ID: 320480
Sample Name:
b15023b1855da1cf5213b061dc626cc2
Cookbook: default.jbs
Time: 12:02:22
Date: 19/11/2020
Version: 31.0.0 Red Diamond

Table of Contents

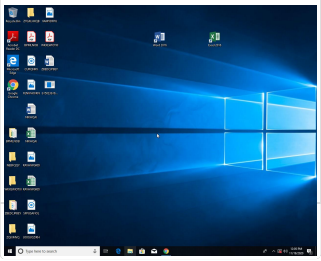
Analysis Report b15023b1855da1cf5213b061dc626cc2

Overview

General Information

Sample Name:	b15023b1855da1cf5213b061dc626cc2 (renamed file extension from none to exe)
Analysis ID:	320480
MD5:	ac5eb6172c287c..
SHA1:	3bb19910b89a39..
SHA256:	da23b9268823cc..
Tags:	HawkEye

Most interesting Screenshot:



Detection

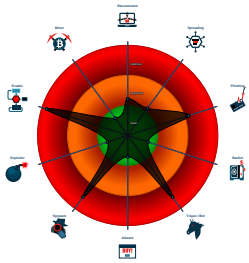
HawkEye
MailPassView

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

Signatures

- Antivirus / Scanner detection for sub…
- Antivirus detection for dropped file
- Detected HawkEye Rat
- Found malware configuration
- Malicious sample detected (through …
- Multi AV Scanner detection for doma…
- Multi AV Scanner detection for dropp…
- Multi AV Scanner detection for subm…
- Sigma detected: Drops script at star…
- Yara detected HawkEye Keylogger
- Yara detected MailPassView
- .NET source code references suspic…

Classification



Startup

- **System is w10x64**
- b15023b1855da1cf5213b061dc626cc2.exe (PID: 6432 cmdline: 'C:\Users\user\Desktop\b15023b1855da1cf5213b061dc626cc2.exe' MD5: AC5EB6172C287CBB954954B56586653F)
  - RegAsm.exe (PID: 6476 cmdline: 'C:\Users\user\Desktop\b15023b1855da1cf5213b061dc626cc2.exe' MD5: 529695608EAFBED00ACA9E61EF333A7C)
    - vbc.exe (PID: 6576 cmdline: 'C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe' /stext 'C:\Users\user\AppData\Local\Temp\tmp992B.tmp' MD5: C63ED21D5706A527419C9FBD730FFB2E)
    - vbc.exe (PID: 6280 cmdline: 'C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe' /stext 'C:\Users\user\AppData\Local\Temp\tmp92CE.tmp' MD5: C63ED21D5706A527419C9FBD730FFB2E)
- xjyxibeifbdmock.exe (PID: 6828 cmdline: 'C:\Users\user\AppData\Roaming\ezocxcvggg\xjyxibeifbdmock.exe' MD5: C0962CFBB4BB43348708437D8CD1D8EF)
  - RegAsm.exe (PID: 6852 cmdline: 'C:\Users\user\AppData\Roaming\ezocxcvggg\xjyxibeifbdmock.exe' MD5: 529695608EAFBED00ACA9E61EF333A7C)
    - vbc.exe (PID: 6948 cmdline: 'C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe' /stext 'C:\Users\user\AppData\Local\Temp\tmpDC10.tmp' MD5: C63ED21D5706A527419C9FBD730FFB2E)
    - vbc.exe (PID: 3252 cmdline: 'C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe' /stext 'C:\Users\user\AppData\Local\Temp\tmpD611.tmp' MD5: C63ED21D5706A527419C9FBD730FFB2E)
- **cleanup**

Malware Configuration

Threatname: HawkEye


```
{
  "Modules": [
    "WebBrowserPassView"
  ],
  "Version": ""
}
```


Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000001.00000002.608241206.00000000035AF000.00000004.00000001.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	

Source	Rule	Description	Author	Strings
00000005.00000002.606139905.0000000002DD2000.00000004.00000001.sdmp	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
00000006.00000002.405206241.000000000400000.00000040.00000001.sdmp	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
00000000.00000002.368012063.0000000032130000.00000004.00000001.sdmp	MAL_HawkEye_Keylogger_Gen_Dec18	Detects HawkEye Keylogger Reborn	Florian Roth	• 0x87c2e:$s1: HawkEye Keylogger • 0x87c97:$s1: HawkEye Keylogger • 0x81071:$s2: _ScreenshotLogger • 0x8103e:$s3: _PasswordStealer
00000000.00000002.368012063.0000000032130000.00000004.00000001.sdmp	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
Click to see the 49 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
4.2.xjyxibeifbdmock.exe.31ee0000.1.unpack	MAL_HawkEye_Keylogger_Gen_Dec18	Detects HawkEye Keylogger Reborn	Florian Roth	• 0x85e2e:$s1: HawkEye Keylogger • 0x85e97:$s1: HawkEye Keylogger • 0x7f271:$s2: _ScreenshotLogger • 0x7f23e:$s3: _PasswordStealer
4.2.xjyxibeifbdmock.exe.31ee0000.1.unpack	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
4.2.xjyxibeifbdmock.exe.31ee0000.1.unpack	HawkEyev9	HawkEye v9 Payload	ditekshen	• 0x85e2e:$id1: HawkEye Keylogger - Reborn v9 - {0} Logs - {1} \ {2} • 0x85e97:$id2: HawkEye Keylogger - Reborn v9{0}{1} Logs{0}{2} \ {3}{0}{0}{4} • 0x7f23e:$str1: _PasswordStealer • 0x7f24f:$str2: _KeyStrokeLogger • 0x7f271:$str3: _ScreenshotLogger • 0x7f260:$str4: _ClipboardLogger • 0x7f283:$str5: _WebCamLogger • 0x7f398:$str6: _AntiVirusKiller • 0x7f386:$str7: _ProcessElevation • 0x7f34d:$str8: _DisableCommandPrompt • 0x7f453:$str9: _WebsiteBlocker • 0x7f463:$str9: _WebsiteBlocker • 0x7f339:$str10: _DisableTaskManager • 0x7f3b4:$str11: _AntiDebugger • 0x7f43e:$str12: _WebsiteVisitorSites • 0x7f363:$str13: _DisableRegEdit • 0x7f3c2:$str14: _ExecutionDelay • 0x7f2e7:$str15: _InstallStartupPersistance
5.2.RegAsm.exe.4d10000.1.raw.unpack	APT_NK_BabyShark_KimJoingRAT_Apr19_1	Detects BabyShark KimJongRAT	Florian Roth	• 0x6b4fa:$a1: logins.json • 0x6b45a:$s3: SELECT id, hostname, httpRealm, formSubmitURL, usernameField, passwordField, encryptedUsername, encryptedPassword FROM moz_login • 0x6bc7e:$s4: \mozsqlite3.dll • 0x6a4ee:$s5: SMTP Password
5.2.RegAsm.exe.4d10000.1.raw.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
Click to see the 37 entries				

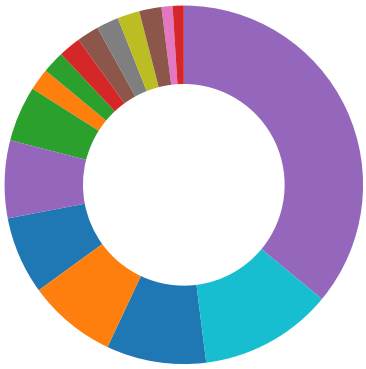
Sigma Overview

System Summary:

Sigma detected: Drops script at startup location

Signature Overview

- AV Detection
- Spreading
- Networking
- Key, Mouse, Clipboard, Microphone and Screen Capturing
- System Summary
- Data Obfuscation
- Persistence and Installation Behavior



Click to jump to signature section

AV Detection:

- Antivirus / Scanner detection for submitted sample
- Antivirus detection for dropped file
- Found malware configuration
- Multi AV Scanner detection for domain / URL
- Multi AV Scanner detection for dropped file
- Multi AV Scanner detection for submitted file
- Machine Learning detection for dropped file
- Machine Learning detection for sample

Key, Mouse, Clipboard, Microphone and Screen Capturing:

- Yara detected HawkEye Keylogger

System Summary:

- Malicious sample detected (through community Yara rule)

Malware Analysis System Evasion:

- Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)
- Tries to delay execution (extensive OutputDebugStringW loop)
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)

HIPS / PFW / Operating System Protection Evasion:

- .NET source code references suspicious native API functions
- Allocates memory in foreign processes
- Injects a PE file into a foreign processes
- Maps a DLL or memory area into another process
- Sample uses process hollowing technique
- Writes to foreign memory regions

Stealing of Sensitive Information:

- Yara detected HawkEye Keylogger

Yara detected MailPassView

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

Tries to steal Instant Messenger accounts or passwords

Tries to steal Mail credentials (via file access)

Tries to steal Mail credentials (via file registry)

Yara detected WebBrowserPassView password recovery tool

Remote Access Functionality:

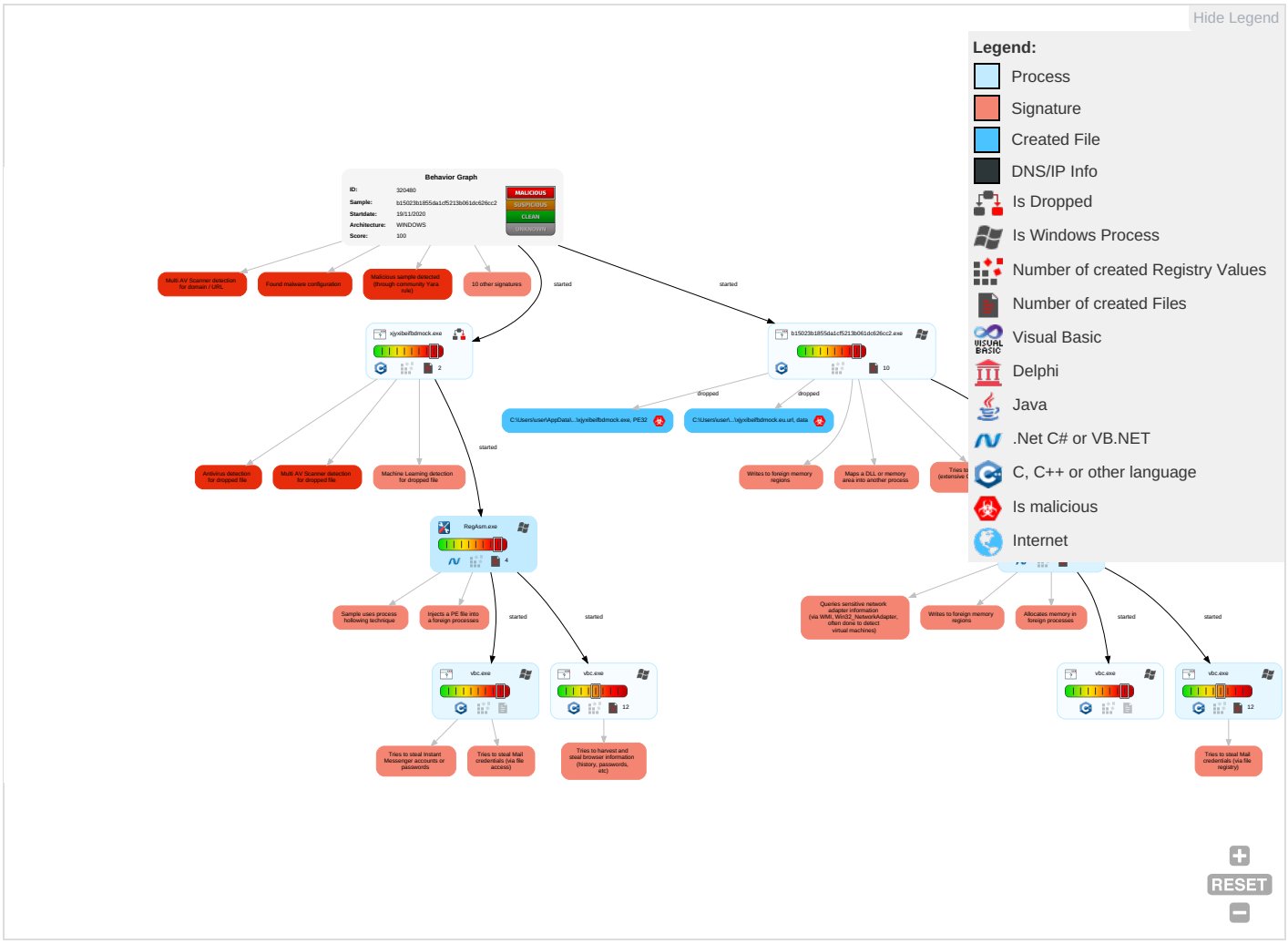
Detected HawkEye Rat

Yara detected HawkEye Keylogger

Mitre Att&ck Matrix

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Valid Accounts	Windows Management Instrumentation 1 1 1	Startup Items 1	Startup Items 1	Disable or Modify Tools 1	OS Credential Dumping 1	System Time Discovery 1	Remote Services	Archive Collected Data 1 1	Exfiltration Over Other Network Medium	Encrypted Channel 1
Default Accounts	Native API 1 1	DLL Side-Loading 1	DLL Side-Loading 1	Deobfuscate/Decode Files or Information 1 1	Credentials in Registry 2	Account Discovery 1	Remote Desktop Protocol	Data from Local System 1	Exfiltration Over Bluetooth	Remote Acce Software 1
Domain Accounts	Shared Modules 1	Application Shimming 1	Application Shimming 1	Obfuscated Files or Information 2	Credentials In Files 1	File and Directory Discovery 2	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Steganograp
Local Accounts	Command and Scripting Interpreter 2	Registry Run Keys / Startup Folder 2	Process Injection 5 1 2	Software Packing 1	NTDS	System Information Discovery 1 9	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer	Protocol Impersonatio
Cloud Accounts	Cron	Network Logon Script	Registry Run Keys / Startup Folder 2	DLL Side-Loading 1	LSA Secrets	Security Software Discovery 3 6	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Masquerading 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 2 3	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicati
External Remote Services	Scheduled Task	Startup Items	Startup Items	Virtualization/Sandbox Evasion 2 3	DCSync	Process Discovery 4	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Process Injection 5 1 2	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protoc

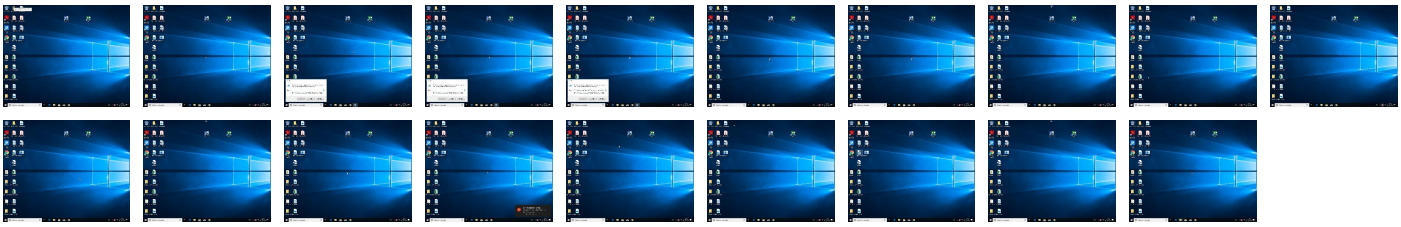
Behavior Graph



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
b15023b1855da1cf5213b061dc626cc2.exe	61%	Virustotal		Browse
b15023b1855da1cf5213b061dc626cc2.exe	51%	Metadefender		Browse
b15023b1855da1cf5213b061dc626cc2.exe	65%	ReversingLabs	Win32.Backdoor.Androm	
b15023b1855da1cf5213b061dc626cc2.exe	100%	Avira	TR/Dropper.Gen	
b15023b1855da1cf5213b061dc626cc2.exe	100%	Joe Sandbox ML		

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\ezocxcvggg\xjyxibeifbdmock.exe	100%	Avira	TR/Dropper.Gen	
C:\Users\user\AppData\Roaming\ezocxcvggg\xjyxibeifbdmock.exe	100%	Joe Sandbox ML		
C:\Users\user\AppData\Roaming\ezocxcvggg\xjyxibeifbdmock.exe	62%	ReversingLabs	Win32.Backdoor.Androm	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
4.2.xjyxibeifbdmock.exe.150000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
2.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
1.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
0.2.b15023b1855da1cf5213b061dc626cc2.exe.a30000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
4.0.xjyxibeifbdmock.exe.150000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Source	Detection	Scanner	Label	Link	Download
6.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File
5.2.RegAsm.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
0.0.b15023b1855da1cf5213b061dc626cc2.exe.a30000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File

Domains

No Antivirus matches

URLs

Source	Detection	Scanner	Label	Link
http://https://a.pomf.cat/	4%	Virustotal		Browse
http://https://a.pomf.cat/	0%	Avira URL Cloud	safe	
http://pomf.cat/upload.php&https://a.pomf.cat/	0%	Avira URL Cloud	safe	
http://pomf.cat/upload.php	9%	Virustotal		Browse
http://pomf.cat/upload.php	0%	Avira URL Cloud	safe	
http://https://2542116.fls.doubleM	0%	Avira URL Cloud	safe	
http://pomf.cat/upload.phpCContent-Disposition:	0%	Avira URL Cloud	safe	

Domains and IPs

Contacted Domains

No contacted domains info

URLs from Memory and Binaries

Name	Source	Malicious	Antivirus Detection	Reputation
http://https://2542116.fls.doubleclick.net/activityi;src=2542116;type=chrom322;cat=chrom01g;ord=30055406629	vbc.exe, 00000002.00000003.368921310.0000000002212000.00000004.00000001.sdmp, vbc.exe, 00000002.00000003.368809279.00000002210000.00000004.00000001.sdmp, vbc.exe, 00000002.00000003.369053591.0000000002213000.00000004.00000001.sdmp, vbc.exe, 00000006.00000003.404653728.00000000020E2000.00000004.00000001.sdmp, vbc.exe, 00000006.00000003.404525940.00000000020E0000.00000004.00000001.sdmp, vbc.exe, 00000006.00000003.404912057.00000000020E3000.00000004.00000001.sdmp, vbc.exe, 00000006.00000003.404720258.00000000020E1000.00000004.00000001.sdmp	false		high
http://https://a.pomf.cat/	RegAsm.exe, 00000001.00000002.605985687.00000000033C3000.00000004.00000001.sdmp, RegAsm.exe, 00000005.00000002.605786252.0000000002D23000.00000004.00000001.sdmp	false	• 4%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=858412214&size=306x271&https=1LMEM	vbc.exe, 00000002.00000002.370773894.000000000076D000.00000004.00000020.sdmp	false		high
http://pomf.cat/upload.php&https://a.pomf.cat/	b15023b1855da1cf5213b061dc626cc2.exe, 00000000.00000002.368012063.0000000032130000.00000004.00000001.sdmp, RegAsm.exe, 00000001.00000002.602404324.0000000000402000.00000040.00000001.sdmp, xjyxibeifbdmock.exe, 00000004.00000002.403557593.0000000031EE0000.00000004.00000001.sdmp, RegAsm.exe, 00000005.00000002.602420435.0000000000402000.00000040.00000001.sdmp	true	• Avira URL Cloud: safe	unknown

Name	Source	Malicious	Antivirus Detection	Reputation
http://pomf.cat/upload.php	RegAsm.exe, 00000001.00000002.605985687.00000000033C3000.00000004.00000001.sdmp, RegAsm.exe, 00000005.00000002.605786252.0000000002D23000.00000004.00000001.sdmp	true	• 9%, Virustotal, Browse • Avira URL Cloud: safe	unknown
http://https://2542116.fls.doubleM	vbc.exe, 00000002.00000002.370773894.000000000076D000.00000004.00000020.sdmp	false	• Avira URL Cloud: safe	unknown
http://https://contextual.media.net/checksync.php?&vsSync=1&cs=1&hb=1&cv=37&ndec=1&cid=8HBI57XIG&prvid=77%2	vbc.exe, 00000006.00000003.404525940.00000000020E0000.00000004.00000001.sdmp, vbc.exe, 00000006.00000003.404912057.00000000020E3000.00000004.00000001.sdmp, vbc.exe, 00000006.00000003.404720258.00000000020E1000.00000004.00000001.sdmp	false		high
http://www.msn.com/?ocid=iehphttp://www.msn.com/http://www.msn.com/de-ch/?ocid=iehphttp://www.msn.co	vbc.exe, 00000006.00000003.404525940.00000000020E0000.00000004.00000001.sdmp, vbc.exe, 00000006.00000003.404912057.00000000020E3000.00000004.00000001.sdmp, vbc.exe, 00000006.00000003.404720258.00000000020E1000.00000004.00000001.sdmp	false		high
http://https://login.yahoo.com/config/login	vbc.exe	false		high
http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=722878611&size=306x271&https=1https://c	vbc.exe, 00000006.00000003.404525940.00000000020E0000.00000004.00000001.sdmp, vbc.exe, 00000006.00000003.404912057.00000000020E3000.00000004.00000001.sdmp, vbc.exe, 00000006.00000003.404720258.00000000020E1000.00000004.00000001.sdmp	false		high
http://www.nirsoft.net	vbc.exe, 00000002.00000002.370154038.000000000019C000.00000004.00000010.sdmp, vbc.exe, 00000006.00000002.405184269.0000000019C000.00000004.00000010.sdmp	false		high
http://www.nirsoft.net/	vbc.exe, 00000013.00000002.540468694.0000000000400000.00000040.00000001.sdmp	false		high
http://https://contextual.media.net/checksync.phphttps://contextual.media.net/checksync.php?&vsSync=1&cs=1&	vbc.exe, 00000006.00000003.404525940.00000000020E0000.00000004.00000001.sdmp, vbc.exe, 00000006.00000003.404912057.00000000020E3000.00000004.00000001.sdmp, vbc.exe, 00000006.00000003.404720258.00000000020E1000.00000004.00000001.sdmp	false		high
http://https://contextual.media.net/medianet.php?cid=8CU157172&crid=722878611&size=306x271&https=1LMEM	vbc.exe, 00000002.00000002.370773894.000000000076D000.00000004.00000020.sdmp	false		high
http://bot.whatismyipaddress.com/	RegAsm.exe, 00000005.00000002.605786252.0000000002D23000.00000004.00000001.sdmp	false		high
http://https://2542116.fls.doubleclick.net/activityi;src=2542116;type=clien612;cat=chromx;ord=1;num=7859736	vbc.exe, 00000002.00000002.370849978.0000000002214000.00000004.00000001.sdmp, vbc.exe, 00000006.00000002.405655164.00000000020E4000.00000004.00000001.sdmp	false		high
http://pomf.cat/upload.phpCContent-Disposition:	RegAsm.exe, 00000001.00000002.605985687.00000000033C3000.00000004.00000001.sdmp, RegAsm.exe, 00000005.00000002.605786252.0000000002D23000.00000004.00000001.sdmp	true	• Avira URL Cloud: safe	unknown

Contacted IPs

No contacted IP infos

General Information

Joe Sandbox Version:	31.0.0 Red Diamond
Analysis ID:	320480
Start date:	19.11.2020
Start time:	12:02:22
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 10m 32s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	b15023b1855da1cf5213b061dc626cc2 (renamed file extension from none to 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.phis.troj.spyw.evad.winEXE@14/5@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 89.9% (good quality ratio 83.1%) • Quality average: 75.9% • Quality standard deviation: 30%
HCA Information:	• Successful, ratio: 77% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All • Exclude process from analysis (whitelisted): MpCmdRun.exe, audiodg.exe, BackgroundTransferHost.exe, WMIADAP.exe, backgroundTaskHost.exe, conhost.exe, svchost.exe • Report size exceeded maximum capacity and may have missing behavior information. • Report size exceeded maximum capacity and may have missing disassembly code.

Simulations

Behavior and APIs

Time	Type	Description
12:03:27	API Interceptor	2x Sleep call for process: RegAsm.exe modified
12:03:27	Autostart	Run: C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\xjyxibeifbdmock.eu.url
12:03:41	API Interceptor	1x Sleep call for process: xjyxibeifbdmock.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Temp\ecfc61d0-e5dc-e5e1-276d-ec9f9689ba6d	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	88
Entropy (8bit):	5.490292840056112
Encrypted:	false
SSDEEP:	3:PFYyImXF9mN2RVQON4NgCkCAUdXM:PHRB6+C3xy
MD5:	454353131947D1483FF5470107478978
SHA1:	C559163C23E5F878BE85D05F3EDEEAA620173C3D
SHA-256:	2DF94DC1C58E952A1EBD1AE1185A291A8A573982CA90EC1BBB87B81126002668
SHA-512:	C8912DA4654C735F7618B0ABEA7EC0197B17E6E072718B825B5799B2E88CC0E8AE8245CA95E1E5955C3AB8F649CA4ED6529975B142B061ECC402D935401B84DE
Malicious:	false
Reputation:	moderate, very likely benign file
Preview:	LeNF7Goy7uuKWKsmWAhDmhEi2BbZGy27JQQaO8wc/LiRcthbCBcu+4Nt6yYR3dz6dYTg/ZHS1axBPoq2xePo2w==

C:\Users\user\AppData\Local\Temp\tmp992B.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	..

C:\Users\user\AppData\Local\Temp\tmpDC10.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Little-endian UTF-16 Unicode text, with no line terminators
Category:	dropped
Size (bytes):	2
Entropy (8bit):	1.0
Encrypted:	false
SSDEEP:	3:Qn:Qn
MD5:	F3B25701FE362EC84616A93A45CE9998
SHA1:	D62636D8CAEC13F04E28442A0A6FA1AFEB024BBB
SHA-256:	B3D510EF04275CA8E698E5B3CBB0ECE3949EF9252F0CDC839E9EE347409A2209

C:\Users\user\AppData\Local\Temp\tmpDC10.tmp	
SHA-512:	98C5F56F3DE340690C139E58EB7DAC111979F0D4DFFE9C4B24FF849510F4B6FFA9FD608C0A3DE9AC3C9FD2190F0EFAF715309061490F9755A9BFDF1C54CA0D 4
Malicious:	false
Reputation:	high, very likely benign file
Preview:	..

C:\Users\user\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\xjyxibeifbdmock.eu.url	
Process:	C:\Users\user\Desktop\b15023b1855da1cf5213b061dc626cc2.exe
File Type:	data
Category:	dropped
Size (bytes):	190
Entropy (8bit):	3.455918016210675
Encrypted:	false
SSDEEP:	3:8uRkiglZlvq5UfKl8lGjLlAdVdhOEjl3QlMIolCl761EC6l4BY7QlAldal:7glZoKfK4XUEZglJPZ7BR716l
MD5:	5D0D1DE1B06B58890AA881EE518BAB84
SHA1:	B1F30C5D5D21BE9A75C1265DE6ABAD72611776DC
SHA-256:	10094922198B9938D46607B73B5433DC47FB4160C7076750F5E7650D07EFE80C
SHA-512:	BC8A58F6BB7241DE9A365AEE00ADFB60B18E5DD067F403BE93DBF30D0B72B3719174D9123A6FFCB60DA712ED09D3179973759B453D94E7DFAE0DCE8DBAA6C 716
Malicious:	**true**
Reputation:	low
Preview:	[.I.n.t.e.r.n.e.t.S.h.o.r.t.c.u.t.]...U.R.L.=.f.i.l.e.:././.C.:.\.U.s.e.r.s.\.e.n.g.i.n.e.e.r.\.A.p.p.D.a.t.a.\.R.o.a.m.i.n.g.\.e.z.o.c.x.c.v.g.g.g.\.x.j.y.x.i.b.e.i.f.b.d.m.o.c.k...e.x.e.

C:\Users\user\AppData\Roaming\ezocxcvggg\xjyxibeifbdmock.exe	
Process:	C:\Users\user\Desktop\b15023b1855da1cf5213b061dc626cc2.exe
File Type:	PE32 executable (GUI) Intel 80386, for MS Windows
Category:	dropped
Size (bytes):	686593
Entropy (8bit):	7.284334525538713
Encrypted:	false
SSDEEP:	12288:3oNmzNhvQsYo9skrJouKDudlPRhirRCb8yyWHpd8Z8WQdQScE+G41AFQixYmw8Yw:4NWNhxi6JoDkirQHLC
MD5:	C0962CFBB4BB43348708437D8CD1D8EF
SHA1:	B726A0128783D7C503890C564A094A997095B2DE
SHA-256:	58B4B3850B7B808CC7C1370A5B42324E2624C137DDC15E24C39FAB2D4B60DE4E
SHA-512:	90F2E67C73F983BCBD941E09A0319241758BE5F0C64B0F4D4E6791275D966C18A75132ED3C0C5C74B12D5CE7CF70FB2313D8F8D64293D4E3FB1B5B065938BA4
Malicious:	**true**
Antivirus:	• Antivirus: Avira, Detection: 100% • Antivirus: Joe Sandbox ML, Detection: 100% • Antivirus: ReversingLabs, Detection: 62%
Reputation:	low
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....V.0...^...^...^.....^....^.....^.....^.).]...^.).[...^.).Z...^.....^...._.H.^..Z...^. ....^.....^..\...^.Rich..^.....PE..L....Ss\.....@.....@.....k..(.....q.....d..... ....d..@.....text..... ..`.rdata...a.....b.....@..@.data....m.....d...X.....@....gfids.....@..@.rsrc...q..... .....@..@.reloc.....j.....@..B..... .....

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386, for MS Windows
Entropy (8bit):	7.284337932398097
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:	b15023b1855da1cf5213b061dc626cc2.exe
File size:	686592
MD5:	ac5eb6172c287cbb954954b56586653f
SHA1:	3bb19910b89a39274957959dec593964bcf12ee4
SHA256:	da23b9268823cc4bcc82fdc74b6bd9c5d8493347507f111 de7c387cbe215b264

General

SHA512:	55f33dc500a7c5ebac4efe9cc8399ec638afe6f9306cb18779825b7b82b5926a5c14f8f04ef8e9967640b3ea810dcf13587c9c15c064ab79ea1719e74620da89
SSDEEP:	12288:3oNmzNhvQsYo9skrJouKDudlPRhirRCb8yyWHpd8Z8WQdQScE+G41AFQixYmw8Yw:4NWNhxi6JoDkirQHLC
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....V.0...^...^...^.....^.....^.....^.).]...^.).[...^.).Z...^.....^..._.H.^...Z...^.....^.....^...\...^.Rich..^.....

File Icon

Icon Hash:	00828e8e8686b000

Static PE Info

General

Entrypoint:	0x4013b4
Entrypoint Section:	.text
Digitally signed:	false
Imagebase:	0x400000
Subsystem:	windows gui
Image File Characteristics:	32BIT_MACHINE, EXECUTABLE_IMAGE
DLL Characteristics:	TERMINAL_SERVER_AWARE, DYNAMIC_BASE
Time Stamp:	0x5C7353AD [Mon Feb 25 02:32:13 2019 UTC]
TLS Callbacks:	
CLR (.Net) Version:	
OS Version Major:	5
OS Version Minor:	1
File Version Major:	5
File Version Minor:	1
Subsystem Version Major:	5
Subsystem Version Minor:	1
Import Hash:	90e4fdc68b40f6ba9c12d9eb0cf8a434

Entrypoint Preview

Instruction
call 00007FDF0CB710BFh
jmp 00007FDF0CB70CC3h
push ebp
push esp
pop ebp
mov eax, dword ptr [0041DC28h]
and eax, 1Fh
push 00000020h
pop ecx
sub ecx, eax
mov eax, dword ptr [ebp+08h]
ror eax, cl
xor eax, dword ptr [0041DC28h]
pop ebp
ret
push ebp
mov ebp, esp
mov eax, dword ptr [ebp+08h]
push esi
mov ecx, dword ptr [eax+3Ch]
add ecx, eax
movzx eax, word ptr [ecx+14h]
lea edx, dword ptr [ecx+18h]
add edx, eax

Instruction
movzx eax, word ptr [ecx+06h]
imul esi, eax, 28h
add esi, edx
cmp edx, esi
je 00007FDF0CB70E4Bh
mov ecx, dword ptr [ebp+0Ch]
cmp ecx, dword ptr [edx+0Ch]
jc 00007FDF0CB70E3Ch
mov eax, dword ptr [edx+08h]
add eax, dword ptr [edx+0Ch]
cmp ecx, eax
jc 00007FDF0CB70E3Eh
add edx, 28h
cmp edx, esi
jne 00007FDF0CB70E1Ch
xor eax, eax
pop esi
pop ebp
ret
push edx
pop eax
jmp 00007FDF0CB70E2Bh
call 00007FDF0CB71566h
or eax, eax
jne 00007FDF0CB70E35h
xor al, al
ret
mov eax, dword ptr fs:[00000018h]
push esi
mov esi, 0041E3B8h
mov edx, dword ptr [eax+04h]
jmp 00007FDF0CB70E36h
cmp edx, eax
je 00007FDF0CB70E42h
xor eax, eax
mov ecx, edx
lock cmpxchg dword ptr [esi], ecx
or eax, eax
jne 00007FDF0CB70E22h
xor al, al
pop esi
ret
mov al, 01h
pop esi
ret
push ebp
push esp
pop ebp
cmp dword ptr [ebp+08h], 00000000h
jne 00007FDF0CB70E39h
mov byte ptr [0041E3D4h], 00000001h
call 00007FDF0CB71387h
call 00007FDF0CB7180Dh
test al, al
jne 00007FDF0CB70E36h
xor al, al
pop ebp
ret
call 00007FDF0CB7459Ch

Rich Headers

Programming Language:	• [LNK] VS2015 UPD3.1 build 24215 • [C] VS2015 UPD3.1 build 24215 • [RES] VS2015 UPD3 build 24213 • [IMP] VS2008 SP1 build 30729

Data Directories

Name	Virtual Address	Virtual Size	Is in Section
IMAGE_DIRECTORY_ENTRY_EXPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IMPORT	0x16bc4	0x28	.rdata
IMAGE_DIRECTORY_ENTRY_RESOURCE	0x20000	0x8aa71	.rsrc
IMAGE_DIRECTORY_ENTRY_EXCEPTION	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_SECURITY	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_BASERELOC	0xab000	0xea0	.reloc
IMAGE_DIRECTORY_ENTRY_DEBUG	0x164c0	0x1c	.rdata
IMAGE_DIRECTORY_ENTRY_COPYRIGHT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_GLOBALPTR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_TLS	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_LOAD_CONFIG	0x164e0	0x40	.rdata
IMAGE_DIRECTORY_ENTRY_BOUND_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_IAT	0x11000	0x100	.rdata
IMAGE_DIRECTORY_ENTRY_DELAY_IMPORT	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_COM_DESCRIPTOR	0x0	0x0	
IMAGE_DIRECTORY_ENTRY_RESERVED	0x0	0x0	

Sections

Name	Virtual Address	Virtual Size	Raw Size	Xored PE	ZLIB Complexity	File Type	Entropy	Characteristics
.text	0x1000	0xf084	0xf200	False	0.603305785124	data	6.68957843183	IMAGE_SCN_MEM_EXECUTE, IMAGE_SCN_CNT_CODE, IMAGE_SCN_MEM_READ
.rdata	0x11000	0x6182	0x6200	False	0.488839285714	data	5.26425207809	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.data	0x18000	0x6de4	0x6400	False	0.7000390625	data	7.02752055826	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_WRITE, IMAGE_SCN_MEM_READ
.gfids	0x1f000	0xac	0x200	False	0.271484375	data	1.40771783792	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.rsrc	0x20000	0x8aa71	0x8ac00	False	0.654043496622	data	7.15231003865	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_READ
.reloc	0xab000	0xea0	0x1000	False	0.75732421875	data	6.27766449099	IMAGE_SCN_CNT_INITIALIZED_DATA, IMAGE_SCN_MEM_DISCARDABLE, IMAGE_SCN_MEM_READ

Resources

Name	RVA	Size	Type	Language	Country
RT_RCDATA	0x2013c	0x8a400	data		
RT_RCDATA	0xaa53c	0xf0	ASCII text, with no line terminators		
RT_VERSION	0xaa62c	0x2c8	data	English	United States
RT_MANIFEST	0xaa8f4	0x17d	XML 1.0 document text	English	United States

Imports

DLL	Import
KERNEL32.dll	QueryPerformanceCounter, GetCurrentProcessId, GetCurrentThreadId, GetSystemTimeAsFileTime, InitializeSListHead, IsDebuggerPresent, UnhandledExceptionFilter, SetUnhandledExceptionFilter, GetStartupInfoW, IsProcessorFeaturePresent, GetModuleHandleW, GetCurrentProcess, TerminateProcess, RtlUnwind, GetLastError, SetLastError, EnterCriticalSection, LeaveCriticalSection, DeleteCriticalSection, InitializeCriticalSectionAndSpinCount, TlsAlloc, TlsGetValue, TlsSetValue, TlsFree, FreeLibrary, GetProcAddress, LoadLibraryExW, GetStdHandle, WriteFile, GetModuleFileNameA, MultiByteToWideChar, WideCharToMultiByte, ExitProcess, GetModuleHandleExW, GetACP, HeapFree, HeapAlloc, CloseHandle, LCMapStringW, GetFileType, SetFilePointerEx, FindClose, FindFirstFileExA, FindNextFileA, IsValidCodePage, GetOEMCP, GetCPInfo, GetCommandLineA, GetCommandLineW, GetEnvironmentStringsW, FreeEnvironmentStringsW, SetStdHandle, GetStringTypeW, GetProcessHeap, FlushFileBuffers, GetConsoleCP, GetConsoleMode, HeapSize, HeapReAlloc, WriteConsoleW, CreateFileW, DecodePointer, RaiseException

Version Infos

Description	Data
LegalCopyright	Copyright (C) Scanderbeg 2018
InternalName	biosterin.exe
FileVersion	8.6.1.1

Description	Data
CompanyName	supertension
ProductName	tend
ProductVersion	4.4.2.6
FileDescription	generously
OriginalFilename	Skivvies.exe
Translation	0x0409 0x04b0

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: b15023b1855da1cf5213b061dc626cc2.exe PID: 6432 Parent PID: 5940

General

Start time:	12:03:16
Start date:	19/11/2020

Path:	C:\Users\user\Desktop\b15023b1855da1cf5213b061dc626cc2.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\b15023b1855da1cf5213b061dc626cc2.exe'
Imagebase:	0xa30000
File size:	686592 bytes
MD5 hash:	AC5EB6172C287CBB954954B56586653F
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000000.00000002.368012063.0000000032130000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000000.00000002.368012063.0000000032130000.00000004.00000001.sdmp, Author: Joe Security • Rule: HawkEyev9, Description: HawkEye v9 Payload, Source: 00000000.00000002.368012063.0000000032130000.00000004.00000001.sdmp, Author: ditekshen
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	A4BFFD	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	A4BFFD	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	A4BFFD	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	A4BFFD	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	A4BFFD	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	A4BFFD	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	A4BFFD	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	A4BFFD	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	A4BFFD	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	A4BFFD	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	A4BFFD	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	A4BFFD	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	A4BFFD	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	A4BFFD	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	A4BFFD	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	A4BFFD	ReadFile

Analysis Process: RegAsm.exe PID: 6476 Parent PID: 6432

General

Start time:	12:03:24
Start date:	19/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\b15023b1855da1cf5213b061dc626cc2.exe'
Imagebase:	0xdd0000
File size:	53248 bytes
MD5 hash:	529695608EAFBED00ACA9E61EF333A7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000001.00000002.608241206.00000000035AF000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000001.00000002.606017869.00000000033C9000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000001.00000002.606017869.00000000033C9000.00000004.00000001.sdmp, Author: Joe Security • Rule: APT_NK_BabyShark_KimJoingRAT_Apr19_1, Description: Detects BabyShark KimJongRAT, Source: 00000001.00000002.608991770.00000000053B0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000001.00000002.608991770.00000000053B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000001.00000002.608991770.00000000053B0000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000001.00000002.609395469.0000000006F61000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000001.00000002.609395469.0000000006F61000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000001.00000002.606262904.0000000003472000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000001.00000003.361093839.0000000004C23000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000001.00000003.361093839.0000000004C23000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000001.00000002.602404324.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000001.00000002.602404324.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Local\Temp\tmp992B.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	83F04A0	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmp92CE.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	83F04A0	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp992B.tmp	success or wait	1	83F08AE	DeleteFileW

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	8173	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	8173	end of file	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	8173	end of file	1	72FE5544	unknown

Analysis Process: vbc.exe PID: 6576 Parent PID: 6476

General

Start time:	12:03:28
Start date:	19/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe' /stext 'C:\Users\user\AppData\Local\Temp\tmp992B.tmp'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000002.00000002.370197886.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmp992B.tmp	unknown	2	ff fe	..	success or wait	1	4089B9	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	100	success or wait	1	416F3E	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	2048	success or wait	1	416F3E	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	2048	success or wait	1	416F3E	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	2048	success or wait	1	416F3E	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	100	success or wait	1	416F3E	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	2048	success or wait	1	416F3E	ReadFile

Analysis Process: xjyxibeifbdmock.exe PID: 6828 Parent PID: 3440

General

Start time:	12:03:35
Start date:	19/11/2020
Path:	C:\Users\user\AppData\Roaming\ezocxcvggg\xjyxibeifbdmock.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\ezocxcvggg\xjyxibeifbdmock.exe'
Imagebase:	0x150000
File size:	686593 bytes
MD5 hash:	C0962CFBB4BB43348708437D8CD1D8EF
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000004.00000002.403557593.0000000031EE0000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000004.00000002.403557593.0000000031EE0000.00000004.00000001.sdmp, Author: Joe Security • Rule: HawkEyev9, Description: HawkEye v9 Payload, Source: 00000004.00000002.403557593.0000000031EE0000.00000004.00000001.sdmp, Author: ditekshen
Antivirus matches:	• Detection: 100%, Avira • Detection: 100%, Joe Sandbox ML • Detection: 62%, ReversingLabs
Reputation:	low

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	16BFFD	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	16BFFD	ReadFile
C:\Users\user\AppData\Roaming\ezocxcvggg\xjyxibeifbdmock.exe	0	686593	success or wait	1	10D003D	NtReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	16BFFD	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	16BFFD	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	16BFFD	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	16BFFD	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	16BFFD	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	16BFFD	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	16BFFD	ReadFile
C:\Windows\SysWOW64\ntdll.dll	unknown	1622408	success or wait	1	16BFFD	ReadFile

Analysis Process: RegAsm.exe PID: 6852 Parent PID: 6828

General

Start time:	12:03:42
Start date:	19/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\RegAsm.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\AppData\Roaming\ezocxcvggg\xjyxibeifbdmock.exe'
Imagebase:	0x720000
File size:	53248 bytes
MD5 hash:	529695608EAFBED00ACA9E61EF333A7C
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET

Yara matches:	• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000005.00000002.606139905.0000000002DD2000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000005.00000002.608017137.0000000002F0D000.00000004.00000001.sdmp, Author: Joe Security • Rule: APT_NK_BabyShark_KimJoingRAT_Apr19_1, Description: Detects BabyShark KimJongRAT, Source: 00000005.00000002.608578652.0000000004D10000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000005.00000002.608578652.0000000004D10000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000005.00000002.608578652.0000000004D10000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000005.00000003.397841054.0000000004583000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000005.00000003.397841054.0000000004583000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000005.00000002.605834694.0000000002D29000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000005.00000002.605834694.0000000002D29000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000005.00000002.609144823.00000000068B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000005.00000002.609144823.00000000068B1000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000005.00000002.602420435.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000005.00000002.602420435.0000000000402000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Created

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol
C:\Users\user	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Roaming	read data or list directory | synchronize	device	directory file | synchronous io non alert | open for backup ident | open reparse point	object name collision	1	72FB60AC	unknown
C:\Users\user\AppData\Local\Temp\tmpDC10.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7E401D8	GetTempFileNameW
C:\Users\user\AppData\Local\Temp\tmpD611.tmp	read attributes | synchronize | generic read	device	synchronous io non alert | non directory file	success or wait	1	7E401D8	GetTempFileNameW

File Deleted

File Path	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpDC10.tmp	success or wait	1	7E408A2	DeleteFileW

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	6304	success or wait	3	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	8173	end of file	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	8173	end of file	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\CONFIG\machine.config	unknown	4095	success or wait	1	72FE8738	ReadFile
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	4095	success or wait	1	72FE5544	unknown
C:\Windows\Microsoft.NET\Framework\v2.0.50727\regasm.exe.config	unknown	8173	end of file	1	72FE5544	unknown
C:\Users\user\AppData\Local\Temp\tmpDC10.tmp	unknown	4096	end of file	1	7E407E3	ReadFile
C:\Users\user\AppData\Local\Temp\tmpDC10.tmp	unknown	4096	success or wait	60	7E407E3	ReadFile
C:\Users\user\AppData\Local\Temp\tmpDC10.tmp	unknown	4096	end of file	60	7E407E3	ReadFile
C:\Users\user\AppData\Local\Temp\tmpD611.tmp	unknown	4096	end of file	29	7E407E3	ReadFile

Analysis Process: vbc.exe PID: 6948 Parent PID: 6852

General

Start time:	12:03:45
Start date:	19/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe' /stext 'C:\Users\user\AppData\Local\Temp\tmpDC10.tmp'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000006.00000002.405206241.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

File Path	Access	Attributes	Options	Completion	Count	Source Address	Symbol

File Written

File Path	Offset	Length	Value	Ascii	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Temp\tmpDC10.tmp	unknown	2	ff fe	..	success or wait	1	4089B9	WriteFile

File Read

File Path	Offset	Length	Completion	Count	Source Address	Symbol
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	100	success or wait	1	416F3E	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	2048	success or wait	1	416F3E	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	2048	success or wait	1	416F3E	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Web Data	unknown	2048	success or wait	1	416F3E	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	100	success or wait	1	416F3E	ReadFile
C:\Users\user\AppData\Local\Google\Chrome\User Data\Default\Login Data	unknown	2048	success or wait	1	416F3E	ReadFile

Analysis Process: vbc.exe PID: 6280 Parent PID: 6476

General

Start time:	12:04:32
Start date:	19/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe' /stext 'C:\Users\user\AppData\Local\Temp\tmp92CE.tmp'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: APT_NK_BabyShark_KimJoingRAT_Apr19_1, Description: Detects BabyShark KimJongRAT, Source: 0000000D.00000002.502433502.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 0000000D.00000002.502433502.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Analysis Process: vbc.exe PID: 3252 Parent PID: 6852

General

Start time:	12:04:49
Start date:	19/11/2020
Path:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe' /stext 'C:\Users\user\AppData\Local\Temp\tmpD611.tmp'
Imagebase:	0x400000
File size:	1171592 bytes
MD5 hash:	C63ED21D5706A527419C9FBD730FFB2E
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Yara matches:	• Rule: APT_NK_BabyShark_KimJoingRAT_Apr19_1, Description: Detects BabyShark KimJongRAT, Source: 00000013.00000002.540468694.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000013.00000002.540468694.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

Disassembly

Code Analysis