ID: 510391
Sample Name:
KFoTnHP6B2.exe
Cookbook: default.jbs
Time: 19:02:20
Date: 27/10/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report KFoTnHP6B2.exe 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Overview 4
Dropped Files 4
Memory Dumps 5
Unpacked PEs 5
Sigma Overview 6
Jbx Signature Overview 6
AV Detection: 6
Spreading: 6
E-Banking Fraud: 6
System Summary: 6
Persistence and Installation Behavior: 6
Boot Survival: 6
HIPS / PFW / Operating System Protection Evasion: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 7
Mitre Att&ck Matrix 7
Behavior Graph 7
Screenshots 8
Thumbnails 8
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 9
Domains 10
URLs 10
Domains and IPs 10
Contacted Domains 10
URLs from Memory and Binaries 10
Contacted IPs 10
General Information 10
Simulations 11
Behavior and APIs 11
Joe Sandbox View / Context 11
IPs 11
Domains 11
ASN 11
JA3 Fingerprints 11
Dropped Files 11
Created / dropped Files 11
Static File Info 43
General 43
File Icon 43
Static PE Info 44
General 44
Entrypoint Preview 44
Rich Headers 44
Data Directories 44
Sections 44
Resources 44
Imports 44
Possible Origin 44
Network Behavior 44
Code Manipulations 44
Statistics 45
Behavior 45
System Behavior 45
Analysis Process: KFoTnHP6B2.exe PID: 5520 Parent PID: 2864 45
General 45
File Activities 45
File Created 45
File Deleted 45
File Written 45
File Read 45
Analysis Process: KFoTnHP6B2.exe PID: 4932 Parent PID: 5520 45
General 45
File Activities 46
File Created 46

File Written 46
File Read 46
Registry Activities 46
Key Value Modified 46
Disassembly 46
Code Analysis 46

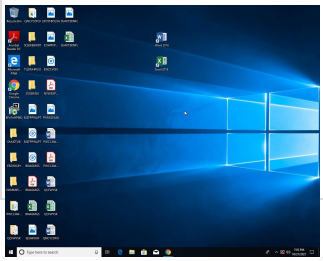
Windows Analysis Report KFoTnHP6B2.exe

Overview

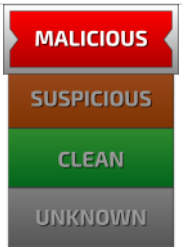
General Information

Sample Name:	KFoTnHP6B2.exe
Analysis ID:	510391
MD5:	df330ab2a2e5aa4.
SHA1:	76b5d1eee342b4..
SHA256:	99a897c5b8f53e1.
Tags:	exe
Infos:	

Most interesting Screenshot:



Detection



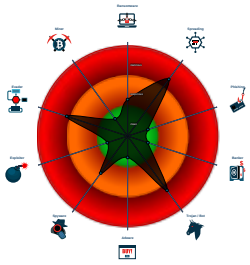
FormBook Neshta

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

Signatures

- Yara detected Neshta
- Multi AV Scanner detection for subm…
- Yara detected FormBook
- Malicious sample detected (through …
- Infects executable files (exe, dll, sys…
- Drops PE files with a suspicious file…
- Drops executable to a common third…
- Machine Learning detection for samp…
- Injects a PE file into a foreign proce…
- Creates an undocumented autostart …
- Machine Learning detection for dropp…
- Uses 32bit PE files

Classification



Process Tree

- **System is w10x64**
- KFoTnHP6B2.exe (PID: 5520 cmdline: 'C:\Users\user\Desktop\KFoTnHP6B2.exe' MD5: DF330AB2A2E5AA4AC947315EE3F93992)
  - KFoTnHP6B2.exe (PID: 4932 cmdline: 'C:\Users\user\Desktop\KFoTnHP6B2.exe' MD5: DF330AB2A2E5AA4AC947315EE3F93992)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Dropped Files

Source	Rule	Description	Author	Strings
C:\Program Files (x86)\Microsoft Office\Office16\NAMECONTROLSERVER.EXE	SUSP_NullSoftInst_Combo_Oct20_1	Detects suspicious NullSoft Installer combination with common Copyright strings	Florian Roth	• 0x8208:$a1: NullsoftInst • 0x10898:$b1: Microsoft Corporation • 0x10a30:$b1: Microsoft Corporation • 0x10ad4:$b1: Microsoft Corporation
C:\Program Files (x86)\Common Files\microsoft shared\Source Engine\OSE.EXE	SUSP_NullSoftInst_Combo_Oct20_1	Detects suspicious NullSoft Installer combination with common Copyright strings	Florian Roth	• 0x8208:$a1: NullsoftInst • 0x2df58:$b1: Microsoft Corporation • 0x2e0b8:$b1: Microsoft Corporation • 0x2e15c:$b1: Microsoft Corporation
C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\MSOSQM.EXE	SUSP_NullSoftInst_Combo_Oct20_1	Detects suspicious NullSoft Installer combination with common Copyright strings	Florian Roth	• 0x8208:$a1: NullsoftInst • 0x2e880:$b1: Microsoft Corporation • 0x2e9f4:$b1: Microsoft Corporation • 0x2ea98:$b1: Microsoft Corporation
C:\Program Files (x86)\Microsoft Office\Office16\misc.exe	SUSP_NullSoftInst_Combo_Oct20_1	Detects suspicious NullSoft Installer combination with common Copyright strings	Florian Roth	• 0x8208:$a1: NullsoftInst • 0xfd580:$b1: Microsoft Corporation • 0xfd700:$b1: Microsoft Corporation • 0xfd7a4:$b1: Microsoft Corporation

Source	Rule	Description	Author	Strings
C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\FLTLDR.EXE	SUSP_NullSoftInst_Combo_Oct20_1	Detects suspicious NullSoft Installer combination with common Copyright strings	Florian Roth	• 0x8208:$a1: NullsoftInst • 0x40d18:$b1: Microsoft Corporation • 0x40e84:$b1: Microsoft Corporation • 0x40f28:$b1: Microsoft Corporation
Click to see the 45 entries				

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000000.254262748.00000000001D0000.00000040.00000001.sdmp	MAL_Neshta_Generic	Detects Neshta malware	Florian Roth	• 0x6130:$op1: 85 C0 93 0F 85 62 FF FF FF 5E 5B 89 EC 5D C2 04 • 0x3e9e:$op2: E8 E5 F1 FF FF 8B C3 E8 C6 FF FF FF 85 C0 75 0C • 0x2460:$op3: EB 02 33 DB 8B C3 5B C3 53 85 C0 74 15 FF 15 34
00000002.00000000.258305894.00000000001D0000.00000040.00000001.sdmp	MAL_Neshta_Generic	Detects Neshta malware	Florian Roth	• 0x6130:$op1: 85 C0 93 0F 85 62 FF FF FF 5E 5B 89 EC 5D C2 04 • 0x3e9e:$op2: E8 E5 F1 FF FF 8B C3 E8 C6 FF FF FF 85 C0 75 0C • 0x2460:$op3: EB 02 33 DB 8B C3 5B C3 53 85 C0 74 15 FF 15 34
00000000.00000002.267620652.000000000F03A000.00000004.00000001.sdmp	JoeSecurity_FormBook	Yara detected FormBook	Joe Security	
00000000.00000002.267620652.000000000F03A000.00000004.00000001.sdmp	Formbook_1	autogenerated rule brought to you by yara-signator	Felix Bilstein - yara-signator at cocacoding dot com	• 0x27408:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0x27792:$sequence_0: 03 C8 0F 31 2B C1 89 45 FC • 0xa6a5:$sequence_1: 3C 24 0F 84 76 FF FF FF 3C 25 74 94 • 0xa191:$sequence_2: 3B 4F 14 73 95 85 C9 74 91 • 0xa7a7:$sequence_3: 3C 69 75 44 8B 7D 18 8B 0F • 0xa91f:$sequence_4: 5D C3 8D 50 7C 80 FA 07 • 0x281aa:$sequence_5: 0F BE 5C 0E 01 0F B6 54 0E 02 83 E3 0F C1 EA 06 • 0x940c:$sequence_6: 57 89 45 FC 89 45 F4 89 45 F8 • 0x28f22:$sequence_7: 66 89 0C 02 5B 8B E5 5D • 0xfb77:$sequence_8: 3C 54 74 04 3C 74 75 F4 • 0x10c1a:$sequence_9: 56 68 03 01 00 00 8D 85 95 FE FF FF 6A 00
00000000.00000002.267620652.000000000F03A000.00000004.00000001.sdmp	Formbook	detect Formbook in memory	JPCERT/CC Incident Response Group	• 0xcaa9:$sqlite3step: 68 34 1C 7B E1 • 0xcbbc:$sqlite3step: 68 34 1C 7B E1 • 0xcad8:$sqlite3text: 68 38 2A 90 C5 • 0xcbfd:$sqlite3text: 68 38 2A 90 C5 • 0xcaeb:$sqlite3blob: 68 53 D8 7F 8C • 0xcc13:$sqlite3blob: 68 53 D8 7F 8C
Click to see the 11 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
2.0.KFoTnHP6B2.exe.1d0000.18.unpack	MAL_Neshta_Generic	Detects Neshta malware	Florian Roth	• 0x5530:$op1: 85 C0 93 0F 85 62 FF FF FF 5E 5B 89 EC 5D C2 04 • 0x329e:$op2: E8 E5 F1 FF FF 8B C3 E8 C6 FF FF FF 85 C0 75 0C • 0x1860:$op3: EB 02 33 DB 8B C3 5B C3 53 85 C0 74 15 FF 15 34
2.0.KFoTnHP6B2.exe.1d0000.8.raw.unpack	MAL_Neshta_Generic	Detects Neshta malware	Florian Roth	• 0x6130:$op1: 85 C0 93 0F 85 62 FF FF FF 5E 5B 89 EC 5D C2 04 • 0x3e9e:$op2: E8 E5 F1 FF FF 8B C3 E8 C6 FF FF FF 85 C0 75 0C • 0x2460:$op3: EB 02 33 DB 8B C3 5B C3 53 85 C0 74 15 FF 15 34
2.0.KFoTnHP6B2.exe.1d0000.12.unpack	MAL_Neshta_Generic	Detects Neshta malware	Florian Roth	• 0x5530:$op1: 85 C0 93 0F 85 62 FF FF FF 5E 5B 89 EC 5D C2 04 • 0x329e:$op2: E8 E5 F1 FF FF 8B C3 E8 C6 FF FF FF 85 C0 75 0C • 0x1860:$op3: EB 02 33 DB 8B C3 5B C3 53 85 C0 74 15 FF 15 34
2.0.KFoTnHP6B2.exe.1d0000.4.unpack	MAL_Neshta_Generic	Detects Neshta malware	Florian Roth	• 0x5530:$op1: 85 C0 93 0F 85 62 FF FF FF 5E 5B 89 EC 5D C2 04 • 0x329e:$op2: E8 E5 F1 FF FF 8B C3 E8 C6 FF FF FF 85 C0 75 0C • 0x1860:$op3: EB 02 33 DB 8B C3 5B C3 53 85 C0 74 15 FF 15 34
2.0.KFoTnHP6B2.exe.1d0000.20.raw.unpack	MAL_Neshta_Generic	Detects Neshta malware	Florian Roth	• 0x6130:$op1: 85 C0 93 0F 85 62 FF FF FF 5E 5B 89 EC 5D C2 04 • 0x3e9e:$op2: E8 E5 F1 FF FF 8B C3 E8 C6 FF FF FF 85 C0 75 0C • 0x2460:$op3: EB 02 33 DB 8B C3 5B C3 53 85 C0 74 15 FF 15 34
Click to see the 20 entries				

Sigma Overview

No Sigma rule has matched

Jbx Signature Overview

Click to jump to signature section

AV Detection:

Multi AV Scanner detection for submitted file

Yara detected FormBook

Machine Learning detection for sample

Machine Learning detection for dropped file

Spreading:

Yara detected Neshta

Infects executable files (exe, dll, sys, html)

E-Banking Fraud:

Yara detected FormBook

System Summary:

Malicious sample detected (through community Yara rule)

Persistence and Installation Behavior:

Yara detected Neshta

Infects executable files (exe, dll, sys, html)

Drops PE files with a suspicious file extension

Drops executable to a common third party application directory

Boot Survival:

Yara detected Neshta

Creates an undocumented autostart registry key

HIPS / PFW / Operating System Protection Evasion:

Injects a PE file into a foreign processes

Stealing of Sensitive Information:

Yara detected Neshta

Yara detected FormBook

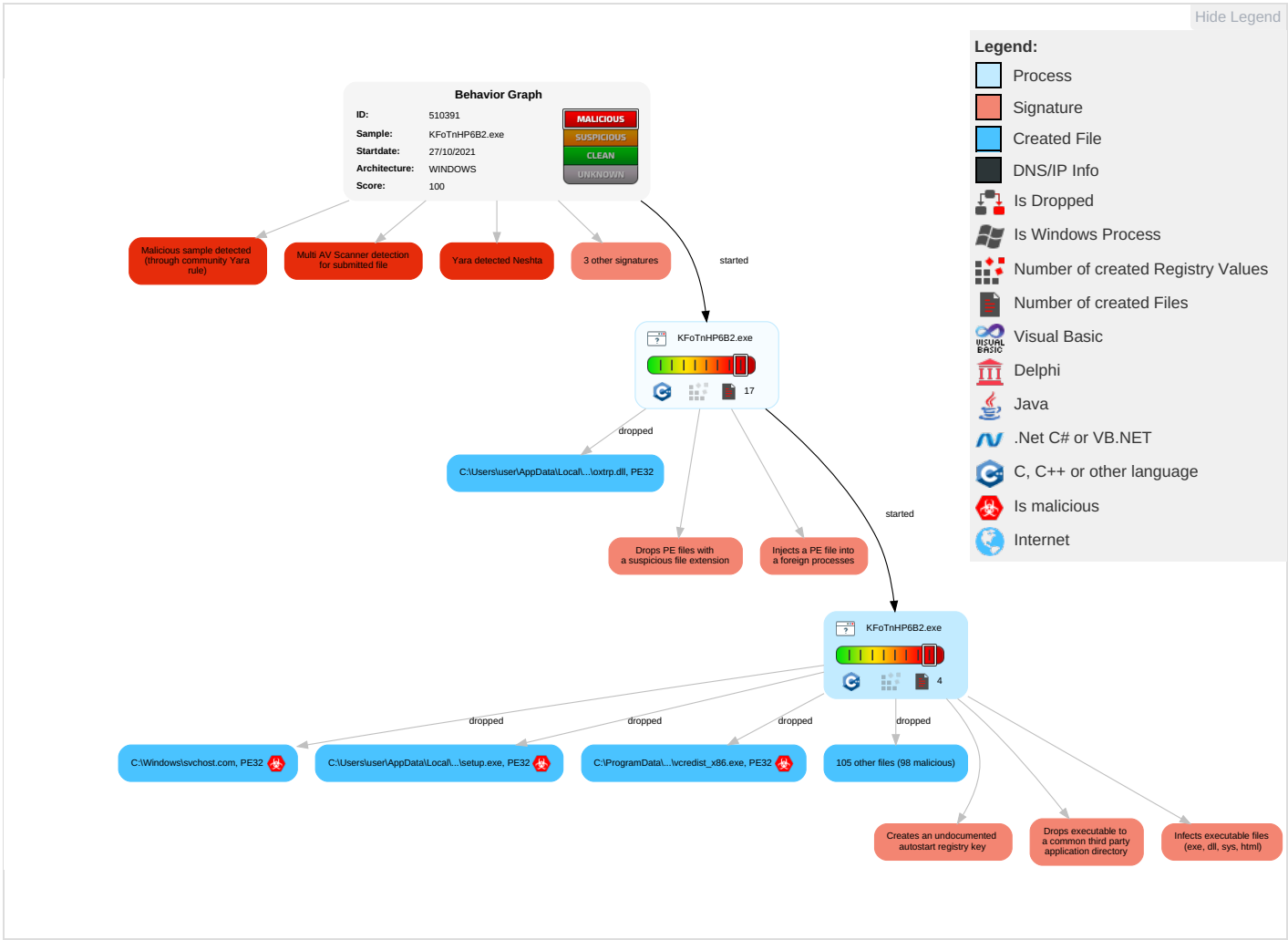
Remote Access Functionality:

Yara detected FormBook

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control	Network Effects
Valid Accounts	Windows Management Instrumentation	Registry Run Keys / Startup Folder 1	Process Injection 1 1 2	Masquerading 2 2	Input Capture 2 1	System Time Discovery 1	Taint Shared Content 1	Input Capture 2 1	Exfiltration Over Other Network Medium	Encrypted Channel 1	Eavesdrop on Insecure Network Communicatio
Default Accounts	Scheduled Task/Job	Boot or Logon Initialization Scripts	Registry Run Keys / Startup Folder 1	Process Injection 1 1 2	LSASS Memory	Security Software Discovery 2	Remote Desktop Protocol	Archive Collected Data 1	Exfiltration Over Bluetooth	Junk Data	Exploit SS7 to Redirect Phon Calls/SMS
Domain Accounts	At (Linux)	Logon Script (Windows)	Logon Script (Windows)	Deobfuscate/Decode Files or Information 1	Security Account Manager	Process Discovery 1	SMB/Windows Admin Shares	Clipboard Data 1	Automated Exfiltration	Steganography	Exploit SS7 to Track Device Location
Local Accounts	At (Windows)	Logon Script (Mac)	Logon Script (Mac)	Obfuscated Files or Information 2	NTDS	File and Directory Discovery 4	Distributed Component Object Model	Input Capture	Scheduled Transfer	Protocol Impersonation	SIM Card Swap
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Software Packing 1	LSA Secrets	System Information Discovery 1 4	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels	Manipulate Device Communicatio

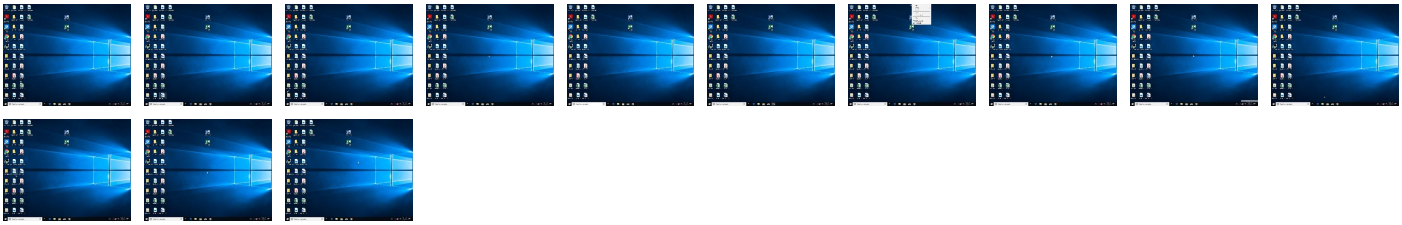
Behavior Graph



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
KFoTnHP6B2.exe	33%	Virustotal		Browse
KFoTnHP6B2.exe	34%	ReversingLabs	Win32.Trojan.Nemesis	
KFoTnHP6B2.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Program Files (x86)\AutoIt3\Aut2Exe\Aut2exe_x64.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\AutoIt3\Au3Check.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\AutoIt3\AutoIt3Help.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Common Files\Java\Java Update\jaureg.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\pi_brokers\32BitMAPIBroker.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroBroker.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\FullTrustNotifier.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\AutoIt3\Aut2Exe\Aut2exe.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\AutoIt3\Au3Info.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\AutoIt3\Au3Info_x64.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\AutoIt3\SciTE\SciTE.exe	100%	Joe Sandbox ML		
C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ose.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\AutoIt3\AutoIt3_x64.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Browser\WCChromeExtn\WCChromeNativeMessagingHost.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AdobeCollabSync.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Eula.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\ADelRCP.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\reader_sl.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\AutoIt3\Uninstall.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\arh.exe	100%	Joe Sandbox ML		
C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\setup.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\LogTransport2.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\wow_helper.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\pi_brokers\64BitMAPIBroker.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\AutoIt3\Aut2Exe\upx.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroTextExtractor.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe	100%	Joe Sandbox ML		
C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARMHelper.exe	100%	Joe Sandbox ML		

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
2.0.KFoTnHP6B2.exe.1d0000.4.unpack	100%	Avira	W32/Delf.I		Download File
2.0.KFoTnHP6B2.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
2.0.KFoTnHP6B2.exe.1d0000.12.unpack	100%	Avira	W32/Delf.I		Download File
0.2.KFoTnHP6B2.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
2.0.KFoTnHP6B2.exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
2.0.KFoTnHP6B2.exe.1d0000.18.unpack	100%	Avira	W32/Delf.I		Download File
2.0.KFoTnHP6B2.exe.400000.9.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
2.2.KFoTnHP6B2.exe.400000.2.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
2.0.KFoTnHP6B2.exe.400000.25.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
2.0.KFoTnHP6B2.exe.400000.13.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
2.0.KFoTnHP6B2.exe.1d0000.8.unpack	100%	Avira	W32/Delf.I		Download File
2.0.KFoTnHP6B2.exe.1d0000.22.unpack	100%	Avira	W32/Delf.I		Download File
0.2.KFoTnHP6B2.exe.f030000.2.unpack	100%	Avira	W32/Delf.I		Download File
2.0.KFoTnHP6B2.exe.1d0000.24.unpack	100%	Avira	W32/Delf.I		Download File
2.0.KFoTnHP6B2.exe.400000.17.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
2.0.KFoTnHP6B2.exe.1d0000.10.unpack	100%	Avira	W32/Delf.I		Download File
2.0.KFoTnHP6B2.exe.1d0000.20.unpack	100%	Avira	W32/Delf.I		Download File
2.0.KFoTnHP6B2.exe.400000.3.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
2.0.KFoTnHP6B2.exe.400000.7.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
2.0.KFoTnHP6B2.exe.400000.5.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
2.0.KFoTnHP6B2.exe.400000.15.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
2.0.KFoTnHP6B2.exe.400000.21.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
2.0.KFoTnHP6B2.exe.1d0000.14.unpack	100%	Avira	W32/Delf.I		Download File
2.0.KFoTnHP6B2.exe.400000.1.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
0.0.KFoTnHP6B2.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
2.0.KFoTnHP6B2.exe.400000.23.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
2.2.KFoTnHP6B2.exe.1d0000.0.unpack	100%	Avira	TR/ATRAPS.Gen		Download File
2.0.KFoTnHP6B2.exe.1d0000.6.unpack	100%	Avira	W32/Delf.I		Download File

Source	Detection	Scanner	Label	Link	Download
2.0.KFoTnHP6B2.exe.400000.19.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
2.2.KFoTnHP6B2.exe.1da698.1.unpack	100%	Avira	TR/Patched.Ren.Gen		Download File
2.0.KFoTnHP6B2.exe.400000.11.unpack	100%	Avira	HEUR/AGEN.1130366		Download File
2.0.KFoTnHP6B2.exe.1d0000.16.unpack	100%	Avira	W32/Delf.I		Download File

Domains

No Antivirus matches

URLs

No Antivirus matches

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	33.0.0 White Diamond
Analysis ID:	510391
Start date:	27.10.2021
Start time:	19:02:20
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 9m 38s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	KFoTnHP6B2.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:	23
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.spre.troj.evad.winEXE@4/111@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 52.1% (good quality ratio 50.2%) • Quality average: 82.8% • Quality standard deviation: 26.8%
HCA Information:	• Successful, ratio: 63% • Number of executed functions: 0 • Number of non-executed functions: 0

Cookbook Comments:	• Adjust boot time • Enable AMSI • Found application associated with file extension: .exe
Warnings:	Show All

Simulations

Behavior and APIs

No simulations

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ose.exe	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	244400
Entropy (8bit):	6.534400579891719
Encrypted:	false
SSDEEP:	6144:wBlL/cFeySe8AIqpoHbnDns1ND97deKzC/y:Ce0yV8hEoHbl3x/1
MD5:	FB6452067D5C2F6F735B1BC3AFCCBC95
SHA1:	075841CD8B1F9FDBE816AA9C29BE925EC849678F
SHA-256:	78164E58DD523291E6FE297191E25E382FF0E13E04E68A1DE30A0A48B72AF710
SHA-512:	3CDBCC421F7470F2DA1D9783D9BB3A561211AD69F77EA72ECCA63610BA2EAC5D9E89010C653B62D8C47A16C13A67CDACD6C5C6B20BA5E96BDB0FBEF5D1AF 7F9A
Malicious:	**true**
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ose.exe, Author: Florian Roth
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low

C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\ose.exe

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\setup.exe

Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	278208
Entropy (8bit):	4.157906791577724
Encrypted:	false
SSDEEP:	3072:wBynOpL12riocLMtFGVO4Mqg+WDr8LRkgUA1nQZs:wBlL/cVQLZLRp1nQm
MD5:	04A4C7405F340503C58C25D834020CC1
SHA1:	907B8F42B9365D80A57986828BD4C7C07944B3CA
SHA-256:	589D81B3CE71B6E63D494F420EBE9BC875A8429A419FA7BE47008EC4F2E7C7A7
SHA-512:	4B99CD292AF85D47DEC137B8B3BB02A7472F823F539548EEFB8D6B88784EFCD9763B241715497A7A7F33C2D9BC07AC0B33E327E89F6F2942608368A6E7B2D92(
Malicious:	**true**
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\MSOCache\All Users\{90160000-0011-0000-0000-0000000FF1CE}-C\setup.exe, Author: Florian Roth
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\ADelRCP.exe

Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	180272
Entropy (8bit):	6.313468115877264
Encrypted:	false
SSDEEP:	3072:wBynOpL12riocLMucYN0KD42sN7UGMovkIJ1jJ7LxcUUPm8aVJD37:wBlL/cuLN0K0NsjM7Lx5rJDr
MD5:	C00FC3EC9921F0E8ABDD0E1702F86270
SHA1:	96CE29B460263F8FBDC8F4F6DFC61224C76F1098
SHA-256:	EFB30DCC6F160C5A13EBB7FFD906BB54C9C83C50661556A1B5B8A8322184E7BB
SHA-512:	0798885519CEAF1CE48E26B7CE83A40DA24FC2DF8FFAB436B60D3F95028F84777E17FD6BE371DCD39A63CF97D51D08B507A9C8818008BC082EA22EA4A646231
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroBroker.exe

Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	340528
Entropy (8bit):	6.605926894448391
Encrypted:	false
SSDEEP:	6144:wBlL/cCZAyHK0TcC+TKfVM7ZoL3czvPOU4MZY7TZoopFAdEm1t:CeCZA2TcC5ko8aVoWAdEmT
MD5:	6EC96A9F1FB7859A069B407CB9D2EBB8
SHA1:	C2BAD8F075494F23896E3E17A00F772AE33D664F
SHA-256:	5117DCB442EEA30C9056E2431E48D4B05AD53C68EFDA302952C19B0922A30A43
SHA-512:	1137DE35FDA76600974D3D61AAE8AD6331A3EED6543E3D8F41B55A76C091EBBC986E5DFA635CF7608883A3071489DE6580D443EC52EC86B037E20211E1FEEAE 9
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroBroker.exe

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroCEF\RdrCEF.exe

Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	9516592
Entropy (8bit):	6.938016533212558
Encrypted:	false
SSDEEP:	98304:hDrMXEU5YPx01Dz2JhT1SbST3fX8ommgE6FWecuhd91h32zNX3CG9M:OEI2JhT1SeD/8BmgE6AkhdLh3QNd9M
MD5:	FAEE05017D753FD54E11D71800EAA075
SHA1:	BFD8C4C2E25C9B8AADB0311BD4A364624EBAFD22
SHA-256:	15B570581A92184A94E9FFBC64A822CDFA37DB5C5C0E1216E1EF29E3929880DA
SHA-512:	FDFDE5F43925ABC777D50932E19E73AA4B5E327C980E0A6503B798C78D0ACB59ECFBE5B6774AE7E99F26A62FF2947B854519E55684B3CAAC04F79B4883B2B14 8
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroRd32.exe

Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	2612784
Entropy (8bit):	6.1138812174009844
Encrypted:	false
SSDEEP:	49152:45j15HcNnCCZjaDpiA6E4O8b8ITDnlC+u:45j1KCC4Dt
MD5:	68ACAABE31116136089364A00752F356
SHA1:	DF25738533ACBE4A3DB39D70323508A5ABABFF66
SHA-256:	3067CF0A5016E0A3FDE83EAB38E5EB43DA8494DFD71776B1F4868FF87872CE1E
SHA-512:	C4EAAF472EAB0872089F83BDFE7F59BCD6FDFB158B1AA34E96ADEA8779D1F53E70BFF113BC331EC95BAA3E5B3F9501A51D1D791C293BB433179695676A188A 02
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroTextExtractor.exe

Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	90160
Entropy (8bit):	6.3649024599426305
Encrypted:	false
SSDEEP:	1536:wBWx2gmwLOuYL12EawcKocLMMMjhUpMPub5+G92qoooZVq/LF:wBynOpL12riocLMpqSwgHVqDF
MD5:	AE281D4CB1ECCBA2B9ED0FF973486164
SHA1:	776CDF79230D281F10E34D8F91CE5C2D37A2F6B9
SHA-256:	568919D9A056136CC1F4823C6BE5396F961B84FF7B29B0AEB05D72583B88373C
SHA-512:	A404115CDDD5C207097C21BDB517C6F9474F81420F7DF65F924F6D8A1C956093C796C12BD463DC844EFA7638B3E5E26F1C68133877B571074B4BE63CCAC02EC
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AcroTextExtractor.exe

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\AdobeCollabSync.exe

Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	6152240
Entropy (8bit):	6.601313953969125
Encrypted:	false
SSDEEP:	98304:yzWaiDMRWPaefvGQCB97iKezm9GIIsgCDlFXHhoswt7HPe8U:y+QI9CzWr3Ws6PpU
MD5:	AD7E7466CED1D43A1C4F1084C3DD1BD8
SHA1:	3FB10C2986F187D37F4EE6D3FFD7D767C46ED0FA
SHA-256:	072BB0AC90EF794920D8030591420A1E33A8EF7D3AFE2CCE0A22BFABE6AB7FCD
SHA-512:	15727F1FF1F7DCDAF599B2054AE08C81011257F43CA5D45AAACD47E14E6814B5013BD51F434FB1DA531CFB86FA5560CF3F1319C6492356CB9277C1E34737840E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Browser\WCChromeExtn\WCChromeNativeMessagingHost.exe

Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	190512
Entropy (8bit):	6.600381615662307
Encrypted:	false
SSDEEP:	3072:wBynOpL12riocLMQ8m4lW4L7c3BG7THxRvyAgnz8n3Nn7b4o4kbT93Kxj2:wBlL/cK4l/Lg3ovHxAcb4oJbNKxj2
MD5:	EF3D65D6F67A0E4B897D87512F7FE50F
SHA1:	1BD358B79322D204A072260DE9202B1D7175113F
SHA-256:	420F3683622A8906733930C69775499A6A57D75C6E66B699B723EFFECFB17690
SHA-512:	5BB9005A69D3C0A5DDE7845C1A428D2DD6798BF10D6695C9F176049736CF2539DDB8BB10F84EBB1E66D0103117ACCF5E6BA128CD822611282660BAFB7EEA3AE
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Eula.exe

Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	140848
Entropy (8bit):	6.325483332406092
Encrypted:	false
SSDEEP:	3072:wBynOpL12riocLMGULomFfWlF+WCP1icSLgpG88b:wBlL/cGC0+ZP1icRov
MD5:	4BF813A3E1CE761987795475996E0885
SHA1:	4970CCB0B098EF60559296A4BC19ED48BAD9ABF3
SHA-256:	E797FD3DA112E54A4337FBD18F1A42B4867D90D8805E3443E861DA160E2B37AE
SHA-512:	0EE151C83B6E00E4E8B47697C92F9310FB49E8A63605324C75F5EB1CAE3BDF87AEA471752368B2444327D7144FB46C7F2E22E5FC0B7A96D33D4B2E9132A1F995
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\Eula.exe

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\FullTrustNotifier.exe

Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	260104
Entropy (8bit):	6.3937958690244905
Encrypted:	false
SSDEEP:	3072:wBynOpL12riocLMjl4dsOc6v2vTzwU+Pho86meq+FaSoB2+vSHr8qcVz5fzsC:wBlL/cQ3PiY+Fa7BdvG1cT7
MD5:	090BDBBD4F8F5D3374A7C00CA755B37D
SHA1:	019B30DFE9E1783FB590055EFFB54B2BC85A435A
SHA-256:	FE7DE0524935466C96F248F5157DB5367EFE83EDFFB66B2E0877EB29AA119B78
SHA-512:	DB906790BA48AD29DD5374679C1B18E77CC201EE3A9122F2CD7FC2E591B1A31D0B00D86821CAD1AF6B56F11E016E7FD534ECB4E342F254B3766183B6E6615CI 9
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\LogTransport2.exe

Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	395344
Entropy (8bit):	6.418275223961166
Encrypted:	false
SSDEEP:	6144:wBlL/cT3n0dK2NP0RHx8D98WTBPW8fF8oABm1nKZ0RsrI:CeCKhHSDeWTRW8fdebmqI
MD5:	6717C805C66DA8280C3143DAF63E4AB6
SHA1:	4D47188EB4BC11F990EEDE290AE0231EBFFF7309
SHA-256:	4E4D189737792AE67F34D5CB902B81D8473E285FF05DF3CE29ACCBD1BD4C81B9
SHA-512:	5AD483E620B41A21462A0524DD58DCF60531AE59C9C85C63B7C095779A70BCC5B6E6EC7E46D8239065DA00ABEC30EEFD4F8EB00C49CD0704DE29A6A2248A5I 0D
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\arh.exe

Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	128160
Entropy (8bit):	6.369167989998417
Encrypted:	false
SSDEEP:	3072:wBynOpL12riocLMhQw/STyr5Jks7MvrMzkm8PL3Eo:wBlL/chQPQLrzkmIL3Eo
MD5:	9F0F36BA8D284D50054DEE3D66A0B073
SHA1:	43D0677D052B3D3F46205B74B1B492A02D442713
SHA-256:	29FB99019F067423BB17830309CA70739C5602382C0712F832757553C3666B65
SHA-512:	BA8E259F2A6EFDA29E1485669BA0A446C760B4DE371C4F9E8A6095E9A6A738D3BB050F4D45FCDE19A2AD58F094EC7806001D96F320EB250D44757C0A2AF2153 B
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\arh.exe

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\pi_brokers\32BitMAPIBroker.exe

Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	146416
Entropy (8bit):	6.383636075627871
Encrypted:	false
SSDEEP:	3072:wBynOpL12riocLMb7HN9fN8sFOE1Z5Y2966ilU9xL:wBlL/cPNr8stZ5/6Jl0B
MD5:	ECF13C84D7063A8AC0DB4379512A707C
SHA1:	EDAE85CB714E74DE57BB3FD676BA54E762B30E7F
SHA-256:	C298BD6484ADE0143B54BBEC3CB3259D99493A0252B2BF9585BAB972A9D61CA1
SHA-512:	A7B0E6E3B6A27B99DCD49401343395B452C5ABD74D0417AF3CDA30AFD7C140EA46D5A99338C7643EA1AD1C268D9A9BAADFF3827B35B30F4480100245F588013 8
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\plug_ins\pi_brokers\64BitMAPIBroker.exe

Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	285168
Entropy (8bit):	6.1201176224057665
Encrypted:	false
SSDEEP:	6144:wBlL/cC1UKupTu8ffMb0/GxsZfcJtqQ1UBZ6g:CeXK+HMYcytZh
MD5:	48341BABC09FDEA896D0A40893B8BD1E
SHA1:	7FE04B35BF54A6D80669EBEBC3DF6CC813F9B90E
SHA-256:	FC5DA93364244BAD97CB2D2C4805244970AFC9EEF985B9FD089A5250D739F7C7
SHA-512:	32AD74B668933232C2E61A6D184E84379B36D68115014994D14ABCDE116967D8EDD53BC3641CAC185145BA93B30E7511238F66F5755F7367CF4DD2EF43A79BD8
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\reader_sl.exe

Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	95216
Entropy (8bit):	6.260401616836404
Encrypted:	false
SSDEEP:	1536:wBWx2gmwLOuYL12EawcKocLMMM16w8MghW4wNlu9HQIXsW/44:wBynOpL12riocLMh6w8oFlKwW//
MD5:	BB5B26AECA7E7467EBAB08B955ADF845
SHA1:	5C676D6A4A7BDCFFAFDBD017AF76BD3AF9D3B788
SHA-256:	42F679AAF7DB1F63C5EBEE3B4A4AE40E043820430D3D0ABAED1976E54BCCB6CB
SHA-512:	C0E7E447962B746E8255C9B7EBD655789B3BE10D2EABAAF76F91F75D16F32622B7E67D97EBD50FEE3E7561EB0405C624BD0BBD1119E0FBB4C52296ED4D4803 C5
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\reader_sl.exe

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Adobe\Acrobat Reader DC\Reader\wow_helper.exe

Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	152112
Entropy (8bit):	6.16005581682288
Encrypted:	false
SSDEEP:	3072:wBynOpL12riocLMOMqf1XEcxJMciBx7mgkC+Jt6gA:wBlL/cOMqfSLkgr+J4P
MD5:	3FFD6CEB8032D3226844C96B07D960B7
SHA1:	2FE80AF2CE26EDDB3A39170C50581C0FC34D5C47
SHA-256:	3C2D45B2724705463EA1B5114667CF6B65256A32EEDA0C9C5A48694C5D7F71C9
SHA-512:	B4253E088160C914601F1D54BA5A4A7C3690DB08A01959B1272C4F4E1692ED5D8054D48FCD69F91D42D6CAD90B654C3C1CB875648FD7EE569A7C313B4C4204(
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\AutoIt3\Au3Check.exe

Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	238776
Entropy (8bit):	6.1887826628129705
Encrypted:	false
SSDEEP:	3072:wBynOpL12riocLMopTjGuX7GVdw3ELPU5+WYPwmsDx5T4XT3CAOA3GeilfrV5EAf:wBlL/cotjGFPy8wjNADHrLEoznVz
MD5:	05D3CEBDA15E24BC0B4F1EFFFE2A5A04
SHA1:	BD046BC45E5B6BB4B23A2D5AC99561CEB68143C8
SHA-256:	1C1327CFF2D2F3655B0578D2020FB381EAEAD2F61CF5273DC5F7DFFF46C218D7
SHA-512:	33AB27340B871C28AB5A97B36AA0D880EABA59734531E18FB797AB7EEA46617C7E3CB5521414D348DB3E89D279930906543A696F4F6B718FB538009035C29445
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\AutoIt3\Au3Info.exe

Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	197808
Entropy (8bit):	6.533706563724328
Encrypted:	false
SSDEEP:	3072:wBynOpL12riocLMsv5cyOZyW6RRWy4ZNC6ZraL3mU3FR5StHe+:wBlL/ca5tbXWBZw6ZraL3mh
MD5:	DA36C342B40B72BA496452E0E0A56131
SHA1:	3DECD6D77BCE749589DC72B1FB37F8A3E4095287
SHA-256:	19039615577179 38E245E246C04DF71C76404BA6EFD402ED3DA9F3966F1E8E3F
SHA-512:	DC28F81DCE1BA6E1428DEB1E87A44E1C8D8F1F25ED6A54D79EA3A9D625C8BCE57A994CDFC487FC7D8D0C92C1586320811E11C2BA53990A73254C19D69288E02
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\AutoIt3\Au3Info_x64.exe	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	217776
Entropy (8bit):	6.291538634392018
Encrypted:	false
SSDEEP:	3072:wBynOpL12riocLMUHThgfQMdmFDCwpcGr/yryIdXRWy4ZNC94QO9UKRGRLK:wBlL/c6TOfZdmFDNS2aOpBZw9xKaK
MD5:	CE7B6BCDC093A888731ADB41D115447F
SHA1:	BD572E572E009BF73DAF318E3C8D29F2F41FE006
SHA-256:	4ABE72249B6B1B8B499F84FFED601CC1585BF94AFC0B16148BF2BE9E7A14DFBC
SHA-512:	934C05703A908D54D08267F0FD47A456F27B7F08048CE6603BE07940FC1BB4A9DFB8735D4CDC345D2B2C2D21BC3AA385AF491D79451418CC94C5CD63CD0756
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\AutoIt3\Aut2Exe\Aut2exe.exe	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	1377456
Entropy (8bit):	7.492868238184331
Encrypted:	false
SSDEEP:	24576:JE0RJ529+RipvL1SXk1QE1RGOTnIEQc4au9NgxnHNnGw:n89+ApwXk1QE1RzsEQPaxHNGw
MD5:	4DE72D2F0A0D597597B1A8D1F3CE6C3E
SHA1:	2D3C1E8FF2B7C7B1587284F6F096071F0D4227C8
SHA-256:	1F512963A54F5CA9C0EF49038D062A43C94A4ECA394AF284FD4DB402D44D7B95
SHA-512:	D62549DC73A3451DE20090C4126CF6BE515F2DBFF9D1FB45507741A90FC8FD10AB86D8D16427C7D16DBDC77FF344A00422658892FC819F09252B2BD3DCEF8B
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\AutoIt3\Aut2Exe\Aut2exe_x64.exe	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	1418416
Entropy (8bit):	7.424772399744647
Encrypted:	false
SSDEEP:	24576:JdBCnx+QJ529+RipvL1SXk1QE1RGOTnIEQc4au9NgxnHNn6uioL:Puxw9+ApwXk1QE1RzsEQPaxHNks
MD5:	8A7288AF801A9D99C9CE20EAB9361A6F
SHA1:	1116258DF700E4535699F998DB62588950FB363D
SHA-256:	29857739AD250D03750F4169A6001291A05444D874C1CBE64552998ED0C1B634
SHA-512:	21C13CA059E1CC0BB23D4C2D6D6B8997191E5AB862640A47D5E223C679ABAAEAD965C43472D3144E088B4DCB8C6B31A1EFA258A8999E0DDC684BF3CE96312 15
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\AutoIt3\Aut2Exe\upx.exe	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	346624

C:\Program Files (x86)\AutoIt3\Aut2Exe\upx.exe	
Entropy (8bit):	7.902716465649219
Encrypted:	false
SSDEEP:	6144:wBlL/c5pXDXz7yIrozs0WuNd3ojusBdgnNW6r4F53ttuGENGFdVCLEYnPO1D7YYG:Ce59zGImAjJdcH4j3ttzFdVCLNSfHoSo
MD5:	F1955701FE1361E04511A6624621A243
SHA1:	91521F0C6F094750A5B730539A9BD11739E0338C
SHA-256:	04923EA0DAF2194FD29FBD9B0B55445FE64AA0DF5F860AAFA1E720DBAD5C1DBD
SHA-512:	5E08EADB224DABA81A3E9FE5B51E28264D5B975FA6A3B81C7672CF074A7F49BB82A1AF789D5DD5AF4F4D253ACD063C6C8F262F09822988B2EA77B86955373DA 0
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\AutoIt3\AutoIt3Help.exe	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	160424
Entropy (8bit):	6.117163517849118
Encrypted:	false
SSDEEP:	3072:wBynOpL12riocLMMO0L5hQCbIJqC3CJyoDjyYB78UAwBvm5:wBlL/c4gLk1B7XBv8
MD5:	BD5A7188F3BF4192AD91044564F9B593
SHA1:	5FA4ADA0F46D222C648D40449345989F68CCB147
SHA-256:	20CFE75E69B4F655C60774F30480AFBDB8B16F562D8E21C4F4FB73592B7D9ED9
SHA-512:	02AC68019A6573D3B704A8563510B6AB10B5FA73918A9AECC6F2BB60D486238BE7E26D700130839A857C4EFE65888A67184970BF4AE4EBFFCDF6890B9002733E
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\AutoIt3\AutoIt3_x64.exe	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	1055400
Entropy (8bit):	6.426924376896415
Encrypted:	false
SSDEEP:	24576:JdmUFhNcmLFj4svqaShRsUiTfjo5ya8j8s8:1Gmxj4svqaShRibza8h8
MD5:	691624FA0DDA3D1C0B0F1FC113351ED5
SHA1:	78D3C6BD16540A755562565F979324387C05B12A
SHA-256:	5F5A8EB38F6F58B8879337CC27CBA687F0B1F69A4FC0A7D31655CA4FE150849E
SHA-512:	3C88EEF582983671866CA016A0CF99946BAAFD1D74E5FB7E73FE6F92380867E35EC2067736FBECCA87E1F5124622D3619F2BA0DA34D1F92A3ACB291889656DD
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\AutoIt3\SciTE\SciTE.exe	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	1298432
Entropy (8bit):	6.689458357800496
Encrypted:	false
SSDEEP:	24576:J7N7dtrjrICw9XuXo7beSTdt5xbX02uvfTXfBxrj3d5E/jKQvVj4YpdjYY0td7kk:VbtnrICSooGSTD5xbX022fjBxrj3MA
MD5:	8240CF2E98F923365186FB30BC8DA068

C:\Program Files (x86)\AutoIt3\SciTE\SciTE.exe	
SHA1:	ADA4ABE3E563BAEB305A2B57F2D3973248406B4C
SHA-256:	FBF4A77FE67BA705DDE90E60A06C2F38D5373FA765F8B3FD0EDCD89D553C6029
SHA-512:	3A80C111199A1AD2EA3DAB57C90D787829AA4C9305EBC0C05305B27B41B81AAEC2376D9A03150C92881E2CEA65098B93B5BA787635EE5536A8442DEFE4EE2F 5
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\AutoIt3\Uninstall.exe	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	108903
Entropy (8bit):	6.778964277857251
Encrypted:	false
SSDEEP:	3072:wBynOpL12riocLMpCrvI11VDDvBPA6jXFN2MceCry:wBlL/cpCrvI11VHBhjmGCr
MD5:	B8F60D4E29DD52C7E024034D85A982AF
SHA1:	8C4F91A0BF030AC842D5E9B60E1DEA57CA6ACC78
SHA-256:	6743AF6DB39A173FC457ACDEC110CD1B8ADB053B700CFD065C6C29C684677D42
SHA-512:	610947ED2A035FD9EFEDE000763168D00B8DC91822C66F69B0BE6F182E06EDE397FB593206038169B790C9B34786ED5ECD819BCE35C3EB101954B828F0C5980
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARM.exe	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	1237016
Entropy (8bit):	5.885271461715482
Encrypted:	false
SSDEEP:	12288:Ce/AREu+r8w3JeKAIke98GpiclVccIp4b9QS5sB+Dn5nV6iUOswKNIYEe7:J/AN08wgFwIp4JsB+D5nVYO5KNIYEe7
MD5:	E4538DF3EB75EE88C213499FBADA511B
SHA1:	8272CD8811DC32D209E672E9F57A43BAA67CD612
SHA-256:	3EBA061A4A7F4CAC3BEA3FF60E361AFB0AD712512CB5FEBC045A367ACA943067
SHA-512:	1A8441C6A299668D6AEB721BAEA805CBD1969430F6F7E17D518ADA335E83C8B32211B77BB09B30FAC93A41B3CC70EC42BE183EDABD44F4CC7CDCA815BEAA F13
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARMHelper.exe	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	464936
Entropy (8bit):	6.3700138958936705
Encrypted:	false
SSDEEP:	6144:wBlL/cQQcslnC3znG+xfbMgyGn7LiJdKkAtyKuskePvX2Zp7DmuXYvr6ys/pJYCf:CeLlnCxjMyn72/KkAtydem3nM6BHYo
MD5:	68EEF6F4C9180056AC1B7F7B2BB3D6E9
SHA1:	4026B47480DC6A5256512F08C2E93A0D08C8D786
SHA-256:	7E8E0440C1E46147F90768CBB570B81AFA8C22F75072B2545877CC3660D90896
SHA-512:	575502D7C421123ACF6006A84184941BEA9C0561C02B14C0CD72E195215786DEEB055DC3F7C067E4B22E717645C7737B7A8F5D0E08019C57265E5B74F6C7ADD
Malicious:	**true**

C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\AdobeARMHelper.exe

Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Common Files\Adobe\ARM\1.0\armsvc.exe

Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	125456
Entropy (8bit):	6.277041146471536
Encrypted:	false
SSDEEP:	3072:wBynOpL12riocLMXkOAsu3v44dOyEv/mxmLO:wBlL/cXkOAsWlOyEv+xgO
MD5:	4A0A3799B177714558006F31B830639F
SHA1:	555AF82240172C38833C8A3DA0CA5A82CB5457C5
SHA-256:	5E1054E67086C7287814F4F0A4F78EE7E485327D3FAD9C33383B2C82F64C7236
SHA-512:	FD57395BAC2FA3E865ED336A68C5C894051B7FD71715546D814323C6E9F59958ABC6476FE5299CC9015E79814B93F9397CEA1773BDFAB7A97338A01D8E4F05A8
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Common Files\Java\Java Update\jaureg.exe

Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	472912
Entropy (8bit):	6.565531440533044
Encrypted:	false
SSDEEP:	12288:CeknFwHDxPuHqaTWl/jFucTsoY7BN3Hti0jKWo:JknFwHGilLFucTO7BN3H00jKWo
MD5:	6ABF927E0EF4BF7CBDC4AA4FC5EEB9BC
SHA1:	91022240F83984F30F52F252723AEA2B3BD25127
SHA-256:	BCE0B14E23597B74AA86FF63DB35A99FF82956536689562158A55C311D2E2B6C
SHA-512:	26022FBFFC6FB50F3C4189E7D91CAB558519305F3DE62CCEC58F9E6EB7094BCD3BA259B8A3F3C0755D922E8916CBFE782F89AD833EC54455118B195E82430C0
Malicious:	**true**
Antivirus:	• Antivirus: Joe Sandbox ML, Detection: 100%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Common Files\Java\Java Update\jucheck.exe

Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	1001296
Entropy (8bit):	6.466396308560745
Encrypted:	false
SSDEEP:	24576:Jf5UFBBhPT+1Gl+B66TmUC5bx0HnBJlxCN:srhQwW5Ts5KJAg
MD5:	D16F5DBAAB1C7121D1CFDFA553B21FAF
SHA1:	FA2F128E27041EF7C01EE70901190048D3D7DBC5
SHA-256:	35B3220582E9889B244CC867BA5DFE07CAA218CF45BF593C3278512339FE5ECC
SHA-512:	9FB6CCCC56AA0FB1A70169C44319E4ABFE7EFC76C9123B571A5CC5C9C047B119AB2993CCD3466F8A75BCFDCC7F0DADEC9B515EA9C3060C8BAC2D476F85C9 B03F
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Common Files\Java\Java Update\jusched.exe	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	686928
Entropy (8bit):	6.66028524430101
Encrypted:	false
SSDEEP:	12288:Ce+xy7dFtEB12w2w6Ahk7Re42UZuy/XlLTsiW0h73OZ+PY7wGPXiCR1bC:JJ7ftE2y6HFX2UAy/XlLTHW0YwPYEGPA
MD5:	E8FCC4B0F22DF7442D72271EE2DA5BAB
SHA1:	22D1A49D5B893EA4EB3EC96D1506B32A83C685F7
SHA-256:	73B8D3825EED9FDE4EE070BBBB2064D436BAAA5DFC996A36F93656C53371F816
SHA-512:	B76053E357C8637BE99BDCFD9AD42C45F395490728EDCD22890C8E2BED7798B96958D1E6E8BB9697E35FB3F795058307F0057D956521850C55DB1EFAC9F191A
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\java.exe	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	233848
Entropy (8bit):	6.766272457047718
Encrypted:	false
SSDEEP:	6144:wBlL/cKFezdlg8S7watoTB2vi9jspTq6Ndsb:CeKFKdlg8CltoTEvilA26Ndsb
MD5:	05DF2D55AC603E38FC6B608EF4902912
SHA1:	00CAAD4F13C39FC6A3C2B57B58088C223CD00D12
SHA-256:	5FE70FA6C95025D3C4CA4DF693566EF97719B47C6C8318F1955857406901BA54
SHA-512:	CE0A0B45274EC5CF3F319662E55D52A6A437E8327295044B3E9BCFF825233609FF993A74CAAAEE3157F69085DF5116EF2E65C862CF98B3A15AAE8DC8CDD9619
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\javaw.exe	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	233848
Entropy (8bit):	6.769964584046299
Encrypted:	false
SSDEEP:	6144:wBlL/cK1CYwUJzdXnSpU4TBdvD2QS0eg6Zs2:CeK1CvgzdXSpU4TTvDMtg6Zs2
MD5:	D15C38FC787A8B479625A01CD5F1F75D
SHA1:	1F2624DCF95F11FAAFD63EC3B6FF06AABF29DCB5
SHA-256:	011FEBFE9D5C398BAA181D2B354495909F4BA7C2D9034B7463E130000BF0FF43
SHA-512:	99B25D28ED01F3DAB6A20989061EB914EDFF1D560D4E61451CBAA4668C403D7E8C5265D0801A40881B346071816BCF9C54EF20F2FF61A74F04A6E72F92AB49C
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\javaws.exe	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	341880
Entropy (8bit):	6.504467281312065
Encrypted:	false
SSDEEP:	6144:wBlL/cKjedYNAMeo/0/3/A//FE/FzdXoktv/Pu29mYx:CeKSmNAMeo/0/OtE/F1tvtFx
MD5:	3117EF5DB01E0D4BCCB060B8F81F1020

C:\Program Files (x86)\Common Files\Oracle\Java\javapath_target_885250\javaws.exe	
SHA1:	61742FBF27CB1495ECEF3B4B8BDA249C4F43F878
SHA-256:	2098352D68C7A603E7055FED10A7EA5EA0D92A51DA5FB525626F9817AD2C6DF4
SHA-512:	9F524AA1D00A7B3469607F39B2B49F47FEBD79D878E3FC2C2060889E0F48C11F324966F7436A518CA8BFDF75EDDDEBB275BE301F2AEC576E0F3535BFECD2100 2
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Common Files\microsoft shared\DW\DW20.EXE	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	2628816
Entropy (8bit):	2.67973572383052
Encrypted:	false
SSDEEP:	12288:CemQ9siEt5LODS6RcvRtd+sGum6QHArfePms//bV5cOXPMiCSmRZQkEKFF:J79A5LODZWvT4sGz6QHVN3bcOhfmRqkf
MD5:	5827AA57AAE4CC896E1D41EBD5AE2A38
SHA1:	AEFD33772E2953DEE7D875A1AD3C2C040225A977
SHA-256:	6E2AB18DDDC81AD78BEA6FDD96E7F63EA96FB24FB068AA04354963B879CB204B
SHA-512:	7123C7D208F0DAA94FF687F6D7E3D3ECBA2E078AA552AB0E873B9D6621508585297313EAD1209A42B5B2227B125A6C669C35F7BE05C826C91F0A6842065E57C4
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Common Files\microsoft shared\DW\DWTRIG20.EXE	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	225512
Entropy (8bit):	6.424610914953199
Encrypted:	false
SSDEEP:	3072:wBynOpL12riocLMTgYp/OAWLTIKE4Vw2v6HXPoYvtT1mxho19K/rEs59s6i/XtXW:wBlL/cTgYp2ARNQYm+1WllgXtj+eC
MD5:	F90FCEFEEEC3A7CA7780BA4CE9E79D09
SHA1:	58369FAEA87B3F5FFFBCC4DF83963487ECFD2FCB
SHA-256:	B977E6DBD938B3422AF9D1A09A3B66EC52E579DB268703FF8B115BD2555BA7EF
SHA-512:	6635352846750DA646AC96B01E45FA026CFD41805718E1F32D00EA5DEDAC000AF0C332BE5E3B94E2DB939EA74B07C8ED4F223803B37F9ED0D95011EAB998C12 7
Malicious:	**true**
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\Program Files (x86)\Common Files\microsoft shared\DW\DWTRIG20.EXE, Author: Florian Roth
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\CMigrate.exe	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	5434136
Entropy (8bit):	6.307121354984186
Encrypted:	false
SSDEEP:	98304:5d4rAkEDQUKrXhluiA7i/9kl0DQW/dq9s2/v5OC5Ca/oz6g1PbxL:Jkz/Z/9k6DQW/dq9syBB8L
MD5:	4362638ACA0311A8DC09C524CDD778B7
SHA1:	A9CBE6C5513EC6F2EF41A08E0E148D501B03FB46
SHA-256:	CBB91C971D7AC5857E4312682AA11864F3D85E88D46FB4D238976AD6FC338F7C
SHA-512:	3C9CB15C97ACCBBBD2DB4C33498835D25BC94866BB152238B3AEC9EA2F7C629F1C3FE32E24C3DA153C07A1B9CA1A8095F258EFB0AD424B329D0FC331D380D E1C
Malicious:	**true**

C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\CMigrate.exe

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\CSISYNCCLIENT.EXE

Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	148832
Entropy (8bit):	6.425276495234216
Encrypted:	false
SSDEEP:	3072:wBynOpL12riocLMkrGOTPVJb+dW0wnbP1EfEDVYpqeyDY:wBlL/clFdW0wbcEDm/yM
MD5:	5D8C49F8E7BCB3DEB56E3E2844A8EF78
SHA1:	73C79054FA1BA08C1027068FA81053C0116E7C30
SHA-256:	ADBEE66A24DB50C35EB1FAD323EAA713FBAEB24BAF5C5F8F558225F6499E6870
SHA-512:	8228B6C34BC907A5F1791DC292B905E04685DE6AAC648050672743E4ADE624448ECE45FEDF182F767EAEE1A077DAD593A3B97814C9274C47F012144457F38122
Malicious:	**true**
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\CSISYNCCLIENT.EXE, Author: Florian Roth
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\FLTLDR.EXE

Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	325808
Entropy (8bit):	5.529553175087222
Encrypted:	false
SSDEEP:	6144:wBlL/cjLqmJHCJMgenwBOPhloudkpkSuULGD5NlKrGS2g1aQ1p:CeCmJHCJMgf0PhPdkCzU6D3ZSh0Q1p
MD5:	5F5363038981A861BDFBAB3FF300B419
SHA1:	696B4ADC35097B0DFCF6C95889190DFFAD242ED5
SHA-256:	9391F86055856C011E8EE0CC9E46EC8DDF366224E5F303E9FFBB2FC127897AB5
SHA-512:	CCF529BA31E8936D9ED935FB3AC5B65FB16C39F3E661AE24827504F7B6E10DF0A5406F84235BF1A0E0F32EFC8CC6F1C4B411C07A5785E30103D98C027E9AD5(
Malicious:	**true**
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\FLTLDR.EXE, Author: Florian Roth
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\LICLUA.EXE

Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	366288
Entropy (8bit):	6.486311134626888
Encrypted:	false
SSDEEP:	6144:wBlL/cJV7oJKtEsCZQ9BMHmD1tYFLqY/W5R02qO7VKCy7KIxanso:CeAotEsCa9+aYFLq3ny7KYo
MD5:	00A6C2E93DC43C69B48CD34D6BA85F9B
SHA1:	78604060D19E716E6CC413FC24F891B9AE03295F
SHA-256:	3ADD7EBB86B2EFBF25B503584F9416C9EACDB26C5D5B2FF72A8D3D040F297821
SHA-512:	D9C391190BEE546EA01D48FFC7FA8A80004B24AFC76BC3CAB0B044E1F862A2EB8872C590AC53614D933CF27F2B7577C0C84AE82D0B511DBB59C380ACAD2083 33
Malicious:	**true**
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\LICLUA.EXE, Author: Florian Roth

C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\LICLUA.EXE	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\MSOICONS.EXE	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	657064
Entropy (8bit):	3.6247362480627197
Encrypted:	false
SSDEEP:	1536:wBWx2gmwLOuYL12EawcKocLMMMJaCAd1uhNRN04gi0o0AdA/AZQJSShpuL4Y4Ykv:wBynOpL12riocLMNd04gi0ouuL4Ytkv
MD5:	BC3290DE4694ACF736DECAF4167CEEAF
SHA1:	A78EC9B7AB5AD248DC7BFE4D218C3D5556B5E239
SHA-256:	0B0DFEEAE88F5A51268A145A413D2F8F5F9A84281C418DBA8AA83273886AB005
SHA-512:	BD6F04E37A9FAAD55C66EB0DC720E232547C2550C6676501511F098A61D45142380B55852B28C6AA3C4A219D942890D535B530E39A0FEE91210A7C86EBC795B9
Malicious:	**true**
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\MSOICONS.EXE, Author: Florian Roth
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\MSOSQM.EXE	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	222904
Entropy (8bit):	3.4737180301620825
Encrypted:	false
SSDEEP:	1536:wBWx2gmwLOuYL12EawcKocLMMMK1uhNROY+WxQ0lEJRaCA:wBynOpL12riocLMqvWtl
MD5:	547B7B1296126891F8FEAC244486B8D7
SHA1:	5C954FE0582D115D52489433ECFD6C38A90FE2DD
SHA-256:	6B2F5E06A2311591DBE57E42B0A13DC88B6BB2291B0ED0B9E359948A4F0FA98D
SHA-512:	3D4164E5EBF35BB86E25FB82C46734E6B7D9505EB3040509BD31C32CE782A587D9527C9A83F30C39A864D40F220E38E7912DC77678BC4EE66D866FB1E489B10
Malicious:	**true**
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\MSOSQM.EXE, Author: Florian Roth
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\MSOXMLED.EXE	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	262344
Entropy (8bit):	4.11486176733499
Encrypted:	false
SSDEEP:	3072:wBynOpL12riocLM6k9v/0xrsRQIouwjQlL:wBlL/cT0xrwQEwElL
MD5:	9909088BC7794C5607F08D97E8535BB9
SHA1:	37723D214FBB74B3D5F168427AA3E0D8A2696EFD
SHA-256:	0DAF72751BDB2F35B11DBB6B63F16FE28940413371E9200FA02862EBEA10C851
SHA-512:	F247D6701B7B278AF02B5E500546D871D4E3F3B2C2A5B34179D9A8170D579DD4D812294149DA9CBC1CBBFFC677625A51C9CD1D27B2ABEB228DC48747490196E
Malicious:	**true**
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\MSOXMLED.EXE, Author: Florian Roth

C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\MSOXMLED.EXE	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\OLicenseHeartbeat.exe	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	166104
Entropy (8bit):	6.263491972778485
Encrypted:	false
SSDEEP:	3072:wBynOpL12riocLM7enbUaOU1IcODjnhyAf98rN7btBAxm2Z/ps/rz:wBlL/c4IUjEwEGDAxm2Z/m/rz
MD5:	5FF9D14ECBEDFAAE12CC2218A702399F
SHA1:	77C5D60870049E606AFDF69AFC15E92412CD4A43
SHA-256:	C5498A4BE7E9267CDCD34895324423E155DCA90A06A9335221E7A2C699B74FDF
SHA-512:	DFB30AB131B1E8E1A19CBFE158F93DF982239DA90BD4FC007C98992A2B359AD84528088F9521D71F3CA20AB6B7703E138E211BF865B49339609F4950A0A4D08E
Malicious:	**true**
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\OLicenseHeartbeat.exe, Author: Florian Roth
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Oarpmany.exe	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	244944
Entropy (8bit):	6.525799409007694
Encrypted:	false
SSDEEP:	6144:wBlL/cCqkGhCM1fqOPHkN/ylyU2mPUOFL:CeCpeCQfqO/3lyUUOFL
MD5:	63EFC01A99731DB0D4B79903979BEC98
SHA1:	492BAF544470A8A5061AC5A3A8F68FC89B4DADD8
SHA-256:	BF0C0CF4893B274E63AC0870F2A77D00411C91E072E56BD61FE11D7559C17CB1
SHA-512:	26287D21D17772352BE817BDB2890B8D4699D2FF8D32C4E2D209FB75DCFBE3E5A305741C35EE35B98AC7C0873752120F879129FBEF20411EE9A88E4BAC38A86
Malicious:	**true**
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Oarpmany.exe, Author: Florian Roth
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Office Setup Controller\ODeploy.exe	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	589976
Entropy (8bit):	5.338574563221662
Encrypted:	false
SSDEEP:	6144:wBlL/cu4aeA+WEnGH1NCmWR5FJYUJupxFdYqIVz:Ce2eLWEnONCmC5Vuzrb6z
MD5:	83D288D30C40F60E87D9F13EA7B67863
SHA1:	394B38D31FE2930B7E763194A34D81A7DEB4689F
SHA-256:	8E38B89CC658022C81F41F6B331264F0DEADBCFCA9103DEBAA974FC710968D61
SHA-512:	A6BBBF794C4879BCBFCC1945D9BD49985B306501BC77E976424CA15C74CD864951EFDA9117CA09666D64ADAF0F43A544AC9F6E5E5ADE0CC7FF8BF2A96CDD1 E25
Malicious:	**true**
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Office Setup Controller\ODeploy.exe, Author: Florian Roth

C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Office Setup Controller\ODeploy.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Office Setup Controller\Setup.exe	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	673304
Entropy (8bit):	5.4440570320090265
Encrypted:	false
SSDEEP:	6144:wBlL/cHua5qijR4ZTvC7yPA1ikaY1xA1VurX6hOI0MjEVQTzfKfle6IZuy7:CeHvqijR4g7h1ikByX/OVE8fle6IZuy7
MD5:	A59165A5DFBB26FA33B2D712C9269A67
SHA1:	3D73ACE16C8AD95E6517379F7B44E7A78642DE5C
SHA-256:	C7B2A5D8689ED64B41388C0A3DE94CC9A9D9B8FE5D1475BF93EFDDD8CC45843E
SHA-512:	F8E269C1F17991A65B93C6FD13DFA0BC22C043CD9A6116A1639D4C0A8039004C383DA9F9B6825B1CD0ED23E5D2250F4765C0D4ACD25F3436A7B1C66032EA58
Malicious:	**true**
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\Program Files (x86)\Common Files\microsoft shared\OFFICE16\Office Setup Controller\Setup.exe, Author: Florian Roth
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Common Files\microsoft shared\Source Engine\OSE.EXE	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	255168
Entropy (8bit):	6.594902116447596
Encrypted:	false
SSDEEP:	3072:wBynOpL12riocLMXzcMqiGhz/fA96A9L45vxfq4qzqD27eIyUX3cM74E5S4uNUxJ:wBlL/cXctXc9L4PCqCz10/Dz1RXMTD
MD5:	F3074AA37FD2F7456515DF9D237F30CC
SHA1:	A1053F5BF43DDBAB52D08C3AFDEA53B8AB26DF99
SHA-256:	1E473C6A8FFC9D2E47442F3872CCA035DC88B9B387F6F8707D11ABCB59B4BE23
SHA-512:	978CE7C3C3F05B62D2897BBE98D9E54FBF283098CD7D9406A0512629F95BA1D13D25C918646CE95144AB1D33BF514FF06DA40597A1F92EE43720AA7E0F846A9
Malicious:	**true**
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\Program Files (x86)\Common Files\microsoft shared\Source Engine\OSE.EXE, Author: Florian Roth
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Common Files\microsoft shared\VSTO\10.0\VSTOInstaller.exe	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	124136
Entropy (8bit):	6.311989636446886
Encrypted:	false
SSDEEP:	3072:wBynOpL12riocLM1Po10JOSdBlrbr1Pg9uCRFRzsxeZ:wBlL/c1g1MOcxPmRFJs0Z
MD5:	32948EAE3C3D22239C05FA5A5C4A360E
SHA1:	4B12C420744E19D88C5EFBFF1597BE38209E7A97
SHA-256:	DD6EBF6178AA7B88068E29F2EF9AC53EA227A0C3F11DC7122ED8ADBBC377163C
SHA-512:	33AB9DEC6103CE85A6D52A62E93E95B3920F16FA51F60335C44ABA23EFB448015187A68B7786C7697E8791CF8B1508C23E406B5BF3A6B115B463E107834E5B38
Malicious:	**true**
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\Program Files (x86)\Common Files\microsoft shared\VSTO\10.0\VSTOInstaller.exe, Author: Florian Roth

C:\Program Files (x86)\Common Files\microsoft shared\VSTO\10.0\VSTOInstaller.exe

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Google\Update\1.3.35.452\GoogleCrashHandler.exe

Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	336840
Entropy (8bit):	6.630971803333895
Encrypted:	false
SSDEEP:	6144:wBlL/cnVk51IBGg39VOmArrPD/B7XAOI2Srxjcx+aKfxboNQ:CenVjBGgNVOmadr62SrGx+aKfxEW
MD5:	A8B0EF7F4206054D36E3959DA171D7A2
SHA1:	77CEDD80B16D9535F9336E16EE8148BEB1BFBBB4
SHA-256:	C72ACB419088FEAE3A115968C7512954E411BC7A54EDC74729ECA49795B378AE
SHA-512:	AE8A75B79C4E1BB32C2C19D9EB3B6313A0B8479B2D748B45B52E69810E8E4CC54743FFA355E471934F0E140E0B52800B4692483573755B5F14C33D32772ED951
Malicious:	**true**
Yara Hits:	• Rule: SUSP_Unsigned_GoogleUpdate, Description: Detects suspicious unsigned GoogleUpdate.exe, Source: C:\Program Files (x86)\Google\Update\1.3.35.452\GoogleCrashHandler.exe, Author: Florian Roth
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Google\Update\1.3.35.452\GoogleCrashHandler64.exe

Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	417736
Entropy (8bit):	6.376129758952312
Encrypted:	false
SSDEEP:	6144:wBlL/cPnGs2VohB+saEY5o6JrrbVT/aj3oh55rrxTMx++FxSA:CePlrq5/Ba7o35rr+x++SA
MD5:	3775B7F3B4769CAE077F923D21A74ECF
SHA1:	ED1D77B52A1E08640C6E2E3125A603B522FF6E62
SHA-256:	5C97823F332E080726A093137031F7F27BF50928DD52D22B1C56B14F4B629F3F
SHA-512:	B2287A04F5C744EDB8A8403AD52A2CAD6AC45682C2754E6A775F03892F75B4309456080CC30D13FD995D2F702C236BC9F7E4B9700AD5C97DFCE4B21B9291576
Malicious:	**true**
Yara Hits:	• Rule: SUSP_Unsigned_GoogleUpdate, Description: Detects suspicious unsigned GoogleUpdate.exe, Source: C:\Program Files (x86)\Google\Update\1.3.35.452\GoogleCrashHandler64.exe, Author: Florian Roth
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Google\Update\1.3.35.452\GoogleUpdate.exe

Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	197576
Entropy (8bit):	6.106227732514612
Encrypted:	false
SSDEEP:	3072:wBynOpL12riocLMuiTOZQvfSERdX9Zk8AtB+llojrWTMK12XdjWtVAlR8yVciqFR:wBlL/cPjRsB+FqAx9
MD5:	2B2464E393BEA279C25D305DBDE8447C
SHA1:	F26D7825E8C397C94C6B5028A46618868532A395
SHA-256:	7DBBF90B4C227BCB35E3377CAD664C640ABF85FA68DFDA9676054F700CA59C20
SHA-512:	3D5A5075CB1693F29BDB2CAEFC5DBCD884C99394C447B51E3AD79618A840C820A3AC405D812CA3AA4FAFB03AAA670E223E1AB1A23EFAC735EB5D279FDE4A2 0E1
Malicious:	**true**
Yara Hits:	• Rule: SUSP_Unsigned_GoogleUpdate, Description: Detects suspicious unsigned GoogleUpdate.exe, Source: C:\Program Files (x86)\Google\Update\1.3.35.452\GoogleUpdate.exe, Author: Florian Roth

C:\Program Files (x86)\Google\Update\1.3.35.452\GoogleUpdate.exe

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Google\Update\1.3.35.452\GoogleUpdateBroker.exe

Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	142792
Entropy (8bit):	6.553026823319148
Encrypted:	false
SSDEEP:	3072:wBynOpL12riocLMViI73i6Q4s+B+e/NKMeCwgh2Bh1c27YX:wBlL/cguC+B+McMeJgM8
MD5:	11C50FF51B31B07F70783B05E72A1984
SHA1:	30AB2F449F319CAA16CE660141E682E59F85680D
SHA-256:	89FDBAD3C92F39FE8BBD8B9092920612A329EF8130259230D863AB9C583A570E
SHA-512:	CDC7CAAD6219D9C03B968CA25BA01C298E485DAC96C73E27FFB3E1FB73C5BF5D2C73987E44B8E216EE059D8B4DB98FAA3F8FEAF99C84784EC48220035DC886E
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Google\Update\1.3.35.452\GoogleUpdateComRegisterShell64.exe

Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	223176
Entropy (8bit):	6.2021563238465385
Encrypted:	false
SSDEEP:	3072:wBynOpL12riocLM9cbW1TJOH7gL7cLJ3wOCtllmoY46WxRh3QgqeCzbR52HdtSx:wBlL/c9cuTo8LmJ3wKoh5WneEbRwqx
MD5:	5177DD0EAFA6A8A87D29C06900E86F9E
SHA1:	03851367C03508EE947706C323C620EF5BB5D086
SHA-256:	0A6A2C441D717FCB7D529A8D9A60DAE219DCCF80B6F1B9C8F230C13D74A0ED8A
SHA-512:	9DFFA79B73B5218FFCA4FF164B0D3CE9C288658AD0E5DB0CEBC042FB4804DFF3049498F4EB741B4EF3F2BBFB3CC2647D38E29554EC3F59E1A78F80D15626BC8E
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Google\Update\1.3.35.452\GoogleUpdateCore.exe

Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	259016
Entropy (8bit):	6.638153869747898
Encrypted:	false
SSDEEP:	6144:wBlL/csACX2p6fGNgKAO0CFrf3x+aFSskWrf:CesA62A+xy4rvx+aFSOrf
MD5:	441517BD9E00EDB9FC1AD297349E4200
SHA1:	C7B0D75A2BE0085BC3894A05C9DDCE2A88F27737
SHA-256:	8C6D4C00BFF9C6637C818D4AC36D53D70E2CDCD63CD604E2CAA80F8269FC4135
SHA-512:	DADB1F3FEF08C96C64E0927DE68CE811B1B0322DA0E7BF98D42BA1E40C9D7A37D4C5DEC57CC085EC03501A71EE37C7083C58302BD4947BB5FF2035499A5AC4B
Malicious:	**true**
Yara Hits:	• Rule: SUSP_Unsigned_GoogleUpdate, Description: Detects suspicious unsigned GoogleUpdate.exe, Source: C:\Program Files (x86)\Google\Update\1.3.35.452\GoogleUpdateCore.exe, Author: Florian Roth
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Google\Update\1.3.35.452\GoogleUpdateOnDemand.exe	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	142792
Entropy (8bit):	6.5533001977978715
Encrypted:	false
SSDEEP:	3072:wBynOpL12riocLMmiI73i6Qas+B+e/SKMICm3sZmGkh182jYX:wBlL/cXu4+B+MRMIh3sMU
MD5:	92F4329EE6149199FFB119236E03DF64
SHA1:	77EAEDB40CDB94DA75470027D5ABD357855CA64C
SHA-256:	0BED2C34EFC980EC8DA9E82AB80E7B16D3F5304D2F77861EE24BA8E82F6F1BEA
SHA-512:	939F2201C709896A83FBCFB031B1F2D12991C828BC8C162C13A446FF8A1373B15674A33AFDAE3AB19042D0C83B5004745B010B508D581FD50FB64FE345418581
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... .....

C:\Program Files (x86)\Google\Update\1.3.35.452\GoogleUpdateSetup.exe	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	1337048
Entropy (8bit):	7.894489681319961
Encrypted:	false
SSDEEP:	24576:JhSWkfRyE2ZcFGUEGNBffACErtoFAocYj+uY64YF5AjXEx2Je7CVSszVrmWWH3:6WJE2ZctEafitmGYj+uYP4D2VPrX+
MD5:	B17E9F04D63C85748CC12B7D50624AB5
SHA1:	3BE2EC52EDE69E6BDA06D6A5BB35F4D92FE594C7
SHA-256:	DE75F90CB81A5CDFCFECE02D1AD114A143A77ED065D69EA23C93DAD5AFB66B1F
SHA-512:	F05E4A95D3E636803A97E57C334AA1A9F08C6C32AD3537F063C4C75BD9CDBB6D5F412D029338310015565E9799BA4125040750C366529D6A5B00368C310786A4
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... .....

C:\Program Files (x86)\Java\jre1.8.0_211\bin\java.exe	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	233848
Entropy (8bit):	6.766272457047718
Encrypted:	false
SSDEEP:	6144:wBlL/cKFezdlg8S7watoTB2vi9jspTq6Ndsb:CeKFKdlg8CltoTEvilA26Ndsb
MD5:	05DF2D55AC603E38FC6B608EF4902912
SHA1:	00CAAD4F13C39FC6A3C2B57B58088C223CD00D12
SHA-256:	5FE70FA6C95025D3C4CA4DF693566EF97719B47C6C8318F1955857406901BA54
SHA-512:	CE0A0B45274EC5CF3F319662E55D52A6A437E8327295044B3E9BCFF825233609FF993A74CAAAEE3157F69085DF5116EF2E65C862CF98B3A15AAE8DC8CDD9619
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... .....

C:\Program Files (x86)\Java\jre1.8.0_211\bin\javacpl.exe	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	116088
Entropy (8bit):	6.520463961257331
Encrypted:	false
SSDEEP:	3072:wBynOpL12riocLMKqJjZqMNdl2dE+bgOkIS:wBlL/cKevC2UgOkIS
MD5:	41EB2AE788C510F6448804DED8578ECB

C:\Program Files (x86)\Java\jre1.8.0_211\bin\javacpl.exe	
SHA1:	0AFCBFCD9D8F82916B53076D9D7985A9F995FCB4
SHA-256:	A7FDC700F5902528B6AC8E4836B67407D2319CC3411D27D0345449904C962AEA
SHA-512:	FD866990D0D3CA4563CE56B152BD76B7C06675003A7B12B00D3F50F869BFB22DC815B0891D45156BC4482B7512866F46C6DB62592C7A5C2CA972AFB9E88CB03
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Java\jre1.8.0_211\bin\javaw.exe	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	233848
Entropy (8bit):	6.769964584046299
Encrypted:	false
SSDEEP:	6144:wBlL/cK1CYwUJzdXnSpU4TBdvD2QS0eg6Zs2:CeK1CvgzdXSpU4TTvDMtg6Zs2
MD5:	D15C38FC787A8B479625A01CD5F1F75D
SHA1:	1F2624DCF95F11FAAFD63EC3B6FF06AABF29DCB5
SHA-256:	011FEBFE9D5C398BAA181D2B354495909F4BA7C2D9034B7463E130000BF0FF43
SHA-512:	99B25D28ED01F3DAB6A20989061EB914EDFF1D560D4E61451CBAA4668C403D7E8C5265D0801A40881B346071816BCF9C54EF20F2FF61A74F04A6E72F92AB49C
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Java\jre1.8.0_211\bin\javaws.exe	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	341880
Entropy (8bit):	6.504467281312065
Encrypted:	false
SSDEEP:	6144:wBlL/cKjedYNAMeo/0/3/A//FE/FzdXoktv/Pu29mYx:CeKSmNAMeo/0/OtE/F1tvtFx
MD5:	3117EF5DB01E0D4BCCB060B8F81F1020
SHA1:	61742FBF27CB1495ECEF3B4B8BDA249C4F43F878
SHA-256:	2098352D68C7A603E7055FED10A7EA5EA0D92A51DA5FB525626F9817AD2C6DF4
SHA-512:	9F524AA1D00A7B3469607F39B2B49F47FEBD79D878E3FC2C2060889E0F48C11F324966F7436A518CA8BFDF75EDDDEBB275BE301F2AEC576E0F3535BFECD2100 2
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Java\jre1.8.0_211\bin\jp2launcher.exe	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	134008
Entropy (8bit):	6.511209467176045
Encrypted:	false
SSDEEP:	3072:wBynOpL12riocLMkRJdaMTcOmFk2W5OX8e77hfFTkd33:wBlL/cidLcOlk24OX8knkn
MD5:	E57F4672C1CA856F61DF322058F99212
SHA1:	ECC98F4DA5105FB9A964679FBDBA9E03431B5F7D
SHA-256:	6BC63BE57E1B25463E9362E4A90AF05458268C1C3E819409C945DFEA5DC2B84F
SHA-512:	D20E1EB3E74E10AC41569439C8F32A806F6F7948835CA65B5BB88467859773DBE00ED7B5562DDC89F117FA9CEBF086C4CA86FADA72FB4F11D6EC57161EA94B 4
Malicious:	**true**

C:\Program Files (x86)\Java\jre1.8.0_211\bin\jp2launcher.exe

Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Java\jre1.8.0_211\bin\ssvagent.exe

Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	99192
Entropy (8bit):	6.3315720343891355
Encrypted:	false
SSDEEP:	3072:wBynOpL12riocLM6OxBZz2GREQQhanIZs8:wBlL/c6OxBLghMIG8
MD5:	6A20B6089460E4F25AB3786611B29A07
SHA1:	231840E0AD02745FDF1762830A0B2542FDF6EDB4
SHA-256:	DA604B58F5F569C434A8CA660B2BB53DA91D5C9AB4A251587D298C9554447CF6
SHA-512:	C530B0D3509A53BB7259976CF14F807327FECF81F1AF3293E337E22B2AE2C570C4D9B681D2F923B7F6A0E1F60122BE057F0FD0FB239C615A04539BEF34ABF49F
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Java\jre1.8.0_211\bin\unpack200.exe

Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	202616
Entropy (8bit):	6.139839372575465
Encrypted:	false
SSDEEP:	3072:wBynOpL12riocLMapI0EAWfL4JVDTBfveag9zQHvIIsSvO55PvV8HVwLZ8qU:wBlL/ca20tsL4jTBneag9zQHvCHVqZc
MD5:	1FD2C983B8BDA42ECD903CF100BD0182
SHA1:	E3103E01D0A8EBFCC687925A9292884B07F972D0
SHA-256:	BD874F379B0595F7D7C6C2637C3B7831C7263F1E30BF012C84A4C574A96737B9
SHA-512:	C1D645E7B8E790E3F014CA73A839EDD56F5ECC79F3F84C786B85EBE356EF3E1DD136A8141BF3C5EEB023A25DDAD08560DFD727B5D3E811F4B6BA026BE67DC 680
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Microsoft Analysis Services\AS OLEDB\110\SQLDumper.exe

Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	136880
Entropy (8bit):	6.10720634238147
Encrypted:	false
SSDEEP:	3072:wBynOpL12riocLMv3Bpj4+gLS8eUxkaenD9UR9whwtvTRMBy:wBlL/cv3Bpj4/E5RUNKBy
MD5:	C00001D4B7B68813ED44FCE9DC31A072
SHA1:	3791D3F2699071312D0FB96FADC02E1DF43579FD
SHA-256:	7652C69DA36E5B9EFD51F8E47D5C509DA7A17BCC780006ECA609010BF79ABEB0
SHA-512:	0C560EC78476A8E90C5994C4B80F9C4BFD0EEBA34B5E387E18773A166023804EF3ECC8A155772FC6F3FB0B7EC8498BFDCA8A60D464CB126030D612A886D3DB C
Malicious:	**true**
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\Program Files (x86)\Microsoft Analysis Services\AS OLEDB\110\SQLDumper.exe, Author: Florian Roth
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Microsoft Office\Office16\ACCICONS.EXE	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	3790504
Entropy (8bit):	3.576358466413868
Encrypted:	false
SSDEEP:	12288:Ce6l5td2vvvvvEvvvvvqb5Z6ziw812i4Qog6SerHqE7sLaMqkh:J65ty5Rw8Dog6RrKas
MD5:	B9E493385B4B548538A40C6F8D2B90B2
SHA1:	F623E0F7C1DDAAD8F19D2AAF96A5751C4A3E61F8
SHA-256:	45F53BFC386DCE0B41E4C1B065B9EBACE4129BF9ADDC9B58DA26C1F889DCB18A
SHA-512:	1ED81654B2D96B619F2C93E5C70CB775EA022C4BEEBFC5276E48184C750D94C733098A2E64383A6F16977DB578B921B4F90C551648F2093E515F706553A7D993
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... .....

C:\Program Files (x86)\Microsoft Office\Office16\AppSharingHookController.exe	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	92664
Entropy (8bit):	6.642754053898558
Encrypted:	false
SSDEEP:	1536:wBWx2gmwLOuYL12EawcKocLMMMPCbkMkBExFhpgLTGlrFBbeEOCr:wBynOpL12riocLM07uTGlr3iE5r
MD5:	5ED546E11813421D501D02D3ECBC0BB0
SHA1:	A041B247F44E7D7743FDF92521FA5135C8315CE9
SHA-256:	167D16FD8ABA643985E4DAF51A45F9A92FE9771B2D04066E281FA6E88B1A8A2C
SHA-512:	B16F60079E67CEE1DCB46828A1E884CC23A9CBFD11740488922E4D59D61D77B464A8ED611BFD7770E4B25A40BCC2C64DF8A5B669298BE7A2547A73F2EA1D46 1
Malicious:	**true**
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\Program Files (x86)\Microsoft Office\Office16\AppSharingHookController.exe, Author: Florian Roth
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... .....

C:\Program Files (x86)\Microsoft Office\Office16\CLVIEW.EXE	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	413888
Entropy (8bit):	6.023164608258184
Encrypted:	false
SSDEEP:	6144:wBlL/c5d8/cXscXt7E1S4yRSZxqZboxNJ6XeJh:Ce5d8/cXsS7OS4yuxqpUmeJh
MD5:	174D4E5397A4C26A9071CBBE3057581A
SHA1:	E93E4856329E7695C57C0545939437A20ADF4E0E
SHA-256:	3BCEF8E94663132B490E32B09C50F0671EFA2EF118D7AFC81C1CDEE112076969
SHA-512:	D3D13954E2A1D680EBB62858C2D9946F3F3B60F63A31EA31F7B18D60888337CBF16B223301D6CCEB1B1AD9239339D5F5350C7D24573E0F6118E49B7142DD7C2
Malicious:	**true**
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\Program Files (x86)\Microsoft Office\Office16\CLVIEW.EXE, Author: Florian Roth
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... .....

C:\Program Files (x86)\Microsoft Office\Office16\CNFNOT32.EXE	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	217896

C:\Program Files (x86)\Microsoft Office\Office16\CNFNOT32.EXE	
Entropy (8bit):	6.209852579384796
Encrypted:	false
SSDEEP:	3072:wBynOpL12riocLMCiPMhRRhO40LIs5L6YrGioAPKhjah2QE2SkXFKJMt:wBlL/cLGn0kE6OrfQs2xt8FKu
MD5:	D35448E287E2A73BB2C0ED453C7BDFC1
SHA1:	2BAE2B2424EC87AAD077D23D4DB45AF186417A6D
SHA-256:	24B2246B92F233F82FA5842B930E863E34308D359E117ADD8189207F0A1906C2
SHA-512:	0051FA74CD97F0C5FD79C1FDFFEB0C518DA64F50C589526F0084592AEFF865F6E05CE9D3B9604CD924F24C4F10A8AF450E1F0F3979D90011028BEAFA6861CBB
Malicious:	**true**
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\Program Files (x86)\Microsoft Office\Office16\CNFNOT32.EXE, Author: Florian Roth
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Microsoft Office\Office16\DCF\DATABASECOMPARE.EXE	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	226656
Entropy (8bit):	6.379622503793066
Encrypted:	false
SSDEEP:	3072:wBynOpL12riocLMBvMQ/58sNZ2OZ2Oe2T8sXF9xDr1BRo+SYZMuW32GhB:wBlL/cB0lsNhgs1f/1BRo+SYZMj2GhB
MD5:	331EFDCC18917A98AB0D29D70E0E8CA4
SHA1:	5C417C3AED83A28E998564A5494FFDFB8C884A86
SHA-256:	9C2BAEED987CA564031D89ED5ADEFB17F7B27B9C8DF5B0753C73D08029AB083D
SHA-512:	2FFD4F1F0C387145FE78D974A7A6FF8E67122E6DCA5D507233E99CFC3DFE8C0BAD0FE8E367D2D59086776A6D22494B64658268B7B7A09FE143B69C79A227090
Malicious:	**true**
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\Program Files (x86)\Microsoft Office\Office16\DCF\DATABASECOMPARE.EXE, Author: Florian Roth
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Microsoft Office\Office16\DCF\SPREADSHEETCOMPARE.EXE	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	496320
Entropy (8bit):	6.6642853206140975
Encrypted:	false
SSDEEP:	6144:wBlL/crDcmdCI6BHAlSpFG/+Ls3ze30xLs+bz0YTirzhafYyf7Pvm7M80yzyiL7k:CerDcmd/6JAB/6N30xQWhRvm7MIDnk
MD5:	50BC9A708BC719ECF048FA399FF5230E
SHA1:	699A7C52415A88CFFE8B7235769B2476B1136CE0
SHA-256:	7EBA8A070B0E1BD02B95A0EFBD31E5ADDADD24D2C7EF846AFFD5BF341ADA15F2
SHA-512:	F2DE5BCC41903FCB86B885A0E5C8572A6FBF829E033CCB55E917F1FACF946DA2C7FF051F81918456341BF4E88B0F988B6E51BB4F4888212720EFEA2EBC92874
Malicious:	**true**
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\Program Files (x86)\Microsoft Office\Office16\DCF\SPREADSHEETCOMPARE.EXE, Author: Florian Roth
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Microsoft Office\Office16\DCF\filecompare.exe	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	284864
Entropy (8bit):	6.443310999067898
Encrypted:	false
SSDEEP:	6144:wBlL/cmWQZIn91zska8o8dfu7hjBjobCUqJXGSOjKCkVWjlc:CeWE91zhTdfu7bU+DkKCkoy

C:\Program Files (x86)\Microsoft Office\Office16\DCF\filecompare.exe	
MD5:	381B2F843B8A8D6490D91891C235038D
SHA1:	69627BA229892D4AF7287347BDBC800C6D05D5EB
SHA-256:	5249956A8E7A74EAF898995D5A9D27431E892E559A269A8364C6BF0A29A9D2B2
SHA-512:	B90BD22BE6D9A39F5988F6012B1F6E5F39C5E77ABEBCC2FCEC640CD9FF6ED9524CAD2BF105DB9A138BF4CADC1F54B94057E88E9BD11E292FB5496FDD11922437
Malicious:	**true**
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\Program Files (x86)\Microsoft Office\Office16\DCF\filecompare.exe, Author: Florian Roth
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Microsoft Office\Office16\FIRSTRUN.EXE	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	813344
Entropy (8bit):	3.5985652169844893
Encrypted:	false
SSDEEP:	6144:wBlL/ce6zNf9laluQoSSBHSUdb5LpB8pN:Cee0laluXyyNLpBi
MD5:	935AB62C8E2DDDD577BBEC2DB7F52EFD
SHA1:	B511FD832964F21261177B2CFC00DCBB9384DCD3
SHA-256:	3E33B7C446944A9227E272CAC83E16646B5C166F3A1214BE72288AD50FFC1BAD
SHA-512:	825CB3C61DF3B8498A91932BB3A1E2BAC7A4A2599DE97760ED12E70FB24A3EAFBD14918D8D9B0A10F79574E73862A1D5588F02557A9223591BF99D641840E68E
Malicious:	**true**
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\Program Files (x86)\Microsoft Office\Office16\FIRSTRUN.EXE, Author: Florian Roth
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Microsoft Office\Office16\GRAPH.EXE	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	4461400
Entropy (8bit):	5.951369325265408
Encrypted:	false
SSDEEP:	98304:TphXvapxXCk1JgTN6Yidt0TGwdp7JJK4AjXYwK/nF+TXx:9hXvapxSk1STN6+JK7jXG/nkrx
MD5:	E6E8BF0D37790E4E6D62D6EA5DCB7289
SHA1:	8998EA6F2EDD5C5E20796A294422AF9CF2D96C21
SHA-256:	95A00B587ACB08B4737E75E0D86AEE77CD093A2E364ACCA813BADF406437DD2D
SHA-512:	E23BB12F85E6ADB22A7B94E83C9516F1746E27493307C67048D3A5402FE9979D4894DC86D17AB4949B6E3A0D7757E8E2EDAF36B31437C438B46915B7A1CB215A
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Microsoft Office\Office16\IEContentService.exe	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	244160
Entropy (8bit):	6.5314974728640385
Encrypted:	false
SSDEEP:	6144:wBlL/c3J4mjSBzUzdiR5CpmCYvwg76HStzaCd9i2:CeoqB85C0CYteH6aCbi2
MD5:	DFC20D168F4B6FED2B223767C870E1FC
SHA1:	850FEF11A3B04349AF9AAFC76876559356610C56
SHA-256:	35BC3E2D19141BFE3E858F9400D2CBBCDDD3642208D677414523A82E9210EB0E

C:\Program Files (x86)\Microsoft Office\Office16\IEContentService.exe	
SHA-512:	4608F005D079A8416AE0389F8BC0B0954689FC44A2CA9B57E89686DAEEDB7A76E722DA1BD66749811FED0719009BE3019DBEF0F096FD6D5193DA9FBE83A457D7
Malicious:	**true**
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\Program Files (x86)\Microsoft Office\Office16\IEContentService.exe, Author: Florian Roth
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....text....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Microsoft Office\Office16\MSOHTMED.EXE	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	118976
Entropy (8bit):	6.308692011288907
Encrypted:	false
SSDEEP:	3072:wBynOpL12riocLMsh3yJFn6dIvibTCaOFeubks:wBlL/cm6FpKHCpe+ks
MD5:	A79E52869A6B4F203886DCD7C0DAC3F4
SHA1:	0317A448222E7A48816667C9D17DF29E843A6BF3
SHA-256:	63CE249E3CC6A5FD7CA613802A41686ED2A62E7384FDB576BBE4E69696C252EC
SHA-512:	CEB9047C7FD0862ED6B888F5785071BFF441F6DDEED1099F0258B55F8D5492B711F1841741E8DEF28AA7610DDEBDDB85EDA2CF432FEEEF6CB676CD7F17F02ED7
Malicious:	**true**
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\Program Files (x86)\Microsoft Office\Office16\MSOHTMED.EXE, Author: Florian Roth
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....text....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Microsoft Office\Office16\MSOSREC.EXE	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	216264
Entropy (8bit):	6.324732882805217
Encrypted:	false
SSDEEP:	3072:wBynOpL12riocLMhk7EhKG9e5aSUTrWT6ALhWYURNwqMb7Heu8LSakmP:wBlL/cG4DqaSOALhW9n0bTeuWSaN
MD5:	60D4AA88F6E21624B65AD2363EE5E35E
SHA1:	FC57E5912F087672F80DDFA2107FCCECD09DFAF7
SHA-256:	65D86477D50754A419344D64D79D25840626140B4D4CE124E7DB142DA9A43776
SHA-512:	8FC806512981BDF7C8E6BA668C628A66F722279DC3A19291309EC964020DA0B59BAA421CF0642C4D2C693ED6D08975210C31DC19269ACB3F681F82ECB22E31A
Malicious:	**true**
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\Program Files (x86)\Microsoft Office\Office16\MSOSREC.EXE, Author: Florian Roth
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....text....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Microsoft Office\Office16\MSOSYNC.EXE	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	508160
Entropy (8bit):	4.217537531397667
Encrypted:	false
SSDEEP:	3072:wBynOpL12riocLM8js2S6bj7lZ6C6zvahEghKaBotvHkHwK:wBlL/c8js363SfShKaBo9EHwK
MD5:	72D9768111B02B7907AD0F4581B554F7
SHA1:	76BF100EA639804CF62A29FC8786227D75775EE3
SHA-256:	CEEAFCD97B02D79485D7F5F76B049004FE113D3DF6E6666528F3A74210D5895F
SHA-512:	9AB754BB98883164CE767A237E8B479516375C8530B9CAC1D4FC62217099DF451693298702F72EA83362AC311C560E9DA3F3369EF78AF98C7D94DFF10999CCB5

C:\Program Files (x86)\Microsoft Office\Office16\MSOSYNC.EXE	
Malicious:	**true**
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\Program Files (x86)\Microsoft Office\Office16\MSOSYNC.EXE, Author: Florian Roth
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Microsoft Office\Office16\MSOUC.EXE	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	564984
Entropy (8bit):	5.743979257156924
Encrypted:	false
SSDEEP:	6144:wBlL/cHYRNgcg+u0BY1QeXBSb+9ZUKyHHzxGBcnYLsFpyHP63/OElEQyqy:CeomP+uZ1QeXBSs6QNM/O55
MD5:	B393633CC0FFE37A64F71415EC6DF6AC
SHA1:	CD695040F9C63C31B1F7F58FE8DA7038B57097D5
SHA-256:	3E1317B84BC16E17F37612DCDADEADD4FB66A032B672E3567F0F804F5B1C3EFF
SHA-512:	F9B74BE428EAA9B8490E6D25DCE609201A1EAB84CBF12453B01E37DDDB7DCB202E9DD3D472C408DD382AF80E40639C63BCA711684CC94334EA49977CEFBDE 30A
Malicious:	**true**
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\Program Files (x86)\Microsoft Office\Office16\MSOUC.EXE, Author: Florian Roth
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Microsoft Office\Office16\MSQRY32.EXE	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	747680
Entropy (8bit):	6.573309755229723
Encrypted:	false
SSDEEP:	12288:CeAiut5wMRQrM5U7GYIiV7WApd8uGk0O3mMYvvmzTrdeM0fsyc/DKRGYP+4hNMy8:JATzwMREM5U7GYIiV7W28XO3mM7aTMy8
MD5:	C0946D02B0DE08986B22A5E47F80EB03
SHA1:	DAE3B7B5196AB873267E13B56BB1AD0F3C1EBF7B
SHA-256:	83560FEE54CBCD20007A83B5AC2FB3610912334AD51AADE4A3EDBF892807E276
SHA-512:	8234119FABB5DA4DBE005489F0C68089A308DD9F0CCA773053C4C74529F50F4C9A3783D6CEBBABBFAB09EEA3FDE87F1E589A1043C77E346D4FFD376523E397 3
Malicious:	**true**
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\Program Files (x86)\Microsoft Office\Office16\MSQRY32.EXE, Author: Florian Roth
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Microsoft Office\Office16\NAMECONTROLSERVER.EXE	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	153392
Entropy (8bit):	6.502271239245034
Encrypted:	false
SSDEEP:	3072:wBynOpL12riocLMKNDS5lSkOjTFa1mr+fkT77NDS5lSu0aD0K8tMk+7ms:wBlL/cKNDS5lSkQa1mr+fmfNDS5lSuLP
MD5:	77F10A6C4BD0BD5F43B2960D53F799A5
SHA1:	1F041A47CA75D6DBF85C982C11E8958496DE5A63
SHA-256:	C65947754E931E89F2F32D6F5C1150875CE8E0B999FB57291F368517C143BEEC
SHA-512:	0EDD2454B7DBA8C76938A6FBCDD5B4C181DDC183DF820A75A3726FE5C807A3331FB3E410DA65341F09F4702D3D6286C908D8D1ED03BD7C9C2F9DCA0DB3B93 4C
Malicious:	**true**

C:\Program Files (x86)\Microsoft Office\Office16\NAMECONTROLSERVER.EXE	
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\Program Files (x86)\Microsoft Office\Office16\NAMECONTROLSERVER.EXE, Author: Florian Roth
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	modified
Size (bytes):	1717544
Entropy (8bit):	6.018937015917722
Encrypted:	false
SSDEEP:	24576:JvWOXuaQ8eUXyfYvgn2ImMjbDowM1BNCkQ3aVremRRo+hQbzPNywi947QsawN:Cl8NXygvgn2KgzEUrhQbzPNyR9lsa2
MD5:	F8B605DD927F629ABDC82DBBA5AEF0DA
SHA1:	11CC0AC535C9940AF2EA86D953D94FB17069028B
SHA-256:	11DDB27F29E21EED0D419CD6A98B72259B5F3E85EE548F765305CD79636B926E
SHA-512:	AB158C914378C76CBA92B6E6382C127172295E6D1E71F1AF3B2C47182604610C2A92371BD1331E0E1DF21DD5C9349E1308287FAD431CC54A9919975413EB2771
Malicious:	**true**
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\Program Files (x86)\Microsoft Office\Office16\ONENOTE.EXE, Author: Florian Roth
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Microsoft Office\Office16\ONENOTEM.EXE	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	199344
Entropy (8bit):	5.617196844195136
Encrypted:	false
SSDEEP:	6144:wBlL/chWnuOvOYOhODOXOYOzODOaOpOxO1O3OvOJO8O+O/ONOHO4O1ONOyOjONOL:CeLe6xml
MD5:	E51BDF9A574C869D0FD23FE961122448
SHA1:	7C28BD42C26BA2EEEF2BCFE9AEB462EF069483A1
SHA-256:	3EA2D6B1F1086F6BB042FFE16078538891E349D975801B592B7EC56B09ABE3A8
SHA-512:	4450180E367FE95387C33E9263B92CF89152EED1CE93F6B650B786C5C0409477384AAA73F57A2521A7D6D9E2DF46B77BD9A6C100958FA3D63855AD22C5E27E09
Malicious:	false
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\Program Files (x86)\Microsoft Office\Office16\ONENOTEM.EXE, Author: Florian Roth
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Microsoft Office\Office16\OcPubMgr.exe	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	1598352
Entropy (8bit):	5.643143730928423
Encrypted:	false
SSDEEP:	24576:JXV2ohJid8Uy2iHlu2w7NbV+D/KTO6lTDMx:yyiuUynHYZVa0OkDMx
MD5:	9D7056F63BD4520E37BF335866E6EF77
SHA1:	0A7AF1A7283B652FFF8D6195984EC119B7BBC1DB
SHA-256:	7B2AD32DA8937A39F438167FDC5549DDBF29531D341B71A06ACAF87D6BC5B9E9
SHA-512:	B51176EC35EDB3DD363AAC0E1260980B0D88825243552A6C9BAE7FCE888C003122B3B07B9050BC818276EFB70DF6659A1BE97F0426ED806940A4E3D7530CFF4
Malicious:	**true**
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\Program Files (x86)\Microsoft Office\Office16\OcPubMgr.exe, Author: Florian Roth

C:\Program Files (x86)\Microsoft Office\Office16\OcPubMgr.exe	
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Microsoft Office\Office16\POWERPNT.EXE	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	1890480
Entropy (8bit):	3.6284877704529466
Encrypted:	false
SSDEEP:	6144:wBlL/cST6ZXFzb5Ucyw4T7po25xx2qNcUcMeTOzhc:CeSTg5Ucy9oexxtcUcMe
MD5:	14F8ED3D20B8C212B49ED173C3F08B64
SHA1:	C1C2BF6F95997B435674B6981A12802D185AB74A
SHA-256:	85492508AEFE03EB6D1EC1B0CB660C58F6FBAC73EED2F61A7D53AEADE0E9F720
SHA-512:	D1D55446E9169E4A7D2B399CD414D2155401974F5B6BC9501D2E4F24382D8AA96A74758A2459D6E24CA02346E929F4CC827EDED387E3EEE731BF25E1E59699F
Malicious:	false
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\Program Files (x86)\Microsoft Office\Office16\POWERPNT.EXE, Author: Florian Roth
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Microsoft Office\Office16\PPTICO.EXE	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	3551912
Entropy (8bit):	3.3581034794175015
Encrypted:	false
SSDEEP:	12288:Ced0knX9Y5Ucy9oexxr5UcykDuD7fcUcMeV:JdxLe3kD0Q
MD5:	18AC2B3667BA6447A1FC3290424AAFC4
SHA1:	0B66EC00BCE191CA1CF95633E6D2ED96FBFB87DA
SHA-256:	B79CD0A3665B1C2C1783F3BABE4C1A4270033CB4F13388B3CABDD767E474F204
SHA-512:	8F56E9025AB4F211CCAF4C7F6070372EF9FCFB4645EE70BFCAC9E7518A01659ECC3260C7DB3572056F18548F6DB3126B3DFDD6081F4008180EE1A4F6E3F5C2E B
Malicious:	false
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Microsoft Office\Office16\SCANPST.EXE	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	97072
Entropy (8bit):	6.554885717671024
Encrypted:	false
SSDEEP:	1536:wBWx2gmwLOuYL12EawcKocLMMMgvNuEJzbmAoDucEMQnF0:wBynOpL12riocLM81uUlbMt
MD5:	D488C2C8A091EA9BBB7D9B70768BC62D
SHA1:	A975B42640EB1B803061EC6A1686493EE3DE5AEA
SHA-256:	FAB7FDB25897D9BBDEACFE7F8972D02EFE52353619C03B62E662CC8FA871B825
SHA-512:	4D5E1333F61DDFC29B4029FDDCFD98CA5A5684C91EC1F8389037025A9347130BB563D6D2B7F986E38411FC8E25CC03788432776F03D58A5020BC6D6ABD6B7B2
Malicious:	false
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\Program Files (x86)\Microsoft Office\Office16\SCANPST.EXE, Author: Florian Roth
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Microsoft Office\Office16\SELFCERT.EXE	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	401112
Entropy (8bit):	6.196413679570548
Encrypted:	false
SSDEEP:	6144:wBlL/cGDppHQA0GZHU0MQdtmutQqrvMcHe6Gg1WLu+ffCvkV2hriVFRG5pcGBvc3:Ce0/CGN+9qrvMciMiCaI8D
MD5:	4F8375F21C5338A424002FDACC22B168
SHA1:	CABFDAA9CE097D2FC836FDDC66FC4222080EC24B
SHA-256:	F4E57FF1E7908A19851E20E7C37AD03EA0AA33F45C6D83BC3937A817EF3BE684
SHA-512:	7594628A0021EFCAFA31DD00714E96C36322B4C5AF9B773A774EA0931F78D811F32220C4F9BC8C242AA8711C4A9D05A5033527DD5738815B194EF0FD7E57EA79
Malicious:	false
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\Program Files (x86)\Microsoft Office\Office16\SELFCERT.EXE, Author: Florian Roth
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Microsoft Office\Office16\lync99.exe	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	779568
Entropy (8bit):	3.9128948309798304
Encrypted:	false
SSDEEP:	6144:wBlL/cHkYNiTF7BjXnhMKNRneNMToeGYAXLMDpQCfhmLV:CeHkHTz9cRLMdQYWV
MD5:	1FB5EA4AAADBA063720A6D41E3F0BCC9
SHA1:	8F8E977B9B5D65574ECD1220F56EEE3544439789
SHA-256:	A8E5B950544C6D84819D71AFC6E95C632648613559DC09D01456AE85D2BF3B25
SHA-512:	CCBBA01B4FB1AE5F1FA75C3F2BEBA921CD52C07A7988DD82EBAC8BBD9075B22EF564DB2D7D2BB023F6B559839506D79741F52E8A0596CA61B165A1DE5DCA1B54
Malicious:	**true**
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\Program Files (x86)\Microsoft Office\Office16\lync99.exe, Author: Florian Roth
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Microsoft Office\Office16\lynchtmlconv.exe	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	9384960
Entropy (8bit):	6.481592589152662
Encrypted:	false
SSDEEP:	196608:scs45Kb0KuviDnYatO4HbnvVa73gRT3BWziGis9qhSfpmL:sNb0KuvenYiOGTV03GxWfis9qhr
MD5:	7E526EB0E28DA43F291F9C11BCE76A2C
SHA1:	B6F0038F12832A1769203F3A7D0380010C378FAA
SHA-256:	BFA6AF0A2FBF9EC83247D2755EA40D1E661E917F57DC15CBACE629DC6DA8BC25
SHA-512:	41AB976D5486852908B70AFB2C1EEB1AA2A047451774D75049267AD7BC56E88DD79CDFCADB9BB05DF9BAAF08166683F32A43D8B96CDBDADEA3E54A288EAF6DE2
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Microsoft Office\Office16\misc.exe	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped

C:\Program Files (x86)\Microsoft Office\Office16\misc.exe	
Size (bytes):	1069224
Entropy (8bit):	3.695307514861535
Encrypted:	false
SSDEEP:	3072:wBynOpL12riocLMto4TUawK1uT040i0ougmQmJDJnJ+20FxPlJPPSSPJ/Z:wBlL/c6243xmQm59UtUSxh
MD5:	F1334EE496A627FD9C8711A948FA1592
SHA1:	782298BA245A3FEB067203A827AE7C0D028136B1
SHA-256:	C0DC87F571ADBAAC3FFBCC34A157F0102C2D6528B2CE8920A1E7F7A36BCFDF69
SHA-512:	B4D9D1330E4917F97A4A831772F1FF4C408A6483B8BB3217266CFF3AC0D36EECBA8628B38970AA5FAECCF73E009A3D5E9C1ABF05AB68B161D3F5B59BA3031F2E
Malicious:	**true**
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\Program Files (x86)\Microsoft Office\Office16\misc.exe, Author: Florian Roth
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....text....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\Program Files (x86)\Microsoft Office\Office16\protocolhandler.exe	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	778768
Entropy (8bit):	5.422629037460947
Encrypted:	false
SSDEEP:	12288:CestfUJogx+ymi4l0AIFkxAavN50P7DKacrdL+GNXuwt:J0UJDxwOfmAe5ADPcrR+GNXuwt
MD5:	EFC7C9309C4FEF7AD8F3EDCC1E8B668E
SHA1:	C825BD8762AB52D99E04E6C51E44C25D23D381DF
SHA-256:	65E6581E10B4D705A9FDC85B303007DE6A52692E4CA1E5438E8A14081AC05771
SHA-512:	D66C16C38F59D336527772B9509A38BE775AB8C45BF31C816C27D0BEDDA2F6E68802F0B06CB9808F432D7428C795981B1B33A58B482A70971E40AA76A756B370
Malicious:	false
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\Program Files (x86)\Microsoft Office\Office16\protocolhandler.exe, Author: Florian Roth
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....text....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\ProgramData\Adobe\ARM\S\11399\AdobeARMHelper.exe	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	464936
Entropy (8bit):	6.3700138958936705
Encrypted:	false
SSDEEP:	6144:wBlL/cQQcslnC3znG+xfbMgyGn7LiJdKkAtyKuskePvX2Zp7DmuXYvr6ys/pJYCf:CeLlnCxjMyn72/KkAtydem3nM6BHYo
MD5:	68EEF6F4C9180056AC1B7F7B2BB3D6E9
SHA1:	4026B47480DC6A5256512F08C2E93A0D08C8D786
SHA-256:	7E8E0440C1E46147F90768CBB570B81AFA8C22F75072B2545877CC3660D90896
SHA-512:	575502D7C421123ACF6006A84184941BEA9C0561C02B14C0CD72E195215786DEEB055DC3F7C067E4B22E717645C7737B7A8F5D0E08019C57265E5B74F6C7ADD
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....text....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\ProgramData\Adobe\ARM\S\1977\AdobeARMHelper.exe	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	464936
Entropy (8bit):	6.3700138958936705
Encrypted:	false
SSDEEP:	6144:wBlL/cQQcslnC3znG+xfbMgyGn7LiJdKkAtyKuskePvX2Zp7DmuXYvr6ys/pJYCf:CeLlnCxjMyn72/KkAtydem3nM6BHYo

C:\ProgramData\Adobe\ARM\S\1977\AdobeARMHelper.exe	
MD5:	68EEF6F4C9180056AC1B7F7B2BB3D6E9
SHA1:	4026B47480DC6A5256512F08C2E93A0D08C8D786
SHA-256:	7E8E0440C1E46147F90768CBB570B81AFA8C22F75072B2545877CC3660D90896
SHA-512:	575502D7C421123ACF6006A84184941BEA9C0561C02B14C0CD72E195215786DEEB055DC3F7C067E4B22E717645C7737B7A8F5D0E08019C57265E5B74F6C7ADD
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\ProgramData\Adobe\Setup\{AC76BA86-7AD7-1033-7B44-AC0F074E4100}\setup.exe	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	506352
Entropy (8bit):	6.097360969203621
Encrypted:	false
SSDEEP:	6144:wBlL/ca5Qw0tneDA/sqhleIc0HftDrkYY1hj63hgDonsogCh6NEpAFH78r:Ce2bM3npxYfj63hgD1Zim8r
MD5:	FF17B36B43E314751E99F5F9905ECF37
SHA1:	D0A87B8286717B314ED481B72078289C46842072
SHA-256:	902F757B1BE9862AC408AA25EC70EDD2936B020E5D38F8A6A3E85288D1459305
SHA-512:	2FCD0BC15CC422410DE1A252446D1903341E8F5F0674DF01A5D4A49DF6CE908FFF109B23D03AD46EFE3390848E63EEDFCF17DED397F1293EB2A7A53D05E9A94
Malicious:	**true**
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\ProgramData\Microsoft\Windows Defender\Scans\MpPayloadData\mpengine.exe	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	193552
Entropy (8bit):	6.418812603146487
Encrypted:	false
SSDEEP:	3072:wBynOpL12riocLMeOIFRq+fPkorzr30W3Zqa/TVm3c+ZIVoarXRKKntTKxsN:wBlL/ce9FfPkoXLZucR5X8KtmKN
MD5:	3988DCBD4BC28122726EECCA5990D21E
SHA1:	3D0A35D599644307C0B26850B0332E7E479C54EA
SHA-256:	9C71444F99408BA4D05A4C88279A6418CFC6096480989B21966BCA517810DAE4
SHA-512:	DAF922D97AD27A9A33887C24A16009D445273CBFACA3E4ABBA0F37B9C07FEBB38FAD1D475D5C8354A47E124BEAAFA72F6FA96DD46E70120B015DDE16A3ACEEBF
Malicious:	**true**
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\ProgramData\Microsoft\Windows Defender\Scans\MpPayloadData\mpengine.exe, Author: Florian Roth
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\ProgramData\Package Cache\{050d4fc8-5d48-4b8f-8972-47c82c46020f}\vcredist_x64.exe	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	502872
Entropy (8bit):	6.915127466988929
Encrypted:	false
SSDEEP:	12288:CexB+pwPprnVmLmDsC+FU+ZOSzt9tzZcymOz:JzDFncLmKDZOSzXFZcLOz
MD5:	A453FED63351808A13037F0A0774442B
SHA1:	8E3CA42161D0AF879251DFD616650736A6258AF0
SHA-256:	0E934BFA9B77E05EB2A110AD990F575F317B4E37716E6D5631EAE9BB5C334372
SHA-512:	87C11B3F546A7A46A1C2E7B1E1E440297B011E8B8A81FF14273EF0EA00F1B235EC94C56CA342500453FCC8D249D59710171FA7714AD452AA8495B63A5595648C
Malicious:	**true**

C:\ProgramData\Package Cache\{050d4fc8-5d48-4b8f-8972-47c82c46020f}\vcredist_x64.exe	
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\ProgramData\Package Cache\{050d4fc8-5d48-4b8f-8972-47c82c46020f}\vcredist_x64.exe, Author: Florian Roth • Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\ProgramData\Package Cache\{050d4fc8-5d48-4b8f-8972-47c82c46020f}\vcredist_x64.exe, Author: Florian Roth
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

C:\ProgramData\Package Cache\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\vcredist_x86.exe	
Process:	C:\Users\user\Desktop\KFoTnHP6B2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Category:	dropped
Size (bytes):	497192
Entropy (8bit):	7.031962788135064
Encrypted:	false
SSDEEP:	12288:Cez0IursYCYQeSnyZJiqlEbXSb9NtoqOFBqkYHkZH:JgMYenGJiKEbXWtpOLl5
MD5:	215FFB3C0FC21120841C33D550C6F658
SHA1:	5BBFC559170BE265247F2A639B25A6887BF131AB
SHA-256:	B951888CFC6BCB3190E169AAFEF942EC3F2CE0434EF5098F9F4FD286CBFF0A47
SHA-512:	148F23F259053060B5ADEA9AB24EFC9418D53D5213954E4B8C4BE2018C30997882531CA00F68B0AC4C04A187E5C3075CA45653C827C2D68FB80100DEBA45B9B
Malicious:	**true**
Yara Hits:	• Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\ProgramData\Package Cache\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\vcredist_x86.exe, Author: Florian Roth • Rule: SUSP_NullSoftInst_Combo_Oct20_1, Description: Detects suspicious NullSoft Installer combination with common Copyright strings, Source: C:\ProgramData\Package Cache\{33d1fd90-4274-48a1-9bc1-97e33d9c2d6f}\vcredist_x86.exe, Author: Florian Roth
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....0(..QF..QF..QF.*^...QF..QG.qQF.*^...QF.rv..QF..W@..QF.Rich.QF .....PE..L...e:.V.....\.....0.....p....@.....t.....p..|.....te xt....Z.....\..... ..`.rdata.....p.....`.....@..@.data...8.....r.....@....ndata.....P.....rsrc.....x.....@..@..... ....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows, Nullsoft Installer self-extracting archive
Entropy (8bit):	7.915461873573666
TrID:	• Win32 Executable (generic) a (10002005/4) 99.96% • Generic Win/DOS Executable (2004/3) 0.02% • DOS Executable Generic (2002/1) 0.02% • Autodesk FLIC Image File (extensions: flc, fli, cel) (7/3) 0.00%
File name:	KFoTnHP6B2.exe
File size:	235529
MD5:	df330ab2a2e5aa4ac947315ee3f93992
SHA1:	76b5d1eee342b47fe58e2136a067712cbd210351
SHA256:	99a897c5b8f53e1d04e51107c748a4f385b754a852ca6b6 05559f5b50820a64f
SHA512:	e65f573d68e8f198024028d553210095173d1551e6074b 0d9543977116a0286f75641f4692049a49e6cd03729b001 027136419d6cf0c71645e800d5522ed895
SSDEEP:	6144:wBlL/c2HMSZ54elOp0S4jfEpGibIsdpwBQ:Ce2HM SZWeO0S4Mh0gS6
File Content Preview:	MZ.....@.....!..L.!Th is program cannot be run in DOS mode....$.....0(..QF.. QF..QF.*^...QF..QG.qQF.*^...QF..rv..QF..W@..QF.Rich. QF.....PE..L...e:.V.....\.....0.....p....@

File Icon

Icon Hash:	b2a88c96b2ca6a72

Static PE Info

General

Entrypoint:	0x4030fb
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	LOCAL_SYMS_STRIPPED, 32BIT_MACHINE, EXECUTABLE_IMAGE, LINE_NUMS_STRIPPED, RELOCS_STRIPPED
DLL Characteristics:	TERMINAL_SERVER_AWARE
Time Stamp:	0x56FF3A65 [Sat Apr 2 03:20:05 2016 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:	b76363e9cb88bf9390860da8e50999d2

Entrypoint Preview

Rich Headers

Data Directories

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0x5aeb	0x5c00	False	0.665123980978	data	6.42230569414	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x7000	0x1196	0x1200	False	0.458984375	data	5.20291736659	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x9000	0x1b038	0x600	False	0.432291666667	data	4.0475118296	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.ndata	0x25000	0x8000	0x0	False	0	empty	0.0	IMAGE_SCN_MEM_WRITE, IMAGE_SCN_CNT_UNINITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x2d000	0x9e0	0xa00	False	0.45625	data	4.50948350161	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ

Resources

Imports

Possible Origin

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

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: KFoTnHP6B2.exe PID: 5520 Parent PID: 2864

General

Start time:	19:03:19
Start date:	27/10/2021
Path:	C:\Users\user\Desktop\KFoTnHP6B2.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\KFoTnHP6B2.exe'
Imagebase:	0x400000
File size:	235529 bytes
MD5 hash:	DF330AB2A2E5AA4AC947315EE3F93992
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_FormBook, Description: Yara detected FormBook, Source: 00000000.00000002.267620652.000000000F03A000.00000004.00000001.sdmp, Author: Joe Security • Rule: Formbook_1, Description: autogenerated rule brought to you by yara-signator, Source: 00000000.00000002.267620652.000000000F03A000.00000004.00000001.sdmp, Author: Felix Bilstein - yara-signator at cocacoding dot com • Rule: Formbook, Description: detect Formbook in memory, Source: 00000000.00000002.267620652.000000000F03A000.00000004.00000001.sdmp, Author: JPCERT/CC Incident Response Group • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: 00000000.00000002.267609639.000000000F030000.00000004.00000001.sdmp, Author: Florian Roth
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: KFoTnHP6B2.exe PID: 4932 Parent PID: 5520

General

Start time:	19:03:20
Start date:	27/10/2021
Path:	C:\Users\user\Desktop\KFoTnHP6B2.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\KFoTnHP6B2.exe'

Imagebase:	0x400000
File size:	235529 bytes
MD5 hash:	DF330AB2A2E5AA4AC947315EE3F93992
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: 00000002.00000000.254262748.00000000001D0000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: 00000002.00000000.258305894.00000000001D0000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: 00000002.00000000.260372806.00000000001D0000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: 00000002.00000000.261268435.00000000001D0000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: 00000002.00000000.263822503.00000000001D0000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: 00000002.00000000.256253314.00000000001D0000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: 00000002.00000000.264363757.00000000001D0000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: 00000002.00000000.262239992.00000000001D0000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: 00000002.00000000.255320812.00000000001D0000.00000040.00000001.sdmp, Author: Florian Roth • Rule: MAL_Neshta_Generic, Description: Detects Neshta malware, Source: 00000002.00000000.257135869.00000000001D0000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_Neshta, Description: Yara detected Neshta, Source: 00000002.00000002.522605654.00000000001D9000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities Show Windows behavior

File Created

File Written

File Read

Registry Activities Show Windows behavior

Key Value Modified

Disassembly

Code Analysis