse	• 104.16.37.47
	http://45.95.168.116	Get hash	malicious	Browse	• 104.16.19.94
	http://https://u7342898.ct.sendgrid.net/ls/click?upn=HCSIWZDf9XI-2FB6XFKqg1zjEMCja-2BnYJ5hRYKkDjy2dSVqjHsLlv5ZMXJXnh9JLSzwabeBrvYMnX699odsYkKotv4jgW-2BTippSHf276Hpn3fz0kcusnYHGKND7vKQPAS7g42-2FTb5zb8CNq57r3z9Ilg-3D-3DWdrE_hNl5WjNXy0NQcJb9Wql7qh7uPLeU7UGDRahFCFKbQLS6qwym7zJ-2B-2BhWsSSLs8pHa1w9VDlWPsA7ahHsZZucjX2ktFkSy5vhVZT2L3Jxh6b-2FoboCHa2CJGLfF19s71-2FI3WPC7rECe-2BEO9fLwbfggsNq2V1-2FqgMhzgJQL411ZuD7Y8pECisPKLf0vf9WvB1fyVO9o6Euui31Jg3e-2FDialpg2CbkM21Us8J-2FBk13yWzh58-3D	Get hash	malicious	Browse	• 104.16.125.175
	dde1df2ac5845a19823cabe182fcd870.exe	Get hash	malicious	Browse	• 104.18.108.8
	dde1df2ac5845a19823cabe182fcd870.exe	Get hash	malicious	Browse	• 104.18.107.8
	jar.jar	Get hash	malicious	Browse	• 104.20.22.46
	http://https://www.canva.com/design/DAEN3YdYVHw/zaVHWoDx-9G9l20JXWSBtg/view?utm_content=DAEN3YdYVHw&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 104.18.215.67
	http://iclickcdn.com/tag.min.js?ndn=m2	Get hash	malicious	Browse	• 104.26.12.118
	NyUnwsFSCa.exe	Get hash	malicious	Browse	• 162.159.133.233
	T-online.de.jar.zip	Get hash	malicious	Browse	• 104.20.22.46
	Order specs19.11.20.exe	Get hash	malicious	Browse	• 104.31.90.162
	Bank SWIFT Advice_pdf.exe	Get hash	malicious	Browse	• 104.28.4.151
	Purchase_Order_11_19_20.exe	Get hash	malicious	Browse	• 104.28.4.151
	http://https://signup.kwikvpn.com/	Get hash	malicious	Browse	• 104.16.19.94
	u8u7GG8XMY.exe	Get hash	malicious	Browse	• 66.235.200.147
	Uwmkxyajs0f2tlf.exe	Get hash	malicious	Browse	• 172.67.153.188
	Purchase Order 40,7045.exe	Get hash	malicious	Browse	• 172.67.199.180
	Proforma Invoice.xls	Get hash	malicious	Browse	• 104.22.1.232
	Payment Advice - Advice Ref GLV823990339.exe	Get hash	malicious	Browse	• 23.227.38.64
	Proforma Invoice.xls	Get hash	malicious	Browse	• 104.22.1.232
CLOUDFLARENETUS	http://https://my.freshbooks.com/#/link/eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJzeXN0ZW1pZCI6OTQ3OTM1LCJ1c2VyaWQiOjYzNDYyNywidHlwZSI6Imludm9pY2UiLCJvYmplY3RpZCI6Mjg4MjQ0OSwiZXhwIjoxNjM3MjY5MTgxLCJsZXZlbCI6MH0.DGVcXxdiwtgxTUka4TzPi_o6GS8zH-kvvTnFJZxapLg?companyName=Amanda&invoiceNumber=00007767&ownerEmail=avigilante%40maxburst.com&type=primary	Get hash	malicious	Browse	• 104.16.37.47
	http://45.95.168.116	Get hash	malicious	Browse	• 104.16.19.94

Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context
	http://https://u7342898.ct.sendgrid.net/ls/click?upn=HCSlWZDf9Xl-2FB6XFKqg1zjEMCja-2BnYJ5hRYKkDjy2dSVqjHsLlv5ZMXJXnh9JLSzwabeBrvYMnX699odsYkKotv4jgW-2BTippSHf276Hpn3fz0kcusnYHGKND7vKQPAS7g42-2FTb5zb8CNq57r3z9Ilg-3D-3DWdrE_hNl5WjNXy0NQcJb9Wql7qh7uPLeU7UGDRahFCFKbQLS6qwym7zJ-2B-2BhWsSSLs8pHa1w9VDlWPsA7ahHsZZucjX2ktFkSy5vhVZT2L3Jxh6b-2FoboCHa2CJGLfF19s71-2FI3WPC7rECe-2BEO9fLwbfggsNq2V1-2FqgMhzgJQL411ZuD7Y8pECisPKLf0vf9WvB1fyVO9o6Euui31Jg3e-2FDialpg2CbkM21Us8J-2FBk13yWzh58-3D	Get hash	malicious	Browse	• 104.16.125.175
	dde1df2ac5845a19823cabe182fcd870.exe	Get hash	malicious	Browse	• 104.18.108.8
	dde1df2ac5845a19823cabe182fcd870.exe	Get hash	malicious	Browse	• 104.18.107.8
	jar.jar	Get hash	malicious	Browse	• 104.20.22.46
	http://https://www.canva.com/design/DAEN3YdYVHw/zaVHWoDx-9G9l20JXWSBtg/view?utm_content=DAEN3YdYVHw&utm_campaign=designshare&utm_medium=link&utm_source=sharebutton	Get hash	malicious	Browse	• 104.18.215.67
	http://iclickcdn.com/tag.min.js?ndn=m2	Get hash	malicious	Browse	• 104.26.12.118
	NyUnwsFSCa.exe	Get hash	malicious	Browse	• 162.159.133.233
	T-online.de.jar.zip	Get hash	malicious	Browse	• 104.20.22.46
	Order specs19.11.20.exe	Get hash	malicious	Browse	• 104.31.90.162
	Bank SWIFT Advice_pdf.exe	Get hash	malicious	Browse	• 104.28.4.151
	Purchase_Order_11_19_20.exe	Get hash	malicious	Browse	• 104.28.4.151
	http://https://signup.kwikvpn.com/	Get hash	malicious	Browse	• 104.16.19.94
	u8u7GG8XMY.exe	Get hash	malicious	Browse	• 66.235.200.147
	Uwmkxyajs0f2tlf.exe	Get hash	malicious	Browse	• 172.67.153.188
	Purchase Order 40,7045.exe	Get hash	malicious	Browse	• 172.67.199.180
	Proforma Invoice.xls	Get hash	malicious	Browse	• 104.22.1.232
	Payment Advice - Advice Ref GLV823990339.exe	Get hash	malicious	Browse	• 23.227.38.64
	Proforma Invoice.xls	Get hash	malicious	Browse	• 104.22.1.232

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_bank-statment _x_319d48559b0a1af85a57a6082102ce05f64a1d9_00000000_15082965\Report.wer

Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	18590
Entropy (8bit):	3.762256301757226
Encrypted:	false
SSDEEP:	192:W9XVjIi+VpjV/C9yq5bMvg/LHZ+nNN2l1rzvq5xk0z5xT5/u7sxS274ItG:YVj6jB7vqsSt/u7sxX4ItG
MD5:	863ACDCCAAFF0865DC43E7C36A83310D
SHA1:	9546F6433676B37EB1402E9979C89BF7573691D5
SHA-256:	0837ABBBE40F4C0CF60097D061154C5D47120608DA89EE9826FC5180253A78F3
SHA-512:	215248AB9672B796C53105752B41E056B0910D94DBDEA7B9B60DFE892ACEE5C28F7FD853856421D6906A6A17D5FCAF5A01BDADE6B6DC49F7CFC9B3A49A0D19D7
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.0.2.7.1.8.2.4.3.8.0.2.7.3.3.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.0.2.7.1.8.2.5.5.8.3.3.9.4.5.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.a.6.a.a.a.1.4.0.-.a.d.f.5.-.4.9.9.9.-.b.0.1.3.-.8.2.3.e.2.d.3.d.d.a.9.e.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.0.9.0.-.0.0.0.1.-.0.0.1.b.-.3.f.d.7.-.b.a.2.9.8.5.b.e.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.0.3.a.0.1.9.e.a.a.4.c.5.0.7.1.3.0.a.a.f.2.7.2.c.4.c.d.5.0.e.d.b.0.0.0.0.f.f.f.f.!.0.0.0.0.1.b.5.5.f.b.a.2.4.2.4.6.0.c.c.0.a.5.b.3.8.2.9.9.a.c.a.a.a.c.f.3.f.5.4.c.5.e.8.7.!.B.A.N.K.-.S.T.A.T.M.E.N.T. ._.x.l.s.x...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.0././.1.1././.1.8.:.0.7.:.4.5.:.1.7.!.0.!.B.A.N.K.-.S.T.A.T.M.E.N.T. ._.x.l.s.x...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.7.2.9.5.....T.a.r.g.e.t.A.s.

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_bank-statment _x_319d48559b0a1af85a57a6082102ce05f64a1d9_00000000_1534c334\Report.wer	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	18586
Entropy (8bit):	3.7636886014541706
Encrypted:	false
SSDEEP:	192:miXVLIi+VpjV/C9yq5bMvg/LHZ+nNN2I1rzvq5xk0z5xT5/u7sWS274ltC:TVL6jB7vqsSt/u7sWX4ltC
MD5:	17613DA2429AF011D8432AF3C01E7178
SHA1:	35453EC2DD80C1F47498A0A2E75519479F1148BF
SHA-256:	B3F9F48E54441A73FD61A902B1B65B6A1C0EFB53BB7FD9AEA4BB30F6BB67A8E9
SHA-512:	6DF5B2C387295EFAFB8F7482C66BEB3A3405875587464C880EC9AE37FD2BEBC7D867E8051EF0629ABAAF7B92A24151E0247705B13076B743F22952BDC9E63134
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.0.2.7.1.8.6.3.8.6.4.5.2.0.3.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.0.2.7.1.8.6.5.0.6.7.6.3.9.7.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.1.a.2.f.b.8.a.c.-.8.e.f.d.-.4.9.1.f.-.a.8.4.7.-.b.5.4.4.6.9.f.5.2.6.b.7.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.8.2.4.-.0.0.0.1.-.0.0.1.b.-.3.b.b.9.-.e.f.4.0.8.5.b.e.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.0.3.a.0.1.9.e.a.a.4.c.5.0.7.1.3.0.a.a.f.2.7.2.c.4.c.d.5.0.e.d.b.0.0.0.0.f.f.f.f.!.0.0.0.0.1.b.5.5.f.b.a.2.4.2.4.6.0.c.c.0.a.5.b.3.8.2.9.9.a.c.a.a.a.c.f.3.f.5.4.c.5.e.8.7.!.B.A.N.K.-.S.T.A.T.M.E.N.T. ._.x.l.s.x...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.0././.1.1././.1.8.:.0.7.:.4.5.:.1.7.!.0.!.B.A.N.K.-.S.T.A.T.M.E.N.T. ._.x.l.s.x...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.7.2.9.5.....T.a.r.g.e.t.A.s.

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_bank-statment _x_319d48559b0a1af85a57a6082102ce05f64a1d9_00000000_17308cf2\Report.wer	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	18590
Entropy (8bit):	3.7637503088136137
Encrypted:	false
SSDEEP:	192:7RyXVYIi+VpjV/C9yq5bMvg/LHZ+nNN2I1rzvq5xk0z5xT5/u7sxS274Itv:sVY6jB7vqsSt/u7sxX4Itv
MD5:	9F4280CAC01546D61470D797E0431BCA
SHA1:	26EE8489F4611F285074202579D7820EDA7F537D
SHA-256:	FB04737A0C746098A4684211CF906B85B0EA6042672A84D5B565E1CFB0D78FD4
SHA-512:	76E38887B92EA678D3BC91AA63EB13CA350C8854966EDC2AB69B079E7DD8447D3CD8A7E82644538C30F0FBBC2F21C28CC2AA8CD0B22E9926FE61DCBF7C278B8
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.0.2.7.1.8.3.9.8.6.4.5.9.9.1.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.0.2.7.1.8.4.1.3.6.4.5.9.6.3.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.5.b.2.2.1.2.8.f.-.d.a.e.5.-.4.8.4.7.-.9.0.f.1.-.9.3.b.d.3.7.a.0.9.6.b.4.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.0.6.0.c.-.0.0.0.1.-.0.0.1.b.-.0.5.2.f.-.c.6.3.1.8.5.b.e.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.0.3.a.0.1.9.e.a.a.4.c.5.0.7.1.3.0.a.a.f.2.7.2.c.4.c.d.5.0.e.d.b.0.0.0.0.f.f.f.f.!.0.0.0.0.1.b.5.5.f.b.a.2.4.2.4.6.0.c.c.0.a.5.b.3.8.2.9.9.a.c.a.a.a.c.f.3.f.5.4.c.5.e.8.7.!.B.A.N.K.-.S.T.A.T.M.E.N.T. ._.x.l.s.x...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.0././.1.1././.1.8.:.0.7.:.4.5.:.1.7.!.0.!.B.A.N.K.-.S.T.A.T.M.E.N.T. ._.x.l.s.x...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.7.2.9.5.....T.a.r.g.e.t.A.s.

C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_bank-statment _x_319d48559b0a1af85a57a6082102ce05f64a1d9_00000000_1aa0f8cb\Report.wer	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	18592
Entropy (8bit):	3.763786373480976
Encrypted:	false
SSDEEP:	192:RZ0XV0Ii+VpjV/C9yq5bMvg/LHZ+nNN2I1rzvq5xk0z5xT5/u7sWS274Iti:fUV06jB7vqsSt/u7sWX4Iti
MD5:	E47DA98DC5C443208459D81E83BDDAAB
SHA1:	52BE95EFA7CB50221CC8A83CC3AE88EE921C8157
SHA-256:	C60A32D4ADB7E38554AC91D789EEBDDA54C28A592DC1B16C4C56857AA2B8EFBF
SHA-512:	A064D319F76DA111ADA6076FA53A1784C566FBFD72149C596E865F0A554660AD762C28C5EB09A132F1002040255CD2164A51FBD3F64944CDA7DB0C60FAF4B74
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.0.2.7.1.8.7.7.5.8.3.2.2.5.2.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.0.2.7.1.8.7.8.7.2.3.8.5.7.1.....R.e.p.o.r.t.S.t.a.t.u.s.=.2.6.8.4.3.5.4.5.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.0.8.1.2.a.2.d.3.-.c.c.c.1.-.4.4.1.2.-.a.8.1.9.-.c.7.3.b.f.c.e.3.4.5.6.3.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.5.c.c.-.0.0.0.1.-.0.0.1.b.-.4.8.8.7.-.5.d.4.8.8.5.b.e.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.0.3.a.0.1.9.e.a.a.4.c.5.0.7.1.3.0.a.a.f.2.7.2.c.4.c.d.5.0.e.d.b.0.0.0.0.f.f.f.f.!.0.0.0.0.1.b.5.5.f.b.a.2.4.2.4.6.0.c.c.0.a.5.b.3.8.2.9.9.a.c.a.a.a.c.f.3.f.5.4.c.5.e.8.7.!.B.A.N.K.-.S.T.A.T.M.E.N.T. ._.x.l.s.x...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.0././.1.1././.1.8.:.0.7.:.4.5.:.1.7.!.0.!.B.A.N.K.-.S.T.A.T.M.E.N.T. ._.x.l.s.x...e.x.e.....B.o.o.t.I.d.=.4.2.9.4.9.6.7.2.9.5.....T.a.r.g.e.t.A.s.

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_bank-statment _x_319d48559b0a1af85a57a6082102ce05f64a1d9_00000000_173bee50\Report.wer	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	Little-endian UTF-16 Unicode text, with CRLF line terminators

C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_bank-statment _x_319d48559b0a1af85a57a6082102ce05f64a1d9_00000000_173bee50\Report.wer	
Category:	dropped
Size (bytes):	18230
Entropy (8bit):	3.7611081288567427
Encrypted:	false
SSDEEP:	192:fZXVGFi+VpjV/C9yq5bMvg/LHZ+nNN2I1rzvq5xk0z5xTc/u7sxS274ItD:hVGjjB7vqsSI/u7sxX4ItD
MD5:	1D6B9C7D1BCA6E5B897721E501AE55F7
SHA1:	55125A143ECECA70B183A7A30C0312EA4C49EC03
SHA-256:	7EAFC56A884B493D22E34ED069F111AC40EBB40CD69B7AFACEEDB2A0916EAC06
SHA-512:	D731A058666AE6E4D559017A4F058183D7C630DB12D0E0A6C2BB773CF45391F246517A7942B8DFA61E1307B007573D8F906220A6B0ACD391099ACBD4C8256801
Malicious:	false
Preview:	..V.e.r.s.i.o.n.=.1.....E.v.e.n.t.T.y.p.e.=.C.L.R.2.0.r.3.....E.v.e.n.t.T.i.m.e.=.1.3.2.5.0.2.7.1.7.7.6.4.5.8.5.5.7.6.....R.e.p.o.r.t.T.y.p.e.=.2.....C.o.n.s.e.n.t.=.1.....U.p.l.o.a.d.T.i.m.e.=.1.3.2.5.0.2.7.1.7.7.8.0.5.2.2.9.9.6.....R.e.p.o.r.t.S.t.a.t.u.s.=.9.6.....R.e.p.o.r.t.I.d.e.n.t.i.f.i.e.r.=.3.d.a.f.b.7.c.6.-.e.e.c.e.-.4.3.1.b.-.b.9.2.f.-.9.d.9.c.b.f.a.4.7.b.e.b.....W.o.w.6.4.H.o.s.t.=.3.4.4.0.4.....W.o.w.6.4.G.u.e.s.t.=.3.3.2.....A.p.p.S.e.s.s.i.o.n.G.u.i.d.=.0.0.0.0.1.1.9.4.-.0.0.0.1.-.0.0.1.b.-.4.0.5.c.-.7.9.0.8.8.5.b.e.d.6.0.1.....T.a.r.g.e.t.A.p.p.I.d.=.W.:.0.0.0.6.0.3.a.0.1.9.e.a.a.4.c.5.0.7.1.3.0.a.a.f.2.7.2.c.4.c.d.5.0.e.d.b.0.0.0.0.f.f.f.f.!.0.0.0.0.1.b.5.5.f.b.a.2.4.2.4.6.0.c.c.0.a.5.b.3.8.2.9.9.a.c.a.a.a.c.f.3.f.5.4.c.5.e.8.7.!.B.A.N.K.-.S.T.A.T.M.E.N.T. ._.x.l.s.x...e.x.e.....T.a.r.g.e.t.A.p.p.V.e.r.=.2.0.2.0././.1.1././.1.8.:.0.7.:.4.5.:.1.7.!.0.!.B.A.N.K.-.S.T.A.T.M.E.N.T. ._.x.l.s.x...e.x.e...B.o.o.t.I.d.=.4.2.9.4.9.6.7.2.9.5.....T.a.r.g.e.t.A.s.I.d.=.3.6.3...

C:\ProgramData\Microsoft\Windows\WER\Temp\WER2128.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	5692
Entropy (8bit):	3.7319624624525853
Encrypted:	false
SSDEEP:	96:RtIU6o7r3GLt3iwZ66l8YZHuvUubSfOyWggwB+aM1lR1f04Oh6QGm:Rrl7r3GLNiwZ66WYZHuvUubS/+p1lR1W
MD5:	8552D2001589AA8518032CD3C584137A
SHA1:	BA2152F9BE4134A2FCE139BC9080A49223A7A717
SHA-256:	52CBB08329A85E99C93B3453D36E529D827643F1E5485D57C7C6ABB9A2CF0A65
SHA-512:	FCC3C0DC2DD96F41D1C2B51A73895D23E0683F5E22F85191870F6F33A3F81C16D276395DE87C9EFC86EE7EC9993A83E35F32580D8794CFFF02EF7C7D5E492DI
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.4.2.4.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER21C5.tmp.xml	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4657
Entropy (8bit):	4.47363119991153
Encrypted:	false
SSDEEP:	48:cvIwSD8zsMJgtWI9sqWSC8BY8fm8M4JFKA7FH+q8v9Ecv4Hqd:uITfKfLSN/JFKKKucvgqd
MD5:	0498ADAFD3AB8965B176B440425C0A7A
SHA1:	432D1586917BF8560D4E8192A0E077908206327F
SHA-256:	BDF1D7678F110EFE8C14134A8D46B0D43974D4EA421F44DFFAEB9C687EAA548C
SHA-512:	07E3C1827F9157B3A4916445D5ED8A1498532F94CF85FC43D2207213BB99ED2E4BA44BECDDE7B0C2E000E27E409ED6E5C84D8509BE6976DBE68D6C5C43DFA72
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="735854" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-11.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5DA4.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	7706
Entropy (8bit):	3.7093624418460873
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNiyK6h4aOv6YD668gmfZHuvUubS/+p1SY1f9PGm:RrlsNif6a6Ye68gmfgvvbS6SCfd

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5DA4.tmp.WERInternalMetadata.xml	
MD5:	13FBDD30D51AB2E61A1A0C2BB9CBAD22
SHA1:	272F7E82FACE89A45E212A5EDC0F5565AE11173F
SHA-256:	A925E98DEE3B85593CD16C62CF16AB0FA1BD7BF09424610A0AAC65166408F4B1
SHA-512:	67518F59765484D7EF9D280D95CD2DCEF9A74BCDE6249B441B93930063185CADCE874D8B9E01BFC829FE87667D547913CDF0C08115A0374BB8F9FB0ABC7E53 8
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.1.5.4.8.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER5E9F.tmp.xml	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4657
Entropy (8bit):	4.476145816240227
Encrypted:	false
SSDEEP:	48:cvIwSD8zsMJgtWI9sqWSC8B78fm8M4JFKA7FRz+q8v9jcv4Hzd:uITfKfLSNCJFKUzKVcvgzd
MD5:	9D066B7E9C821DD3E2968B9327FFC583
SHA1:	E91C21354D81A329C86162F31B4484397FD48B5B
SHA-256:	0B15A5BB24EB7D299148838CE4185DB9E47322DA48250D399B4196D8F25DD9EC
SHA-512:	257C0134D7415CE5FA8AFDD8AE1564C8AFEC4DFEB694E35304F5AC38CE40AEBB4CD747EBE7E80FE7C1F13B78EC5B2B5849F2ABD673416C40EEFA9ABBD6BD 2FD7
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="735854" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WER65F6.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	7664
Entropy (8bit):	3.7013706190950346
Encrypted:	false
SSDEEP:	192:Rrl7r3GLNijr6PT6Ygr6QgmfZHuvUubS/+p1XX1fw9m:RrlsNiP676YU6QgmfgvvbS6XlfH
MD5:	670D94A4E814A0E3DA13F43F224F812E
SHA1:	4DF1A1C5AA3C09BCB38AE5F54A01A591B6331B50
SHA-256:	1DAC09070F73B6B270783D2F400482A35E7DA0DD394BCB880064B7A1132552A2
SHA-512:	9F8B8C5771CB0BC7554DE8804172EFB796619B948E1C81BD1C45DC919E1FF8D23F43C67C8FFA8F2C37BCB310DDFB6D1F9F8ACE5287CF89C9D2EE9C6FA5A08 A2
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d. o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o. <./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.4.5.0.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WER66C2.tmp.xml	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4657
Entropy (8bit):	4.476517921665472
Encrypted:	false
SSDEEP:	48:cvIwSD8zs5JgtWI9sqWSC8Bu8fm8M4JFKA7FW+q8v9ncv4HBd:uITfLfLSNNJFKTKtcvgBd
MD5:	D73E09E3709B8D13B9C98DCD2411FEA7
SHA1:	76A6F85365798CA0986552BCE6C4E737ECE35A6E
SHA-256:	55715E63CB2EF0E28F697DD1F5A72E8F87EBCC0FA14EF90EEC49EF6132A0BC01
SHA-512:	D4F3F73F6320AF8CDEF6F1A840F349E7263136841ABFA69F9A3AF94A96FAEB04295564FB6D0CD46B70F294DE9F032AE76F1849C9A96FC0F265D912F8C930718F

C:\ProgramData\Microsoft\Windows\WER\Temp\WER66C2.tmp.xml	
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="735853" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBB64.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	5692
Entropy (8bit):	3.7362665521032725
Encrypted:	false
SSDEEP:	96:RtIU6o7r3GLt3idP6ccbYZHuvUubSfOyWggwB+aM1UDI1fYBGm:Rrl7r3GLNidP6ccbYZHuvUubS/+p1UDh
MD5:	017FD89E3734E63FACECEBC9D6C71C99
SHA1:	198175B96A6310BC6F2EC8B944FA855D55D07664
SHA-256:	58BCDD3A8523766D70B9B7601D1CBE9C1BE53F02873EEC64F8C60444E82F1CDB
SHA-512:	CD7AF9624B643E9810A0856D0BFB095EBCDCBFC4D7A65AE63054B4AE54A469CB44E79266968B461FC11C7773B9D76AC49BB1FD5E1FADEE46E730D28AA60F2C6E
Malicious:	false
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.6.1.8.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERBC01.tmp.xml	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4657
Entropy (8bit):	4.476622485131769
Encrypted:	false
SSDEEP:	48:cvIwSD8zszJgtWI9sqWSC8BG8fm8M4JFKA7Fo+q8v9ocv4H+d:uITfNfLSNZJFKpKCcvg+d
MD5:	55661D3A5A477629000B09FD2C3C93D3
SHA1:	A1CCD794CA275B2EE5D5838C2DE3E9D9D710AC2D
SHA-256:	0A1564FA4EBFCC9E226BAE441CDF3F28C45BFA00819361EBE641834A4EC7E0A6
SHA-512:	A60C6204867768D8DBF69B414C649696D4C028299ACB064C99A71C23CA5AEFC51E66CA3A666BD2586EBDD4E5565E2BF3C7E09921C8A623C69DD9534D9B1240C
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="735855" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF0FB.tmp.WERInternalMetadata.xml	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	XML 1.0 document, Little-endian UTF-16 Unicode text, with CRLF line terminators
Category:	dropped
Size (bytes):	5692
Entropy (8bit):	3.7361337278264863
Encrypted:	false
SSDEEP:	96:RtIU6o7r3GLt3iiR6U9cEIXDkYZHuvUubSfOyWggwB+aM1uc1fEXam:Rrl7r3GLNiiR69rzkYZHuvUubS/+p1uj
MD5:	282364D123559D1559F1BE3C7CE12993
SHA1:	1900116F8645DD67581E3A3E880588384FA5C3A9
SHA-256:	A8FA38E71D604414E4ABF48AF5479B672B5613A273F9E56F06C2FB369DA8F7C7
SHA-512:	8087299D86A418356FD8E61D76688562A136D3ED384136B1F6900A865D3555FBA0036E12B9BF045A2F762ADCC71DD1E479557DBA86177DF6B58E8C95C59CD8A
Malicious:	false

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF0FB.tmp.WERInternalMetadata.xml	
Preview:	..<.?.x.m.l. .v.e.r.s.i.o.n.=.".1...0.". .e.n.c.o.d.i.n.g.=.".U.T.F.-.1.6.".?.>.....<.W.E.R.R.e.p.o.r.t.M.e.t.a.d.a.t.a.>.....<.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.1.0...0.<./.W.i.n.d.o.w.s.N.T.V.e.r.s.i.o.n.>.....<.B.u.i.l.d.>.1.7.1.3.4.<./.B.u.i.l.d.>.....<.P.r.o.d.u.c.t.>.(.0.x.3.0.).:. .W.i.n.d.o.w.s. .1.0. .P.r.o.<./.P.r.o.d.u.c.t.>.....<.E.d.i.t.i.o.n.>.P.r.o.f.e.s.s.i.o.n.a.l.<./.E.d.i.t.i.o.n.>.....<.B.u.i.l.d.S.t.r.i.n.g.>.1.7.1.3.4...1...a.m.d.6.4.f.r.e...r.s.4._.r.e.l.e.a.s.e...1.8.0.4.1.0.-.1.8.0.4.<./.B.u.i.l.d.S.t.r.i.n.g.>.....<.R.e.v.i.s.i.o.n.>.1.<./.R.e.v.i.s.i.o.n.>.....<.F.l.a.v.o.r.>.M.u.l.t.i.p.r.o.c.e.s.s.o.r. .F.r.e.e.<./.F.l.a.v.o.r.>.....<.A.r.c.h.i.t.e.c.t.u.r.e.>.X.6.4.<./.A.r.c.h.i.t.e.c.t.u.r.e.>.....<.L.C.I.D.>.1.0.3.3.<./.L.C.I.D.>.....<./.O.S.V.e.r.s.i.o.n.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.r.o.c.e.s.s.I.n.f.o.r.m.a.t.i.o.n.>.....<.P.i.d.>.5.5.8.0.<./.P.i.d.>.....

C:\ProgramData\Microsoft\Windows\WER\Temp\WERF1C7.tmp.xml	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	4657
Entropy (8bit):	4.476286019433985
Encrypted:	false
SSDEEP:	48:cvIwSD8zszJgtWI9sqWSC8BE8fm8M4JFKA7Fk+q8v9+cv4Hdd:uITfNfLSNHJFKZKAcvgdd
MD5:	9E3FCD004985DFA030F0F51B1AB27043
SHA1:	CDB35AD87D4306A2461EAE7D41BE6F62577E9B07
SHA-256:	73BE6578D438CAEBB83EB34868719FC42AB31EA1C82BE191CAE33BD0B0CFC22E
SHA-512:	619345A0AC68CB08AC5201B8E75E6F95288B7CE6ACF06A4084F3EC3ED996CDF71828211B0E6C20263C86C6F75BB5F4FAF6B7F02E314D9EF5C788C110F89607C
Malicious:	false
Preview:	<?xml version="1.0" encoding="UTF-8" standalone="yes"?>..<req ver="2">.. <tlm>.. <src>.. <desc>.. <mach>.. <os>.. <arg nm="vermaj" val="10" />.. <arg nm="vermin" val="0" />.. <arg nm="verbld" val="17134" />.. <arg nm="vercsdbld" val="1" />.. <arg nm="verqfe" val="1" />.. <arg nm="csdbld" val="1" />.. <arg nm="versp" val="0" />.. <arg nm="arch" val="9" />.. <arg nm="lcid" val="1033" />.. <arg nm="geoid" val="244" />.. <arg nm="sku" val="48" />.. <arg nm="domain" val="0" />.. <arg nm="prodsuite" val="256" />.. <arg nm="ntprodtype" val="1" />.. <arg nm="platid" val="2" />.. <arg nm="tmsi" val="735855" />.. <arg nm="osinsty" val="1" />.. <arg nm="iever" val="11.1.17134.0-1 1.0.47" />.. <arg nm="portos" val="0" />.. <arg nm="ram" val="4096" />..

C:\Users\user\AppData\Local\Temp\holderwb.txt	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Preview:	..

C:\Users\user\AppData\Roaming\pid.txt	
Process:	C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	4
Entropy (8bit):	2.0
Encrypted:	false
SSDEEP:	3:BR:n
MD5:	EF0D17B3BDB4EE2AA741BA28C7255C53
SHA1:	E3479C19053568CE27FCC573669D61191419B296
SHA-256:	CF5DF267131383187BDB3D2C59A8718E37AC3103AE6612E9EE5FD113A75116E9
SHA-512:	FD2595FEEB081D9BC1938F59C4F641B895DABD0AD71987F0CA5E278666714B866B4BCC4DDEB8056D1280292C09B82022B9E01C4448B63FF2A8CE9A0C17064BA A
Malicious:	false
Preview:	2864

C:\Users\user\AppData\Roaming\pidloc.txt	
Process:	C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	46
Entropy (8bit):	4.50771291359613

C:\Users\user\AppData\Roaming\pidloc.txt	
Encrypted:	false
SSDEEP:	3:oNt+WfWna2ivf6+J:oNwva7jJ
MD5:	17A331B7B14347C9BF55C859D564272C
SHA1:	44A7FB06E7DC2D59BDADBA10D88E936BAF85C9ED
SHA-256:	714BF368D097C449B0C4A831E70AAF6C077860B7B2FFF3BD68687879F2C73D8E
SHA-512:	A5AE156BBE52F34AA62C31BAA5B8A4A8CA893E36A843D7862B0039101781757AD242C0A6998AAF58491ACE8316C071579CEAB1623163B473F27BEB78F074869D
Malicious:	false
Preview:	C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	6.9327470610312085
TrID:	• Win32 Executable (generic) a (10002005/4) 99.24% • InstallShield setup (43055/19) 0.43% • Win32 Executable Delphi generic (14689/80) 0.15% • Windows Screen Saver (13104/52) 0.13% • Win16/32 Executable Delphi generic (2074/23) 0.02%
File name:	BANK-STATMENT _xlsx.exe
File size:	965120
MD5:	debe564cd4c27c02d23c828df27fe27f
SHA1:	1b55fba242460cc0a5b38299acaaacf3f54c5e87
SHA256:	edafe7e62738e180cb882d93f37d2d306627aef482d6f7a7a06c69198c61cd58
SHA512:	07091b073d5885787f830a6a02a39f1064a80767ac02aea87bbc66ccb93406fba2f7a7bdd9d02d4c04f18b54bb59b34d0fd3e97649584363008c56b126801c37
SSDEEP:	24576:6odaqxzLqAc4TDlEO9KqOidDy70cd4gKsvi:Rj1uVmhpOidDyv1Ksa
File Content Preview:	MZP.....@.....!..L.!.. This program must be run under Win32..$7..... ....

File Icon

Icon Hash:	be9eeecece709286

Static PE Info

General

Entrypoint:	0x46add0
Entrypoint Section:	CODE
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, BYTES_REVERSED_LO, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, BYTES_REVERSED_HI
DLL Characteristics:	
Time Stamp:	0x2A425E19 [Fri Jun 19 22:22:17 1992 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
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:	dfbd2d8adc9d5f58fb80cc271c1cf580

Entrypoint Preview

Instruction
push ebp
mov ebp, esp
add esp, FFFFFFF0h
mov eax, 0046AC20h
call 00007F6BE4B3C7C9h
mov eax, dword ptr [00486C60h]
mov eax, dword ptr [eax]
call 00007F6BE4B8B5D1h
mov ecx, dword ptr [00486D50h]
mov eax, dword ptr [00486C60h]
mov eax, dword ptr [eax]
mov edx, dword ptr [0046A72Ch]
call 00007F6BE4B8B5D1h
mov eax, dword ptr [00486C60h]
mov eax, dword ptr [eax]
call 00007F6BE4B8B645h
call 00007F6BE4B3A2C0h
lea eax, dword ptr [eax+00h]
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Instruction
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al
add byte ptr [eax], al

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x88000	0x247a	.idata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x95000	0x5bc5c	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0x8d000	0x7044	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x8c000	0x18	.rdata
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
CODE	0x1000	0x69e18	0x6a000	False	0.524259747199	data	6.51526332301	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
DATA	0x6b000	0x1bddc	0x1be00	False	0.171822449552	data	2.72180144261	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
BSS	0x87000	0xc79	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.idata	0x88000	0x247a	0x2600	False	0.350637335526	data	4.93470816555	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.tls	0x8b000	0x10	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.rdata	0x8c000	0x18	0x200	False	0.048828125	data	0.20058190744	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.reloc	0x8d000	0x7044	0x7200	False	0.581483004386	data	6.62684722592	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ
.rsrc	0x95000	0x5bc5c	0x5be00	False	0.887537202381	data	7.51848710017	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_SHARED, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_CURSOR	0x96250	0x134	data		
RT_CURSOR	0x96384	0x134	data		
RT_CURSOR	0x964b8	0x134	data		
RT_CURSOR	0x965ec	0x134	data		
RT_CURSOR	0x96720	0x134	data		
RT_CURSOR	0x96854	0x134	data		
RT_CURSOR	0x96988	0x134	data		
RT_BITMAP	0x96abc	0x1d0	data		
RT_BITMAP	0x96c8c	0x1e4	data		
RT_BITMAP	0x96e70	0x1d0	data		
RT_BITMAP	0x97040	0x1d0	data		
RT_BITMAP	0x97210	0x1d0	data		
RT_BITMAP	0x973e0	0x1d0	data		
RT_BITMAP	0x975b0	0x1d0	data		
RT_BITMAP	0x97780	0x1d0	data		
RT_BITMAP	0x97950	0x53c6e	data	English	United States
RT_BITMAP	0xeb5c0	0x1d0	data		
RT_BITMAP	0xeb790	0xd8	data		
RT_BITMAP	0xeb868	0x128	data		
RT_BITMAP	0xeb990	0x128	data		
RT_BITMAP	0xebab8	0x128	data		
RT_BITMAP	0xebbe0	0xe8	data		
RT_BITMAP	0xebcc8	0x128	data		
RT_BITMAP	0xebdf0	0x128	data		
RT_BITMAP	0xebf18	0xd0	data		
RT_BITMAP	0xebfe8	0x128	data		
RT_BITMAP	0xec110	0x128	data		
RT_BITMAP	0xec238	0x128	data		
RT_BITMAP	0xec360	0x128	data		
RT_BITMAP	0xec488	0x128	data		
RT_BITMAP	0xec5b0	0xe8	data		
RT_BITMAP	0xec698	0x128	data		
RT_BITMAP	0xec7c0	0x128	data		
RT_BITMAP	0xec8e8	0xd0	data		
RT_BITMAP	0xec9b8	0x128	data		
RT_BITMAP	0xecae0	0x128	data		
RT_BITMAP	0xecc08	0x128	data		
RT_BITMAP	0xecd30	0x128	data		
RT_BITMAP	0xece58	0x128	data		
RT_BITMAP	0xecf80	0xe8	data		
RT_BITMAP	0xed068	0x128	data		
RT_BITMAP	0xed190	0x128	data		
RT_BITMAP	0xed2b8	0xd0	data		
RT_BITMAP	0xed388	0x128	data		
RT_BITMAP	0xed4b0	0x128	data		
RT_BITMAP	0xed5d8	0xd8	data		
RT_BITMAP	0xed6b0	0xd8	data		
RT_BITMAP	0xed788	0xd8	data		
RT_BITMAP	0xed860	0xd8	data		
RT_ICON	0xed938	0x568	GLS_BINARY_LSB_FIRST	English	United States
RT_STRING	0xedea0	0xdc	data		
RT_STRING	0xedf7c	0x2d8	data		
RT_STRING	0xee254	0xd8	data		
RT_STRING	0xee32c	0x160	data		
RT_STRING	0xee48c	0x218	data		
RT_STRING	0xee6a4	0x470	data		
RT_STRING	0xeeb14	0x380	data		
RT_STRING	0xeee94	0x394	data		
RT_STRING	0xef228	0x418	data		
RT_STRING	0xef640	0xf4	data		
RT_STRING	0xef734	0xc4	data		
RT_STRING	0xef7f8	0x2e0	data		
RT_STRING	0xefad8	0x35c	data		
RT_STRING	0xefe34	0x2b4	data		

Name	RVA	Size	Type	Language	Country
RT_RCDATA	0xf00e8	0x10	data		
RT_RCDATA	0xf00f8	0x224	data		
RT_RCDATA	0xf031c	0x807	Delphi compiled form 'TForm1'		
RT_GROUP_CURSOR	0xf0b24	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xf0b38	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xf0b4c	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xf0b60	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xf0b74	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xf0b88	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_CURSOR	0xf0b9c	0x14	Lotus unknown worksheet or configuration, revision 0x1		
RT_GROUP_ICON	0xf0bb0	0x14	data	English	United States
RT_HTML	0xf0bc4	0x98	data	English	United States

Imports

DLL	Import
kernel32.dll	DeleteCriticalSection, LeaveCriticalSection, EnterCriticalSection, InitializeCriticalSection, VirtualFree, VirtualAlloc, LocalFree, LocalAlloc, GetCurrentThreadId, InterlockedDecrement, InterlockedIncrement, VirtualQuery, WideCharToMultiByte, SetCurrentDirectoryA, MultiByteToWideChar, lstrlenA, lstrcpynA, LoadLibraryExA, GetThreadLocale, GetStartupInfoA, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetLastError, GetCurrentDirectoryA, GetCommandLineA, FreeLibrary, FindFirstFileA, FindClose, ExitProcess, WriteFile, UnhandledExceptionFilter, SetFilePointer, SetEndOfFile, RtlUnwind, ReadFile, RaiseException, GetStdHandle, GetFileSize, GetFileType, CreateFileA, CloseHandle
user32.dll	GetKeyboardType, LoadStringA, MessageBoxA, CharNextA
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey
oleaut32.dll	SysFreeString, SysReAllocStringLen, SysAllocStringLen
kernel32.dll	TlsSetValue, TlsGetValue, LocalAlloc, GetModuleHandleA
advapi32.dll	RegQueryValueExA, RegOpenKeyExA, RegCloseKey
kernel32.dll	lstrcpyA, WriteFile, WaitForSingleObject, VirtualQuery, VirtualProtectEx, VirtualProtect, VirtualAlloc, Sleep, SizeofResource, SetThreadLocale, SetFilePointer, SetEvent, SetErrorMode, SetEndOfFile, ResetEvent, ReadFile, MulDiv, LockResource, LoadResource, LoadLibraryA, LeaveCriticalSection, InitializeCriticalSection, GlobalUnlock, GlobalReAlloc, GlobalHandle, GlobalLock, GlobalFree, GlobalFindAtomA, GlobalDeleteAtom, GlobalAlloc, GlobalAddAtomA, GetVersionExA, GetVersion, GetTickCount, GetThreadLocale, GetSystemTime, GetSystemInfo, GetStringTypeExA, GetStdHandle, GetProcAddress, GetModuleHandleA, GetModuleFileNameA, GetLocaleInfoA, GetLastError, GetFullPathNameA, GetDiskFreeSpaceA, GetCurrentThreadId, GetCurrentProcessId, GetCPInfo, GetACP, FreeResource, FreeLibrary, FormatMessageA, FindResourceA, FindNextFileA, FindFirstFileA, FindClose, FileTimeToLocalFileTime, FileTimeToDosDateTime, ExitProcess, EnumCalendarInfoA, EnterCriticalSection, DeleteCriticalSection, CreateThread, CreateFileA, CreateEventA, CompareStringA, CloseHandle
gdi32.dll	UnrealizeObject, StretchBlt, SetWindowOrgEx, SetWindowExtEx, SetWinMetaFileBits, SetViewportOrgEx, SetViewportExtEx, SetTextColor, SetStretchBltMode, SetROP2, SetPixel, SetMapMode, SetEnhMetaFileBits, SetDIBColorTable, SetBrushOrgEx, SetBkMode, SetBkColor, SelectPalette, SelectObject, SaveDC, RestoreDC, Rectangle, RectVisible, RealizePalette, Polyline, PolyPolyline, PlayEnhMetaFile, PatBlt, MoveToEx, MaskBlt, LineTo, IntersectClipRect, GetWindowOrgEx, GetWinMetaFileBits, GetTextMetricsA, GetTextExtentPoint32A, GetSystemPaletteEntries, GetStockObject, GetPixel, GetPaletteEntries, GetObjectA, GetEnhMetaFilePaletteEntries, GetEnhMetaFileHeader, GetEnhMetaFileBits, GetDeviceCaps, GetDIBits, GetDIBColorTable, GetDCOrgEx, GetCurrentPositionEx, GetClipBox, GetBrushOrgEx, GetBitmapBits, ExtCreatePen, ExcludeClipRect, DeleteObject, DeleteEnhMetaFile, DeleteDC, CreateSolidBrush, CreatePenIndirect, CreatePalette, CreateHalftonePalette, CreateFontIndirectA, CreateDIBitmap, CreateDIBSection, CreateCompatibleDC, CreateCompatibleBitmap, CreateBrushIndirect, CreateBitmap, CopyEnhMetaFileA, BitBlt
user32.dll	WindowFromPoint, WinHelpA, WaitMessage, ValidateRect, UpdateWindow, UnregisterClassA, UnionRect, UnhookWindowsHookEx, TranslateMessage, TranslateMDISysAccel, TrackPopupMenu, SystemParametersInfoA, ShowWindow, ShowScrollBar, ShowOwnedPopups, ShowCursor, SetWindowsHookExA, SetWindowTextA, SetWindowPos, SetWindowPlacement, SetWindowLongA, SetTimer, SetScrollRange, SetScrollPos, SetScrollInfo, SetRect, SetPropA, SetMenuItemInfoA, SetMenu, SetKeyboardState, SetForegroundWindow, SetFocus, SetCursor, SetClipboardData, SetClassLongA, SetCapture, SetActiveWindow, SendMessageA, ScrollWindowEx, ScrollWindow, ScreenToClient, RemovePropA, RemoveMenu, ReleaseDC, ReleaseCapture, RegisterWindowMessageA, RegisterClipboardFormatA, RegisterClassA, RedrawWindow, PtInRect, PostQuitMessage, PostMessageA, PeekMessageA, OpenClipboard, OffsetRect, OemToCharA, MessageBoxA, MessageBeep, MapWindowPoints, MapVirtualKeyA, LoadStringA, LoadKeyboardLayoutA, LoadIconA, LoadCursorA, LoadBitmapA, KillTimer, IsZoomed, IsWindowVisible, IsWindowEnabled, IsWindow, IsRectEmpty, IsIconic, IsDialogMessageA, IsChild, IsCharAlphaNumericA, IsCharAlphaA, InvalidateRect, IntersectRect, InsertMenuItemA, InsertMenuA, InflateRect, GetWindowThreadProcessId, GetWindowTextA, GetWindowRect, GetWindowPlacement, GetWindowLongA, GetWindowDC, GetTopWindow, GetSystemMetrics, GetSystemMenu, GetSysColor, GetSubMenu, GetScrollRange, GetScrollPos, GetScrollInfo, GetPropA, GetParent, GetWindow, GetMessageTime, GetMenuStringA, GetMenuState, GetMenuItemInfoA, GetMenuItemID, GetMenuItemCount, GetMenu, GetLastActivePopup, GetKeyboardState, GetKeyboardLayoutList, GetKeyboardLayout, GetKeyState, GetKeyNameTextA, GetIconInfo, GetForegroundWindow, GetFocus, GetDoubleClickTime, GetDesktopWindow, GetDCEx, GetDC, GetCursorPos, GetCursor, GetClipboardData, GetClientRect, GetClassNameA, GetClassInfoA, GetCaretPos, GetCapture, GetActiveWindow, FrameRect, FindWindowA, FillRect, EqualRect, EnumWindows, EnumThreadWindows, EnumClipboardFormats, EndPaint, EndDeferWindowPos, EnableWindow, EnableScrollBar, EnableMenuItem, EmptyClipboard, DrawTextA, DrawMenuBar, DrawIconEx, DrawIcon, DrawFrameControl, DrawFocusRect, DrawEdge, DispatchMessageA, DestroyWindow, DestroyMenu, DestroyIcon, DestroyCursor, DeleteMenu, DeferWindowPos, DefWindowProcA, DefMDIChildProcA, DefFrameProcA, CreateWindowExA, CreatePopupMenu, CreateMenu, CreateIcon, CloseClipboard, ClientToScreen, CheckMenuItem, CallWindowProcA, CallNextHookEx, BeginPaint, BeginDeferWindowPos, CharNextA, CharLowerBuffA, CharLowerA, CharUpperBuffA, AdjustWindowRectEx, ActivateKeyboardLayout
kernel32.dll	Sleep

DLL	Import
oleaut32.dll	SafeArrayPtrOfIndex, SafeArrayPutElement, SafeArrayGetElement, SafeArrayGetUBound, SafeArrayGetLBound, SafeArrayRedim, SafeArrayCreate, VariantChangeTypeEx, VariantCopyInd, VariantCopy, VariantClear, VariantInit
comctl32.dll	ImageList_SetIconSize, ImageList_GetIconSize, ImageList_Write, ImageList_Read, ImageList_GetDragImage, ImageList_DragShowNolock, ImageList_SetDragCursorImage, ImageList_DragMove, ImageList_DragLeave, ImageList_DragEnter, ImageList_EndDrag, ImageList_BeginDrag, ImageList_Remove, ImageList_DrawEx, ImageList_Replace, ImageList_Draw, ImageList_GetBkColor, ImageList_SetBkColor, ImageList_ReplaceIcon, ImageList_Add, ImageList_GetImageCount, ImageList_Destroy, ImageList_Create
kernel32.dll	MulDiv
winmm.dll	mciSendCommandA, mciGetErrorStringA
kernel32.dll	AddVectoredExceptionHandler

Possible Origin

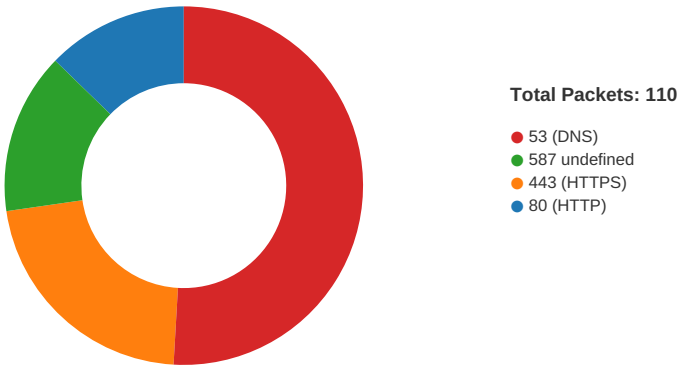
Language of compilation system	Country where language is spoken	Map
English	United States	

Network Behavior

Snort IDS Alerts

Timestamp	Protocol	SID	Message	Source Port	Dest Port	Source IP	Dest IP
11/19/20-16:03:11.245137	TCP	2019926	ET TROJAN HawkEye Keylogger Report SMTP	49746	587	192.168.2.4	166.62.27.57

Network Port Distribution



TCP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 16:02:54.499708891 CET	49738	80	192.168.2.4	104.16.154.36
Nov 19, 2020 16:02:54.516001940 CET	80	49738	104.16.154.36	192.168.2.4
Nov 19, 2020 16:02:54.516113997 CET	49738	80	192.168.2.4	104.16.154.36
Nov 19, 2020 16:02:54.517074108 CET	49738	80	192.168.2.4	104.16.154.36
Nov 19, 2020 16:02:54.533266068 CET	80	49738	104.16.154.36	192.168.2.4
Nov 19, 2020 16:02:54.541414976 CET	80	49738	104.16.154.36	192.168.2.4
Nov 19, 2020 16:02:54.594522953 CET	49738	80	192.168.2.4	104.16.154.36
Nov 19, 2020 16:02:54.594763994 CET	49739	443	192.168.2.4	104.16.154.36
Nov 19, 2020 16:02:54.611154079 CET	443	49739	104.16.154.36	192.168.2.4
Nov 19, 2020 16:02:54.611242056 CET	49739	443	192.168.2.4	104.16.154.36
Nov 19, 2020 16:02:54.672023058 CET	49739	443	192.168.2.4	104.16.154.36
Nov 19, 2020 16:02:54.688457966 CET	443	49739	104.16.154.36	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 16:02:54.688901901 CET	443	49739	104.16.154.36	192.168.2.4
Nov 19, 2020 16:02:54.689006090 CET	443	49739	104.16.154.36	192.168.2.4
Nov 19, 2020 16:02:54.689054966 CET	49739	443	192.168.2.4	104.16.154.36
Nov 19, 2020 16:02:54.758867025 CET	49739	443	192.168.2.4	104.16.154.36
Nov 19, 2020 16:02:54.762535095 CET	49740	443	192.168.2.4	104.16.154.36
Nov 19, 2020 16:02:54.775322914 CET	443	49739	104.16.154.36	192.168.2.4
Nov 19, 2020 16:02:54.778700113 CET	443	49740	104.16.154.36	192.168.2.4
Nov 19, 2020 16:02:54.779587030 CET	49740	443	192.168.2.4	104.16.154.36
Nov 19, 2020 16:02:54.779609919 CET	49740	443	192.168.2.4	104.16.154.36
Nov 19, 2020 16:02:54.798758984 CET	443	49740	104.16.154.36	192.168.2.4
Nov 19, 2020 16:02:54.799081087 CET	443	49740	104.16.154.36	192.168.2.4
Nov 19, 2020 16:02:54.799626112 CET	443	49740	104.16.154.36	192.168.2.4
Nov 19, 2020 16:02:54.799702883 CET	49740	443	192.168.2.4	104.16.154.36
Nov 19, 2020 16:02:54.800508022 CET	49740	443	192.168.2.4	104.16.154.36
Nov 19, 2020 16:02:54.816796064 CET	443	49740	104.16.154.36	192.168.2.4
Nov 19, 2020 16:03:08.611728907 CET	49746	587	192.168.2.4	166.62.27.57
Nov 19, 2020 16:03:08.882777929 CET	587	49746	166.62.27.57	192.168.2.4
Nov 19, 2020 16:03:08.882930994 CET	49746	587	192.168.2.4	166.62.27.57
Nov 19, 2020 16:03:09.597856998 CET	587	49746	166.62.27.57	192.168.2.4
Nov 19, 2020 16:03:09.598325968 CET	49746	587	192.168.2.4	166.62.27.57
Nov 19, 2020 16:03:09.869668961 CET	587	49746	166.62.27.57	192.168.2.4
Nov 19, 2020 16:03:09.873588085 CET	49746	587	192.168.2.4	166.62.27.57
Nov 19, 2020 16:03:10.145303011 CET	587	49746	166.62.27.57	192.168.2.4
Nov 19, 2020 16:03:10.145670891 CET	49746	587	192.168.2.4	166.62.27.57
Nov 19, 2020 16:03:10.425162077 CET	587	49746	166.62.27.57	192.168.2.4
Nov 19, 2020 16:03:10.426595926 CET	49746	587	192.168.2.4	166.62.27.57
Nov 19, 2020 16:03:10.697953939 CET	587	49746	166.62.27.57	192.168.2.4
Nov 19, 2020 16:03:10.699817896 CET	49746	587	192.168.2.4	166.62.27.57
Nov 19, 2020 16:03:10.972868919 CET	587	49746	166.62.27.57	192.168.2.4
Nov 19, 2020 16:03:10.973298073 CET	49746	587	192.168.2.4	166.62.27.57
Nov 19, 2020 16:03:11.244473934 CET	587	49746	166.62.27.57	192.168.2.4
Nov 19, 2020 16:03:11.244570017 CET	587	49746	166.62.27.57	192.168.2.4
Nov 19, 2020 16:03:11.245136976 CET	49746	587	192.168.2.4	166.62.27.57
Nov 19, 2020 16:03:11.245273113 CET	49746	587	192.168.2.4	166.62.27.57
Nov 19, 2020 16:03:11.245419979 CET	49746	587	192.168.2.4	166.62.27.57
Nov 19, 2020 16:03:11.245482922 CET	49746	587	192.168.2.4	166.62.27.57
Nov 19, 2020 16:03:11.245569944 CET	49746	587	192.168.2.4	166.62.27.57
Nov 19, 2020 16:03:11.245651960 CET	49746	587	192.168.2.4	166.62.27.57
Nov 19, 2020 16:03:11.517080069 CET	587	49746	166.62.27.57	192.168.2.4
Nov 19, 2020 16:03:11.517100096 CET	587	49746	166.62.27.57	192.168.2.4
Nov 19, 2020 16:03:11.518004894 CET	587	49746	166.62.27.57	192.168.2.4
Nov 19, 2020 16:03:11.527730942 CET	587	49746	166.62.27.57	192.168.2.4
Nov 19, 2020 16:03:11.580365896 CET	49746	587	192.168.2.4	166.62.27.57
Nov 19, 2020 16:03:38.239831924 CET	49738	80	192.168.2.4	104.16.154.36
Nov 19, 2020 16:03:38.239991903 CET	49746	587	192.168.2.4	166.62.27.57
Nov 19, 2020 16:03:42.909209967 CET	49764	80	192.168.2.4	104.16.155.36
Nov 19, 2020 16:03:42.925932884 CET	80	49764	104.16.155.36	192.168.2.4
Nov 19, 2020 16:03:42.927194118 CET	49764	80	192.168.2.4	104.16.155.36
Nov 19, 2020 16:03:42.927691936 CET	49764	80	192.168.2.4	104.16.155.36
Nov 19, 2020 16:03:42.944050074 CET	80	49764	104.16.155.36	192.168.2.4
Nov 19, 2020 16:03:42.956650972 CET	80	49764	104.16.155.36	192.168.2.4
Nov 19, 2020 16:03:43.004832029 CET	49764	80	192.168.2.4	104.16.155.36
Nov 19, 2020 16:03:43.006668091 CET	49765	443	192.168.2.4	104.16.154.36
Nov 19, 2020 16:03:43.023049116 CET	443	49765	104.16.154.36	192.168.2.4
Nov 19, 2020 16:03:43.023211956 CET	49765	443	192.168.2.4	104.16.154.36
Nov 19, 2020 16:03:43.093427896 CET	49765	443	192.168.2.4	104.16.154.36
Nov 19, 2020 16:03:43.109797001 CET	443	49765	104.16.154.36	192.168.2.4
Nov 19, 2020 16:03:43.113091946 CET	443	49765	104.16.154.36	192.168.2.4
Nov 19, 2020 16:03:43.113338947 CET	443	49765	104.16.154.36	192.168.2.4
Nov 19, 2020 16:03:43.113598108 CET	49765	443	192.168.2.4	104.16.154.36
Nov 19, 2020 16:03:43.115885019 CET	49765	443	192.168.2.4	104.16.154.36
Nov 19, 2020 16:03:43.117397070 CET	49766	443	192.168.2.4	104.16.154.36
Nov 19, 2020 16:03:43.132205963 CET	443	49765	104.16.154.36	192.168.2.4
Nov 19, 2020 16:03:43.133662939 CET	443	49766	104.16.154.36	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 16:03:43.134159088 CET	49766	443	192.168.2.4	104.16.154.36
Nov 19, 2020 16:03:43.134731054 CET	49766	443	192.168.2.4	104.16.154.36
Nov 19, 2020 16:03:43.151000023 CET	443	49766	104.16.154.36	192.168.2.4
Nov 19, 2020 16:03:43.151611090 CET	443	49766	104.16.154.36	192.168.2.4
Nov 19, 2020 16:03:43.152143002 CET	443	49766	104.16.154.36	192.168.2.4
Nov 19, 2020 16:03:43.154800892 CET	49766	443	192.168.2.4	104.16.154.36
Nov 19, 2020 16:03:43.156320095 CET	49766	443	192.168.2.4	104.16.154.36
Nov 19, 2020 16:03:43.172498941 CET	443	49766	104.16.154.36	192.168.2.4
Nov 19, 2020 16:03:51.623248100 CET	49764	80	192.168.2.4	104.16.155.36
Nov 19, 2020 16:03:58.110135078 CET	49774	80	192.168.2.4	104.16.155.36
Nov 19, 2020 16:03:58.126528978 CET	80	49774	104.16.155.36	192.168.2.4
Nov 19, 2020 16:03:58.126627922 CET	49774	80	192.168.2.4	104.16.155.36
Nov 19, 2020 16:03:58.127439022 CET	49774	80	192.168.2.4	104.16.155.36
Nov 19, 2020 16:03:58.143625021 CET	80	49774	104.16.155.36	192.168.2.4
Nov 19, 2020 16:03:58.157450914 CET	80	49774	104.16.155.36	192.168.2.4
Nov 19, 2020 16:03:58.206037998 CET	49775	443	192.168.2.4	104.16.155.36
Nov 19, 2020 16:03:58.222534895 CET	443	49775	104.16.155.36	192.168.2.4
Nov 19, 2020 16:03:58.222623110 CET	49775	443	192.168.2.4	104.16.155.36
Nov 19, 2020 16:03:58.255884886 CET	49774	80	192.168.2.4	104.16.155.36
Nov 19, 2020 16:03:58.290390015 CET	49775	443	192.168.2.4	104.16.155.36
Nov 19, 2020 16:03:58.306818008 CET	443	49775	104.16.155.36	192.168.2.4
Nov 19, 2020 16:03:58.307987928 CET	443	49775	104.16.155.36	192.168.2.4
Nov 19, 2020 16:03:58.308088064 CET	443	49775	104.16.155.36	192.168.2.4
Nov 19, 2020 16:03:58.308149099 CET	49775	443	192.168.2.4	104.16.155.36

UDP Packets

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 16:02:37.347265005 CET	49910	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:02:37.374398947 CET	53	49910	8.8.8.8	192.168.2.4
Nov 19, 2020 16:02:38.091876030 CET	55854	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:02:38.118879080 CET	53	55854	8.8.8.8	192.168.2.4
Nov 19, 2020 16:02:39.153587103 CET	64549	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:02:39.180571079 CET	53	64549	8.8.8.8	192.168.2.4
Nov 19, 2020 16:02:40.477577925 CET	63153	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:02:40.504650116 CET	53	63153	8.8.8.8	192.168.2.4
Nov 19, 2020 16:02:41.419821024 CET	52991	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:02:41.446788073 CET	53	52991	8.8.8.8	192.168.2.4
Nov 19, 2020 16:02:42.287302017 CET	53700	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:02:42.314332962 CET	53	53700	8.8.8.8	192.168.2.4
Nov 19, 2020 16:02:48.014317989 CET	51726	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:02:48.058628082 CET	53	51726	8.8.8.8	192.168.2.4
Nov 19, 2020 16:02:53.947966099 CET	56794	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:02:53.983439922 CET	53	56794	8.8.8.8	192.168.2.4
Nov 19, 2020 16:02:54.437556982 CET	56534	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:02:54.475153923 CET	53	56534	8.8.8.8	192.168.2.4
Nov 19, 2020 16:02:54.565713882 CET	56627	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:02:54.592853069 CET	53	56627	8.8.8.8	192.168.2.4
Nov 19, 2020 16:02:59.422950029 CET	56621	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:02:59.449935913 CET	53	56621	8.8.8.8	192.168.2.4
Nov 19, 2020 16:03:01.729206085 CET	63116	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:03:01.756218910 CET	53	63116	8.8.8.8	192.168.2.4
Nov 19, 2020 16:03:03.427460909 CET	64078	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:03:03.454576969 CET	53	64078	8.8.8.8	192.168.2.4
Nov 19, 2020 16:03:06.844546080 CET	64801	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:03:06.871615887 CET	53	64801	8.8.8.8	192.168.2.4
Nov 19, 2020 16:03:08.569644928 CET	61721	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:03:08.608561039 CET	53	61721	8.8.8.8	192.168.2.4
Nov 19, 2020 16:03:26.334978104 CET	51255	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:03:26.370476961 CET	53	51255	8.8.8.8	192.168.2.4
Nov 19, 2020 16:03:27.336630106 CET	61522	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:03:27.372004986 CET	53	61522	8.8.8.8	192.168.2.4
Nov 19, 2020 16:03:27.923398972 CET	52337	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:03:27.950417042 CET	53	52337	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 16:03:28.391411066 CET	55046	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:03:28.429313898 CET	53	55046	8.8.8.8	192.168.2.4
Nov 19, 2020 16:03:28.727895975 CET	49612	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:03:28.763827085 CET	53	49612	8.8.8.8	192.168.2.4
Nov 19, 2020 16:03:29.180068016 CET	49285	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:03:29.215704918 CET	53	49285	8.8.8.8	192.168.2.4
Nov 19, 2020 16:03:29.484210014 CET	50601	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:03:29.528075933 CET	53	50601	8.8.8.8	192.168.2.4
Nov 19, 2020 16:03:29.613588095 CET	60875	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:03:29.649548054 CET	53	60875	8.8.8.8	192.168.2.4
Nov 19, 2020 16:03:30.169581890 CET	56448	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:03:30.207268953 CET	53	56448	8.8.8.8	192.168.2.4
Nov 19, 2020 16:03:31.013119936 CET	59172	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:03:31.048868895 CET	53	59172	8.8.8.8	192.168.2.4
Nov 19, 2020 16:03:31.545161009 CET	62420	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:03:31.572143078 CET	53	62420	8.8.8.8	192.168.2.4
Nov 19, 2020 16:03:32.255084038 CET	60579	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:03:32.282471895 CET	53	60579	8.8.8.8	192.168.2.4
Nov 19, 2020 16:03:32.378735065 CET	50183	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:03:32.415395975 CET	53	50183	8.8.8.8	192.168.2.4
Nov 19, 2020 16:03:32.917269945 CET	61531	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:03:32.944896936 CET	53	61531	8.8.8.8	192.168.2.4
Nov 19, 2020 16:03:33.035890102 CET	49228	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:03:33.063143969 CET	53	49228	8.8.8.8	192.168.2.4
Nov 19, 2020 16:03:42.322643995 CET	59794	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:03:42.349766016 CET	53	59794	8.8.8.8	192.168.2.4
Nov 19, 2020 16:03:42.565202951 CET	55916	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:03:42.601363897 CET	53	55916	8.8.8.8	192.168.2.4
Nov 19, 2020 16:03:42.855329990 CET	52752	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:03:42.890909910 CET	53	52752	8.8.8.8	192.168.2.4
Nov 19, 2020 16:03:42.963808060 CET	60542	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:03:43.004244089 CET	53	60542	8.8.8.8	192.168.2.4
Nov 19, 2020 16:03:45.724968910 CET	60689	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:03:45.760621071 CET	53	60689	8.8.8.8	192.168.2.4
Nov 19, 2020 16:03:49.401329994 CET	64206	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:03:49.440566063 CET	53	64206	8.8.8.8	192.168.2.4
Nov 19, 2020 16:03:56.284164906 CET	50904	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:03:56.319935083 CET	53	50904	8.8.8.8	192.168.2.4
Nov 19, 2020 16:03:58.046384096 CET	57525	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:03:58.082009077 CET	53	57525	8.8.8.8	192.168.2.4
Nov 19, 2020 16:03:58.168235064 CET	53814	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:03:58.204073906 CET	53	53814	8.8.8.8	192.168.2.4
Nov 19, 2020 16:03:58.208667994 CET	53418	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:03:58.235800982 CET	53	53418	8.8.8.8	192.168.2.4
Nov 19, 2020 16:03:59.443418980 CET	62833	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:03:59.470434904 CET	53	62833	8.8.8.8	192.168.2.4
Nov 19, 2020 16:04:01.499191046 CET	59260	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:04:01.534805059 CET	53	59260	8.8.8.8	192.168.2.4
Nov 19, 2020 16:04:10.725539923 CET	49944	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:04:10.771277905 CET	53	49944	8.8.8.8	192.168.2.4
Nov 19, 2020 16:04:18.482359886 CET	63300	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:04:18.509577990 CET	53	63300	8.8.8.8	192.168.2.4
Nov 19, 2020 16:04:21.843602896 CET	61449	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:04:21.879123926 CET	53	61449	8.8.8.8	192.168.2.4
Nov 19, 2020 16:04:22.194811106 CET	51275	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:04:22.230504036 CET	53	51275	8.8.8.8	192.168.2.4
Nov 19, 2020 16:04:22.299546957 CET	63492	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:04:22.309029102 CET	58945	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:04:22.335187912 CET	53	63492	8.8.8.8	192.168.2.4
Nov 19, 2020 16:04:22.344558001 CET	53	58945	8.8.8.8	192.168.2.4
Nov 19, 2020 16:04:25.163994074 CET	60779	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:04:25.191025019 CET	53	60779	8.8.8.8	192.168.2.4
Nov 19, 2020 16:04:35.599082947 CET	64014	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:04:35.634669065 CET	53	64014	8.8.8.8	192.168.2.4

Timestamp	Source Port	Dest Port	Source IP	Dest IP
Nov 19, 2020 16:04:35.926879883 CET	57091	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:04:35.962539911 CET	53	57091	8.8.8.8	192.168.2.4
Nov 19, 2020 16:04:36.047477961 CET	55904	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:04:36.082937956 CET	53	55904	8.8.8.8	192.168.2.4
Nov 19, 2020 16:04:38.866419077 CET	52109	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:04:38.893517017 CET	53	52109	8.8.8.8	192.168.2.4
Nov 19, 2020 16:04:47.181365967 CET	54450	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:04:47.216671944 CET	53	54450	8.8.8.8	192.168.2.4
Nov 19, 2020 16:04:47.244704962 CET	49374	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:04:47.279954910 CET	53	49374	8.8.8.8	192.168.2.4
Nov 19, 2020 16:04:47.332782984 CET	50436	53	192.168.2.4	8.8.8.8
Nov 19, 2020 16:04:47.368083954 CET	53	50436	8.8.8.8	192.168.2.4

DNS Queries

Timestamp	Source IP	Dest IP	Trans ID	OP Code	Name	Type	Class
Nov 19, 2020 16:02:53.947966099 CET	192.168.2.4	8.8.8.8	0x1630	Standard query (0)	201.75.14.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Nov 19, 2020 16:02:54.437556982 CET	192.168.2.4	8.8.8.8	0xb1c	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)
Nov 19, 2020 16:02:54.565713882 CET	192.168.2.4	8.8.8.8	0x3b3c	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)
Nov 19, 2020 16:03:08.569644928 CET	192.168.2.4	8.8.8.8	0x1187	Standard query (0)	mail.iigcest.com	A (IP address)	IN (0x0001)
Nov 19, 2020 16:03:42.565202951 CET	192.168.2.4	8.8.8.8	0xa237	Standard query (0)	201.75.14.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Nov 19, 2020 16:03:42.855329990 CET	192.168.2.4	8.8.8.8	0x1544	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)
Nov 19, 2020 16:03:42.963808060 CET	192.168.2.4	8.8.8.8	0x9d9e	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)
Nov 19, 2020 16:03:56.284164906 CET	192.168.2.4	8.8.8.8	0xabe9	Standard query (0)	201.75.14.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Nov 19, 2020 16:03:58.046384096 CET	192.168.2.4	8.8.8.8	0xf967	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)
Nov 19, 2020 16:03:58.168235064 CET	192.168.2.4	8.8.8.8	0xc658	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)
Nov 19, 2020 16:04:10.725539923 CET	192.168.2.4	8.8.8.8	0x5c45	Standard query (0)	mail.iigcest.com	A (IP address)	IN (0x0001)
Nov 19, 2020 16:04:21.843602896 CET	192.168.2.4	8.8.8.8	0x2ed2	Standard query (0)	201.75.14.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Nov 19, 2020 16:04:22.194811106 CET	192.168.2.4	8.8.8.8	0x93bd	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)
Nov 19, 2020 16:04:22.309029102 CET	192.168.2.4	8.8.8.8	0x693a	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)
Nov 19, 2020 16:04:35.599082947 CET	192.168.2.4	8.8.8.8	0x3a36	Standard query (0)	201.75.14.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Nov 19, 2020 16:04:35.926879883 CET	192.168.2.4	8.8.8.8	0x5b58	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)
Nov 19, 2020 16:04:36.047477961 CET	192.168.2.4	8.8.8.8	0x4193	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)
Nov 19, 2020 16:04:47.181365967 CET	192.168.2.4	8.8.8.8	0x9317	Standard query (0)	201.75.14.0.in-addr.arpa	PTR (Pointer record)	IN (0x0001)
Nov 19, 2020 16:04:47.244704962 CET	192.168.2.4	8.8.8.8	0xce8d	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)
Nov 19, 2020 16:04:47.332782984 CET	192.168.2.4	8.8.8.8	0xf3c1	Standard query (0)	whatismyip address.com	A (IP address)	IN (0x0001)

DNS Answers

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 19, 2020 16:02:53.983439922 CET	8.8.8.8	192.168.2.4	0x1630	Name error (3)	201.75.14.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Nov 19, 2020 16:02:54.475153923 CET	8.8.8.8	192.168.2.4	0xb1c	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)
Nov 19, 2020 16:02:54.475153923 CET	8.8.8.8	192.168.2.4	0xb1c	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Nov 19, 2020 16:02:54.592853069 CET	8.8.8.8	192.168.2.4	0x3b3c	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 19, 2020 16:02:54.592853069 CET	8.8.8.8	192.168.2.4	0x3b3c	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Nov 19, 2020 16:03:08.608561039 CET	8.8.8.8	192.168.2.4	0x1187	No error (0)	mail.iigcest.com		166.62.27.57	A (IP address)	IN (0x0001)
Nov 19, 2020 16:03:42.601363897 CET	8.8.8.8	192.168.2.4	0xa237	Name error (3)	201.75.14.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Nov 19, 2020 16:03:42.890909910 CET	8.8.8.8	192.168.2.4	0x1544	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Nov 19, 2020 16:03:42.890909910 CET	8.8.8.8	192.168.2.4	0x1544	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)
Nov 19, 2020 16:03:43.004244089 CET	8.8.8.8	192.168.2.4	0x9d9e	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)
Nov 19, 2020 16:03:43.004244089 CET	8.8.8.8	192.168.2.4	0x9d9e	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Nov 19, 2020 16:03:56.319935083 CET	8.8.8.8	192.168.2.4	0xabe9	Name error (3)	201.75.14.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Nov 19, 2020 16:03:58.082009077 CET	8.8.8.8	192.168.2.4	0xf967	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Nov 19, 2020 16:03:58.082009077 CET	8.8.8.8	192.168.2.4	0xf967	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)
Nov 19, 2020 16:03:58.204073906 CET	8.8.8.8	192.168.2.4	0xc658	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Nov 19, 2020 16:03:58.204073906 CET	8.8.8.8	192.168.2.4	0xc658	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)
Nov 19, 2020 16:04:10.771277905 CET	8.8.8.8	192.168.2.4	0x5c45	No error (0)	mail.iigcest.com		166.62.27.57	A (IP address)	IN (0x0001)
Nov 19, 2020 16:04:21.879123926 CET	8.8.8.8	192.168.2.4	0x2ed2	Name error (3)	201.75.14.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Nov 19, 2020 16:04:22.230504036 CET	8.8.8.8	192.168.2.4	0x93bd	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)
Nov 19, 2020 16:04:22.230504036 CET	8.8.8.8	192.168.2.4	0x93bd	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Nov 19, 2020 16:04:22.344558001 CET	8.8.8.8	192.168.2.4	0x693a	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)
Nov 19, 2020 16:04:22.344558001 CET	8.8.8.8	192.168.2.4	0x693a	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Nov 19, 2020 16:04:35.634669065 CET	8.8.8.8	192.168.2.4	0x3a36	Name error (3)	201.75.14.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Nov 19, 2020 16:04:35.962539911 CET	8.8.8.8	192.168.2.4	0x5b58	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)
Nov 19, 2020 16:04:35.962539911 CET	8.8.8.8	192.168.2.4	0x5b58	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Nov 19, 2020 16:04:36.082937956 CET	8.8.8.8	192.168.2.4	0x4193	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)
Nov 19, 2020 16:04:36.082937956 CET	8.8.8.8	192.168.2.4	0x4193	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Nov 19, 2020 16:04:47.216671944 CET	8.8.8.8	192.168.2.4	0x9317	Name error (3)	201.75.14.0.in-addr.arpa	none	none	PTR (Pointer record)	IN (0x0001)
Nov 19, 2020 16:04:47.279954910 CET	8.8.8.8	192.168.2.4	0xce8d	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)
Nov 19, 2020 16:04:47.279954910 CET	8.8.8.8	192.168.2.4	0xce8d	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)

Timestamp	Source IP	Dest IP	Trans ID	Reply Code	Name	CName	Address	Type	Class
Nov 19, 2020 16:04:47.368083954 CET	8.8.8.8	192.168.2.4	0xf3c1	No error (0)	whatismyip address.com		104.16.155.36	A (IP address)	IN (0x0001)
Nov 19, 2020 16:04:47.368083954 CET	8.8.8.8	192.168.2.4	0xf3c1	No error (0)	whatismyip address.com		104.16.154.36	A (IP address)	IN (0x0001)

HTTP Request Dependency Graph

- whatismyipaddress.com

HTTP Packets

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
0	192.168.2.4	49738	104.16.154.36	80	C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe

Timestamp	kBytes transferred	Direction	Data
Nov 19, 2020 16:02:54.517074108 CET	1095	OUT	GET / HTTP/1.1 Host: whatismyipaddress.com Connection: Keep-Alive
Nov 19, 2020 16:02:54.541414976 CET	1096	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 19 Nov 2020 15:02:54 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Thu, 19 Nov 2020 16:02:54 GMT Location: https://whatismyipaddress.com/ cf-request-id: 0682a0b73b000097f6a09da000000001 Server: cloudflare CF-RAY: 5f4ad09ecebf97f6-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
1	192.168.2.4	49764	104.16.155.36	80	C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe

Timestamp	kBytes transferred	Direction	Data
Nov 19, 2020 16:03:42.927691936 CET	2233	OUT	GET / HTTP/1.1 Host: whatismyipaddress.com Connection: Keep-Alive
Nov 19, 2020 16:03:42.956650972 CET	2234	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 19 Nov 2020 15:03:42 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Thu, 19 Nov 2020 16:03:42 GMT Location: https://whatismyipaddress.com/ cf-request-id: 0682a1745600002bd6a58a5000000001 Server: cloudflare CF-RAY: 5f4ad1cd5d052bd6-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
2	192.168.2.4	49774	104.16.155.36	80	C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe

Timestamp	kBytes transferred	Direction	Data
Nov 19, 2020 16:03:58.127439022 CET	6336	OUT	GET / HTTP/1.1 Host: whatismyipaddress.com Connection: Keep-Alive
Nov 19, 2020 16:03:58.157450914 CET	6337	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 19 Nov 2020 15:03:58 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Thu, 19 Nov 2020 16:03:58 GMT Location: https://whatismyipaddress.com/ cf-request-id: 0682a1afb50000dfcfea8ac000000001 Server: cloudflare CF-RAY: 5f4ad22c5b78dfcf-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
3	192.168.2.4	49783	104.16.154.36	80	C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe

Timestamp	kBytes transferred	Direction	Data
Nov 19, 2020 16:04:22.275377035 CET	6390	OUT	GET / HTTP/1.1 Host: whatismyipaddress.com Connection: Keep-Alive
Nov 19, 2020 16:04:22.298597097 CET	6391	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 19 Nov 2020 15:04:22 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Thu, 19 Nov 2020 16:04:22 GMT Location: https://whatismyipaddress.com/ cf-request-id: 0682a20e0900002b29571f3000000001 Server: cloudflare CF-RAY: 5f4ad2c34bba2b29-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
4	192.168.2.4	49789	104.16.154.36	80	C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe

Timestamp	kBytes transferred	Direction	Data
Nov 19, 2020 16:04:36.009860039 CET	6414	OUT	GET / HTTP/1.1 Host: whatismyipaddress.com Connection: Keep-Alive
Nov 19, 2020 16:04:36.037992001 CET	6414	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 19 Nov 2020 15:04:36 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Thu, 19 Nov 2020 16:04:36 GMT Location: https://whatismyipaddress.com/ cf-request-id: 0682a243b00000c29552921000000001 Server: cloudflare CF-RAY: 5f4ad3191c7fc295-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

Session ID	Source IP	Source Port	Destination IP	Destination Port	Process
5	192.168.2.4	49794	104.16.154.36	80	C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe

Timestamp	kBytes transferred	Direction	Data
Nov 19, 2020 16:04:47.301661015 CET	6429	OUT	GET / HTTP/1.1 Host: whatismyipaddress.com Connection: Keep-Alive
Nov 19, 2020 16:04:47.330806971 CET	6430	IN	HTTP/1.1 301 Moved Permanently Date: Thu, 19 Nov 2020 15:04:47 GMT Transfer-Encoding: chunked Connection: keep-alive Cache-Control: max-age=3600 Expires: Thu, 19 Nov 2020 16:04:47 GMT Location: https://whatismyipaddress.com/ cf-request-id: 0682a26fcf00000eaf462bc000000001 Server: cloudflare CF-RAY: 5f4ad35fbef10eaf-FRA Data Raw: 30 0d 0a 0d 0a Data Ascii: 0

SMTP Packets

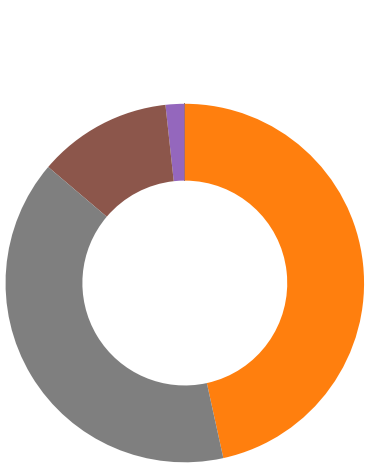
Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 19, 2020 16:03:09.597856998 CET	587	49746	166.62.27.57	192.168.2.4	220-sg2plcpnl0157.prod.sin2.secureserver.net ESMTP Exim 4.93 #2 Thu, 19 Nov 2020 08:03:09 -0700 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 19, 2020 16:03:09.598325968 CET	49746	587	192.168.2.4	166.62.27.57	EHLO 936905

Timestamp	Source Port	Dest Port	Source IP	Dest IP	Commands
Nov 19, 2020 16:03:09.869668961 CET	587	49746	166.62.27.57	192.168.2.4	250-sg2plcpnl0157.prod.sin2.secureserver.net Hello 936905 [84.17.52.25] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-CHUNKING 250-STARTTLS 250-SMTPUTF8 250 HELP
Nov 19, 2020 16:03:09.873588085 CET	49746	587	192.168.2.4	166.62.27.57	AUTH login YW5zYWZAaWlnY2VzdC5jb20=
Nov 19, 2020 16:03:10.145303011 CET	587	49746	166.62.27.57	192.168.2.4	334 UGFzc3dvcmQ6
Nov 19, 2020 16:03:10.425162077 CET	587	49746	166.62.27.57	192.168.2.4	235 Authentication succeeded
Nov 19, 2020 16:03:10.426595926 CET	49746	587	192.168.2.4	166.62.27.57	MAIL FROM:<ansaf@iigcest.com>
Nov 19, 2020 16:03:10.697953939 CET	587	49746	166.62.27.57	192.168.2.4	250 OK
Nov 19, 2020 16:03:10.699817896 CET	49746	587	192.168.2.4	166.62.27.57	RCPT TO:<ansaf@iigcest.com>
Nov 19, 2020 16:03:10.972868919 CET	587	49746	166.62.27.57	192.168.2.4	250 Accepted
Nov 19, 2020 16:03:10.973298073 CET	49746	587	192.168.2.4	166.62.27.57	DATA
Nov 19, 2020 16:03:11.244570017 CET	587	49746	166.62.27.57	192.168.2.4	354 Enter message, ending with "." on a line by itself
Nov 19, 2020 16:03:11.245651960 CET	49746	587	192.168.2.4	166.62.27.57	.
Nov 19, 2020 16:03:11.527730942 CET	587	49746	166.62.27.57	192.168.2.4	250 OK id=1kflSp-007rOY-24
Nov 19, 2020 16:04:11.305751085 CET	587	49780	166.62.27.57	192.168.2.4	220-sg2plcpnl0157.prod.sin2.secureserver.net ESMTP Exim 4.93 #2 Thu, 19 Nov 2020 08:04:11 -0700 220-We do not authorize the use of this system to transport unsolicited, 220 and/or bulk e-mail.
Nov 19, 2020 16:04:11.306165934 CET	49780	587	192.168.2.4	166.62.27.57	EHLO 936905
Nov 19, 2020 16:04:11.568952084 CET	587	49780	166.62.27.57	192.168.2.4	250-sg2plcpnl0157.prod.sin2.secureserver.net Hello 936905 [84.17.52.25] 250-SIZE 52428800 250-8BITMIME 250-PIPELINING 250-AUTH PLAIN LOGIN 250-CHUNKING 250-STARTTLS 250-SMTPUTF8 250 HELP
Nov 19, 2020 16:04:11.569655895 CET	49780	587	192.168.2.4	166.62.27.57	AUTH login YW5zYWZAaWlnY2VzdC5jb20=
Nov 19, 2020 16:04:11.837136030 CET	587	49780	166.62.27.57	192.168.2.4	334 UGFzc3dvcmQ6
Nov 19, 2020 16:04:12.112052917 CET	587	49780	166.62.27.57	192.168.2.4	235 Authentication succeeded
Nov 19, 2020 16:04:12.112370968 CET	49780	587	192.168.2.4	166.62.27.57	MAIL FROM:<ansaf@iigcest.com>
Nov 19, 2020 16:04:12.375014067 CET	587	49780	166.62.27.57	192.168.2.4	250 OK

Code Manipulations

Statistics

Behavior



- BANK-STATMENT _xlsx.exe
- BANK-STATMENT _xlsx.exe
- BANK-STATMENT _xlsx.exe
- dw20.exe
- vbc.exe
- vbc.exe
- BANK-STATMENT _xlsx.exe
- BANK-STATMENT _xlsx.exe
- BANK-STATMENT _xlsx.exe
- dw20.exe
- BANK-STATMENT _xlsx.exe
- BANK-STATMENT _xlsx.exe
- BANK-STATMENT _xlsx.exe
- dw20.exe
- vbc.exe
- vbc.exe
- BANK-STATMENT _xlsx.exe
- BANK-STATMENT _xlsx.exe
- BANK-STATMENT _xlsx.exe
- dw20.exe
- BANK-STATMENT _xlsx.exe
- BANK-STATMENT _xlsx.exe
- BANK-STATMENT _xlsx.exe
- dw20.exe

BANK-STATMENT _xlsx.exe
BANK-STATMENT _xlsx.exe
BANK-STATMENT _xlsx.exe

Click to jump to process

System Behavior

Analysis Process: BANK-STATMENT _xlsx.exe PID: 1496 Parent PID: 5864

General

Start time:	16:02:43
Start date:	19/11/2020
Path:	C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe'
Imagebase:	0x400000
File size:	965120 bytes
MD5 hash:	DEBE564CD4C27C02D23C828DF27FE27F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000002.666309079.0000000002817000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000002.666309079.0000000002817000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.666309079.0000000002817000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000002.666309079.0000000002817000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000002.666309079.0000000002817000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000000.00000002.666235176.0000000002782000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000000.00000002.666235176.0000000002782000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.666235176.0000000002782000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000000.00000002.666235176.0000000002782000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000000.00000002.666235176.0000000002782000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

Analysis Process: BANK-STATMENT _xlsx.exe PID: 4500 Parent PID: 1496

General

Start time:	16:02:43
Start date:	19/11/2020
Path:	C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe'

Imagebase:	0x400000
File size:	965120 bytes
MD5 hash:	DEBE564CD4C27C02D23C828DF27FE27F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000001.00000002.765706717.0000000000497000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000001.00000002.765706717.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000001.00000002.765706717.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000001.00000002.765706717.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000001.00000002.765706717.0000000000497000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000001.00000002.765500046.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000001.00000002.765500046.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000001.00000002.765500046.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000001.00000002.765500046.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000001.00000002.765500046.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000001.00000002.766725359.0000000002292000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000001.00000002.766725359.0000000002292000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000001.00000002.766725359.0000000002292000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000001.00000002.766725359.0000000002292000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000001.00000002.766725359.0000000002292000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000001.00000002.766451642.00000000009D0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000001.00000002.766451642.00000000009D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000001.00000002.766451642.00000000009D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000001.00000002.766451642.00000000009D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000001.00000002.766451642.00000000009D0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000001.00000002.771774923.0000000003AF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000001.00000002.771774923.0000000003AF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000001.00000002.767298778.00000000023B2000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000001.00000002.767298778.00000000023B2000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000001.00000002.767298778.00000000023B2000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source:

	00000001.00000002.767298778.00000000023B2000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000001.00000002.767298778.00000000023B2000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000001.00000002.770219917.0000000002AF1000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000001.00000002.770219917.0000000002AF1000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000001.00000002.770219917.0000000002AF1000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	722760AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	722760AC	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	722760AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	722760AC	unknown
C:\Users\user\AppData\Roaming\pid.txt	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	233BCAB	CreateFileW
C:\Users\user\AppData\Roaming\pidloc.txt	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	233BCAB	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\holdermail.txt	success or wait	1	4C95E86	DeleteFileW
C:\Users\user\AppData\Local\Temp\holderwb.txt	success or wait	1	4C95E86	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\pid.txt	unknown	4	34 35 30 30	4500	success or wait	1	4C90093	WriteFile
C:\Users\user\AppData\Roaming\pidloc.txt	unknown	46	43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 44 65 73 6b 74 6f 70 5c 42 41 4e 4b 2d 53 54 41 54 4d 45 4e 54 20 5f 78 6c 73 78 2e 65 78 65	C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe	success or wait	1	4C90093	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	4C90093	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	4C90093	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	4C90093	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	4C90093	ReadFile
C:\Users\user\AppData\Local\Temp\holdermail.txt	unknown	4096	end of file	1	4C90093	ReadFile
C:\Users\user\AppData\Local\Temp\holderwb.txt	unknown	4096	success or wait	1	4C90093	ReadFile
C:\Users\user\AppData\Local\Temp\holderwb.txt	unknown	4096	end of file	1	4C90093	ReadFile
C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe	unknown	4096	success or wait	1	7234BF06	unknown
C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe	unknown	512	success or wait	1	7234BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7234BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7234BF06	unknown

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Key Value Modified

Key Path	Name	Type	Old Data	New Data	Completion	Count	Source Address	Symbol
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced	Hidden	dword	2	1	success or wait	1	4C95326	RegSetValueExW

Analysis Process: BANK-STATMENT _xlsx.exe PID: 3984 Parent PID: 1496

General

Start time:	16:02:44
Start date:	19/11/2020
Path:	C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe' 2 4500 5715437
Imagebase:	0x400000
File size:	965120 bytes
MD5 hash:	DEBE564CD4C27C02D23C828DF27FE27F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low

Analysis Process: dw20.exe PID: 5996 Parent PID: 4500

General

Start time:	16:02:55
Start date:	19/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
Wow64 process (32bit):	true
Commandline:	dw20.exe -x -s 2264

Imagebase:	0x10000000
File size:	33936 bytes
MD5 hash:	8D10DA8A3E11747E51F23C882C22BBC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Completion	Count	Source Address	Symbol

Registry Activities

Key Path	Completion	Count	Source Address	Symbol

Key Path	Name	Type	Data	Completion	Count	Source Address	Symbol

Analysis Process: vbc.exe PID: 6920 Parent PID: 4500

General

Start time:	16:02:59
Start date:	19/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holdermail.txt'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000006.00000002.702728827.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\holdermail.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	405EFC	CreateFileA

Analysis Process: vbc.exe PID: 7044 Parent PID: 4500

General

Start time:	16:02:59
Start date:	19/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holderwb.txt'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000007.00000002.704959597.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\holderwb.txt	read attributes | synchronize | generic write	device	synchronous io non alert | non directory file	success or wait	1	407175	CreateFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\holderwb.txt	unknown	2	ff fe	..	success or wait	1	407BCF	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	100	success or wait	1	414E52	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	2048	success or wait	1	414E52	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	2048	success or wait	1	414E52	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	100	success or wait	1	414E52	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	2048	success or wait	1	414E52	ReadFile

Analysis Process: BANK-STATMENT _xlsx.exe PID: 1900 Parent PID: 3984

General

Start time:	16:03:38
Start date:	19/11/2020
Path:	C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe
Imagebase:	0x400000
File size:	965120 bytes
MD5 hash:	DEBE564CD4C27C02D23C828DF27FE27F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi

Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000E.00000002.788401031.0000000002642000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000E.00000002.788401031.0000000002642000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000E.00000002.788401031.0000000002642000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000E.00000002.788401031.0000000002642000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000E.00000002.788401031.0000000002642000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000E.00000002.788526759.00000000026D7000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000E.00000002.788526759.00000000026D7000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000E.00000002.788526759.00000000026D7000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000E.00000002.788526759.00000000026D7000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000E.00000002.788526759.00000000026D7000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

Analysis Process: BANK-STATMENT _xlsx.exe PID: 4240 Parent PID: 1900

General

Start time:	16:03:39
Start date:	19/11/2020
Path:	C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe
Imagebase:	0x400000
File size:	965120 bytes
MD5 hash:	DEBE564CD4C27C02D23C828DF27FE27F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000F.00000002.803619602.0000000002F08000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000F.00000002.803780001.0000000003A81000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000F.00000002.803780001.0000000003A81000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000F.00000002.799181132.0000000002312000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000F.00000002.799181132.0000000002312000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000F.00000002.799181132.0000000002312000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000F.00000002.799181132.0000000002312000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000F.00000002.799181132.0000000002312000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000F.00000002.803587831.0000000002F02000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000F.00000002.803587831.0000000002F02000.00000004.00000001.sdmp, Author:

	JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000F.00000002.797891393.0000000000497000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000F.00000002.797891393.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000F.00000002.797891393.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000F.00000002.797891393.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000F.00000002.797891393.0000000000497000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000F.00000002.797771687.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000F.00000002.797771687.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000F.00000002.797771687.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000F.00000002.797771687.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000F.00000002.797771687.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000F.00000002.798965975.0000000002252000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000F.00000002.798965975.0000000002252000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000F.00000002.798965975.0000000002252000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000F.00000002.798965975.0000000002252000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000F.00000002.798965975.0000000002252000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000F.00000002.798500055.0000000000810000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000F.00000002.798500055.0000000000810000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000F.00000002.798500055.0000000000810000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000000F.00000002.798500055.0000000000810000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000F.00000002.798500055.0000000000810000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000000F.00000001.785219561.00000000004D2000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000F.00000001.785219561.00000000004D2000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000000F.00000001.785219561.00000000004D2000.00000040.00020000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000000F.00000001.785219561.00000000004D2000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	722760AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	722760AC	unknown
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	722760AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	722760AC	unknown
C:\Users\user\AppData\Roaming\pid.txt	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	22FBCAB	CreateFileW
C:\Users\user\AppData\Roaming\pidloc.txt	read attributes | synchronize | generic write	device	sequential only | synchronous io non alert | non directory file | open no recall	success or wait	1	22FBCAB	CreateFileW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\pid.txt	success or wait	1	2612D8E	DeleteFileW
C:\Users\user\AppData\Roaming\pidloc.txt	success or wait	1	2612D8E	DeleteFileW

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Roaming\pid.txt	unknown	4	34 32 34 30	4240	success or wait	1	2610093	WriteFile
C:\Users\user\AppData\Roaming\pidloc.txt	unknown	46	43 3a 5c 55 73 65 72 73 5c 6a 6f 6e 65 73 5c 44 65 73 6b 74 6f 70 5c 42 41 4e 4b 2d 53 54 41 54 4d 45 4e 54 20 5f 78 6c 73 78 2e 65 78 65	C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe	success or wait	1	2610093	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	8175	end of file	1	722A5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	2610093	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	2610093	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	success or wait	1	2610093	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4096	end of file	1	2610093	ReadFile
C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe	unknown	4096	success or wait	1	7234BF06	unknown
C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe	unknown	512	success or wait	1	7234BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	4096	success or wait	1	7234BF06	unknown
C:\Windows\assembly\GAC_32\mscorlib\2.0.0.0__b77a5c561934e089\mscorlib.dll	unknown	512	success or wait	1	7234BF06	unknown

Analysis Process: BANK-STATMENT _xlsx.exe PID: 6452 Parent PID: 1900

General

Start time:	16:03:41
Start date:	19/11/2020
Path:	C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe' 2 4240 5772140
Imagebase:	0x400000
File size:	965120 bytes
MD5 hash:	DEBE564CD4C27C02D23C828DF27FE27F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low

Analysis Process: dw20.exe PID: 5456 Parent PID: 4240

General

Start time:	16:03:44
Start date:	19/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
Wow64 process (32bit):	true
Commandline:	dw20.exe -x -s 2304
Imagebase:	0x10000000
File size:	33936 bytes
MD5 hash:	8D10DA8A3E11747E51F23C882C22BBC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: BANK-STATMENT _xlsx.exe PID: 3028 Parent PID: 6452

General

Start time:	16:03:52
Start date:	19/11/2020
Path:	C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe
Imagebase:	0x400000
File size:	965120 bytes
MD5 hash:	DEBE564CD4C27C02D23C828DF27FE27F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi

Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000014.00000002.826494513.0000000002747000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000014.00000002.826494513.0000000002747000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000014.00000002.826494513.0000000002747000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000014.00000002.826494513.0000000002747000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000014.00000002.826494513.0000000002747000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000014.00000002.825220908.00000000026B2000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000014.00000002.825220908.00000000026B2000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000014.00000002.825220908.00000000026B2000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000014.00000002.825220908.00000000026B2000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000014.00000002.825220908.00000000026B2000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

Analysis Process: BANK-STATMENT _xlsx.exe PID: 1548 Parent PID: 3028

General

Start time:	16:03:53
Start date:	19/11/2020
Path:	C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe
Imagebase:	0x400000
File size:	965120 bytes
MD5 hash:	DEBE564CD4C27C02D23C828DF27FE27F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000015.00000002.852456722.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000015.00000002.852456722.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000015.00000002.852456722.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000015.00000002.852456722.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000015.00000002.852456722.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000015.00000002.853095833.00000000021E2000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000015.00000002.853095833.00000000021E2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000015.00000002.853095833.00000000021E2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000015.00000002.853095833.00000000021E2000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000015.00000002.853095833.00000000021E2000.00000004.00000001.sdmp, Author:

	JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000015.00000002.853013004.0000000002150000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000015.00000002.853013004.0000000002150000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000015.00000002.853013004.0000000002150000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000015.00000002.853013004.0000000002150000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000015.00000002.853013004.0000000002150000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000015.00000002.852539322.0000000000497000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000015.00000002.852539322.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000015.00000002.852539322.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000015.00000002.852539322.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000015.00000002.852539322.0000000000497000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000015.00000002.857805866.0000000003A31000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000015.00000002.857805866.0000000003A31000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000015.00000002.855941175.0000000002A31000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000015.00000002.855941175.0000000002A31000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000015.00000002.855941175.0000000002A31000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000015.00000001.813031999.00000000004D2000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000015.00000001.813031999.00000000004D2000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000015.00000001.813031999.00000000004D2000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000015.00000001.813031999.00000000004D2000.00000040.00020000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000015.00000001.813031999.00000000004D2000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000015.00000002.853286228.00000000022C2000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000015.00000002.853286228.00000000022C2000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000015.00000002.853286228.00000000022C2000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000015.00000002.853286228.00000000022C2000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000015.00000002.853286228.00000000022C2000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

Analysis Process: BANK-STATMENT _xlsx.exe PID: 2240 Parent PID: 3028

General

Start time:	16:03:54
Start date:	19/11/2020
Path:	C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe' 2 1548 5785125
Imagebase:	0x400000
File size:	965120 bytes
MD5 hash:	DEBE564CD4C27C02D23C828DF27FE27F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low

Analysis Process: dw20.exe PID: 5992 Parent PID: 1548

General

Start time:	16:03:59
Start date:	19/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
Wow64 process (32bit):	true
Commandline:	dw20.exe -x -s 2288
Imagebase:	0x10000000
File size:	33936 bytes
MD5 hash:	8D10DA8A3E11747E51F23C882C22BBC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: vbc.exe PID: 5676 Parent PID: 1548

General

Start time:	16:04:02
Start date:	19/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holdermail.txt'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000019.00000002.833212497.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: vbc.exe PID: 6708 Parent PID: 1548

General

Start time:	16:04:02
Start date:	19/11/2020

Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe /stext 'C:\Users\user\AppData\Local\Temp\holderwb.txt'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001A.00000002.838140213.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: BANK-STATMENT _xlsx.exe PID: 6984 Parent PID: 2240

General

Start time:	16:04:17
Start date:	19/11/2020
Path:	C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe
Imagebase:	0x400000
File size:	965120 bytes
MD5 hash:	DEBE564CD4C27C02D23C828DF27FE27F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000001C.00000002.870010845.00000000027A2000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001C.00000002.870010845.00000000027A2000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000001C.00000002.870010845.00000000027A2000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001C.00000002.870010845.00000000027A2000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000001C.00000002.870010845.00000000027A2000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000001C.00000002.870272329.0000000002837000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001C.00000002.870272329.0000000002837000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000001C.00000002.870272329.0000000002837000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001C.00000002.870272329.0000000002837000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000001C.00000002.870272329.0000000002837000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

Analysis Process: BANK-STATMENT _xlsx.exe PID: 6180 Parent PID: 6984

General

Start time:	16:04:18

Start date:	19/11/2020
Path:	C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe
Imagebase:	0x400000
File size:	965120 bytes
MD5 hash:	DEBE564CD4C27C02D23C828DF27FE27F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000001D.00000002.885749429.0000000002F48000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000001D.00000002.883606602.0000000002462000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001D.00000002.883606602.0000000002462000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000001D.00000002.883606602.0000000002462000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001D.00000002.883606602.0000000002462000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000001D.00000002.883606602.0000000002462000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000001D.00000002.883042234.0000000000AD0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001D.00000002.883042234.0000000000AD0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000001D.00000002.883042234.0000000000AD0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001D.00000002.883042234.0000000000AD0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000001D.00000002.883042234.0000000000AD0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000001D.00000002.885702309.0000000002F42000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000001D.00000002.885702309.0000000002F42000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001D.00000002.886068587.0000000003AC1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001D.00000002.886068587.0000000003AC1000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000001D.00000002.883478400.00000000023D2000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001D.00000002.883478400.00000000023D2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000001D.00000002.883478400.00000000023D2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001D.00000002.883478400.00000000023D2000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000001D.00000002.883478400.00000000023D2000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000001D.00000002.882401105.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001D.00000002.882401105.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000001D.00000002.882401105.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001D.00000002.882401105.0000000000402000.00000040.00000001.sdmp, Author:

	Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000001D.00000002.882401105.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 0000001D.00000002.882514988.0000000000497000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000001D.00000002.882514988.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 0000001D.00000002.882514988.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 0000001D.00000002.882514988.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 0000001D.00000002.882514988.0000000000497000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

Analysis Process: BANK-STATMENT _xlsx.exe PID: 6188 Parent PID: 6984

General

Start time:	16:04:19
Start date:	19/11/2020
Path:	C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe' 2 6180 5810484
Imagebase:	0x400000
File size:	965120 bytes
MD5 hash:	DEBE564CD4C27C02D23C828DF27FE27F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low

Analysis Process: dw20.exe PID: 5484 Parent PID: 6180

General

Start time:	16:04:23
Start date:	19/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
Wow64 process (32bit):	true
Commandline:	dw20.exe -x -s 2264
Imagebase:	0x10000000
File size:	33936 bytes
MD5 hash:	8D10DA8A3E11747E51F23C882C22BBC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: BANK-STATMENT _xlsx.exe PID: 5540 Parent PID: 6188

General

Start time:	16:04:30
Start date:	19/11/2020
Path:	C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe
Wow64 process (32bit):	true

Commandline:	C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe
Imagebase:	0x400000
File size:	965120 bytes
MD5 hash:	DEBE564CD4C27C02D23C828DF27FE27F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000021.00000002.903399921.0000000002642000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000021.00000002.903399921.0000000002642000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000021.00000002.903399921.0000000002642000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000021.00000002.903399921.0000000002642000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000021.00000002.903399921.0000000002642000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000021.00000002.903584502.00000000026D7000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000021.00000002.903584502.00000000026D7000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000021.00000002.903584502.00000000026D7000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000021.00000002.903584502.00000000026D7000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000021.00000002.903584502.00000000026D7000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

Analysis Process: BANK-STATMENT _xlsx.exe PID: 5580 Parent PID: 5540

General

Start time:	16:04:30
Start date:	19/11/2020
Path:	C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe
Imagebase:	0x400000
File size:	965120 bytes
MD5 hash:	DEBE564CD4C27C02D23C828DF27FE27F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000022.00000002.915921004.0000000003032000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000022.00000002.915921004.0000000003032000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000022.00000002.912614884.0000000002362000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000022.00000002.912614884.0000000002362000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000022.00000002.912614884.0000000002362000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000022.00000002.912614884.0000000002362000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000022.00000002.912614884.0000000002362000.00000004.00000001.sdmp, Author:

	JPCERT/CC Incident Response Group • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000022.00000002.915989570.0000000003038000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000022.00000001.893606211.00000000004D2000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000022.00000001.893606211.00000000004D2000.00000040.00020000.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000022.00000001.893606211.00000000004D2000.00000040.00020000.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000022.00000001.893606211.00000000004D2000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000022.00000002.912543574.00000000022D0000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000022.00000002.912543574.00000000022D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000022.00000002.912543574.00000000022D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000022.00000002.912543574.00000000022D0000.00000004.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000022.00000002.912543574.00000000022D0000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000022.00000002.912719183.0000000002402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000022.00000002.912719183.0000000002402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000022.00000002.912719183.0000000002402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000022.00000002.912719183.0000000002402000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000022.00000002.912719183.0000000002402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000022.00000002.911923188.0000000000497000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000022.00000002.911923188.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000022.00000002.911923188.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000022.00000002.911923188.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000022.00000002.911923188.0000000000497000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000022.00000002.916237371.0000000003BB1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000022.00000002.916237371.0000000003BB1000.00000004.00000001.sdmp, Author: Joe Security • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000022.00000002.911809266.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000022.00000002.911809266.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000022.00000002.911809266.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000022.00000002.911809266.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000022.00000002.911809266.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
Reputation:	low

Analysis Process: BANK-STATMENT _xlsx.exe PID: 5588 Parent PID: 5540

General

Start time:	16:04:31
Start date:	19/11/2020
Path:	C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe' 2 5580 5822718
Imagebase:	0x400000
File size:	965120 bytes
MD5 hash:	DEBE564CD4C27C02D23C828DF27FE27F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi
Reputation:	low

Analysis Process: dw20.exe PID: 6904 Parent PID: 5580

General

Start time:	16:04:37
Start date:	19/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\dw20.exe
Wow64 process (32bit):	true
Commandline:	dw20.exe -x -s 2324
Imagebase:	0x10000000
File size:	33936 bytes
MD5 hash:	8D10DA8A3E11747E51F23C882C22BBC3
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: BANK-STATMENT _xlsx.exe PID: 6176 Parent PID: 5588

General

Start time:	16:04:43
Start date:	19/11/2020
Path:	C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe
Imagebase:	0x400000
File size:	965120 bytes
MD5 hash:	DEBE564CD4C27C02D23C828DF27FE27F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi

Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000025.00000002.926331050.0000000002857000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000025.00000002.926331050.0000000002857000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000025.00000002.926331050.0000000002857000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000025.00000002.926331050.0000000002857000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000025.00000002.926331050.0000000002857000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000025.00000002.926178784.00000000027C2000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000025.00000002.926178784.00000000027C2000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000025.00000002.926178784.00000000027C2000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000025.00000002.926178784.00000000027C2000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000025.00000002.926178784.00000000027C2000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group

Analysis Process: BANK-STATMENT _xlsx.exe PID: 2864 Parent PID: 6176

General

Start time:	16:04:44
Start date:	19/11/2020
Path:	C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe
Imagebase:	0x400000
File size:	965120 bytes
MD5 hash:	DEBE564CD4C27C02D23C828DF27FE27F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000026.00000002.928753119.0000000000497000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000026.00000002.928753119.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000026.00000002.928753119.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000026.00000002.928753119.0000000000497000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000026.00000002.928753119.0000000000497000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000026.00000002.928377317.0000000000402000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net> • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000026.00000002.928377317.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000026.00000002.928377317.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000026.00000002.928377317.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000026.00000002.928377317.0000000000402000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group

- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000026.00000002.932841604.0000000002F34000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000026.00000002.932841604.0000000002F34000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000026.00000002.933151800.0000000003AC1000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000026.00000002.933151800.0000000003AC1000.00000004.00000001.sdmp, Author: Joe Security
- Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000026.00000001.923369049.00000000004D2000.00000040.00020000.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000026.00000001.923369049.00000000004D2000.00000040.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000026.00000001.923369049.00000000004D2000.00000040.00020000.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000026.00000001.923369049.00000000004D2000.00000040.00020000.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000026.00000001.923369049.00000000004D2000.00000040.00020000.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000026.00000002.930718312.00000000022C2000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000026.00000002.930718312.00000000022C2000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000026.00000002.930718312.00000000022C2000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000026.00000002.930718312.00000000022C2000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000026.00000002.930718312.00000000022C2000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000026.00000002.930882020.0000000002352000.00000040.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000026.00000002.930882020.0000000002352000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000026.00000002.930882020.0000000002352000.00000040.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000026.00000002.930882020.0000000002352000.00000040.00000001.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000026.00000002.930882020.0000000002352000.00000040.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: RAT_HawkEye, Description: Detects HawkEye RAT, Source: 00000026.00000002.930539943.0000000002230000.00000004.00000001.sdmp, Author: Kevin Breen <kevin@techanarchy.net>
- Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000026.00000002.930539943.0000000002230000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000026.00000002.930539943.0000000002230000.00000004.00000001.sdmp, Author: Joe Security
- Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000026.00000002.930539943.0000000002230000.00000004.00000001.sdmp, Author: Joe Security
- Rule: Hawkeye, Description: detect HawkEye in memory, Source: 00000026.00000002.930539943.0000000002230000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group
- Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000026.00000002.932871258.0000000002F3A000.00000004.00000001.sdmp, Author: Joe Security

Analysis Process: BANK-STATMENT _xlsx.exe PID: 4608 Parent PID: 6176

General

Start time:	16:04:45
Start date:	19/11/2020
Path:	C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\BANK-STATMENT _xlsx.exe' 2 2864 5836578
Imagebase:	0x400000
File size:	965120 bytes
MD5 hash:	DEBE564CD4C27C02D23C828DF27FE27F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	Borland Delphi

Disassembly

Code Analysis