ID: 474426
Sample Name: 60L3nw00Uk
Cookbook: default.jbs
Time: 23:48:21
Date: 30/08/2021
Version: 33.0.0 White Diamond

Table of Contents

Table of Contents 2
Windows Analysis Report 60L3nw00Uk 4
Overview 4
General Information 4
Detection 4
Signatures 4
Classification 4
Process Tree 4
Malware Configuration 4
Yara Overview 4
Memory Dumps 4
Unpacked PEs 5
Sigma Overview 5
Jbx Signature Overview 5
AV Detection: 5
Key, Mouse, Clipboard, Microphone and Screen Capturing: 5
System Summary: 5
Data Obfuscation: 5
Boot Survival: 5
Malware Analysis System Evasion: 6
HIPS / PFW / Operating System Protection Evasion: 6
Stealing of Sensitive Information: 6
Remote Access Functionality: 6
Mitre Att&ck Matrix 6
Behavior Graph 7
Screenshots 7
Thumbnails 7
Antivirus, Machine Learning and Genetic Malware Detection 8
Initial Sample 8
Dropped Files 8
Unpacked PE Files 8
Domains 8
URLs 9
Domains and IPs 9
Contacted Domains 9
URLs from Memory and Binaries 9
Contacted IPs 9
General Information 9
Simulations 10
Behavior and APIs 10
Joe Sandbox View / Context 10
IPs 10
Domains 10
ASN 10
JA3 Fingerprints 10
Dropped Files 10
Created / dropped Files 10
Static File Info 13
General 13
File Icon 13
Network Behavior 13
Code Manipulations 13
Statistics 13
Behavior 13
System Behavior 13
Analysis Process: 60L3nw00Uk.exe PID: 312 Parent PID: 5792 13
General 14
File Activities 14
File Created 14
File Deleted 14
File Written 14
File Read 14
Analysis Process: schtasks.exe PID: 6832 Parent PID: 312 14
General 14
File Activities 14
Analysis Process: conhost.exe PID: 6880 Parent PID: 6832 14
General 15
Analysis Process: 60L3nw00Uk.exe PID: 6848 Parent PID: 312 15
General 15
File Activities 15
File Created 15
File Deleted 16
File Written 16
File Read 16
Analysis Process: vbc.exe PID: 7024 Parent PID: 6848 16
General 16

Copyright Joe Security LLC 2021

File Activities 16
File Created 16
File Deleted 16
File Written 16
File Read 16
Analysis Process: vbc.exe PID: 5260 Parent PID: 6848 16
General 16
Disassembly 17
Code Analysis 17

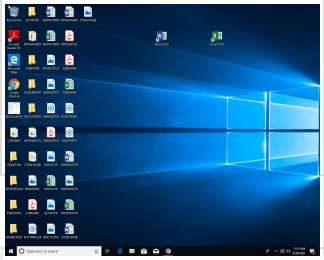
Windows Analysis Report 60L3nw00Uk

Overview

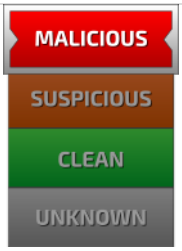
General Information

Sample Name:	60L3nw00Uk (renamed file extension from none to exe)
Analysis ID:	474426
MD5:	1e6ec142ba08c7..
SHA1:	6b52334ca53b1c..
SHA256:	e773f60aeb241f8..
Tags:	exe HawkEye
Infos:	

Most interesting Screenshot:



Detection



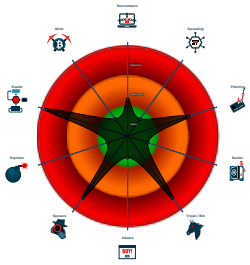
HawkEye
MailPassView

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

Signatures

- Yara detected MailPassView
- Multi AV Scanner detection for subm…
- Yara detected HawkEye Keylogger
- Malicious sample detected (through …
- Yara detected AntiVM3
- Detected HawkEye Rat
- Multi AV Scanner detection for dropp…
- Sample uses process hollowing tech…
- Writes to foreign memory regions
- .NET source code references suspic…
- Tries to detect sandboxes and other…
- Tries to steal Mail credentials (via fil…

Classification



Process Tree

- **System is w10x64**
- 60L3nw00Uk.exe (PID: 312 cmdline: 'C:\Users\user\Desktop\60L3nw00Uk.exe' MD5: 1E6EC142BA08C7DEAFD25BDEA76F32D4)
  - schtasks.exe (PID: 6832 cmdline: 'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\UaoePQDdm' /XML 'C:\Users\user\AppData\Local\Temp\tmp16F.tmp' MD5: 15FF7D8324231381BAD48A052F85DF04)
    - conhost.exe (PID: 6880 cmdline: C:\Windows\system32\conhost.exe 0xffffffff -ForceV1 MD5: EA777DEEA782E8B4D7C7C33BBF8A4496)
  - 60L3nw00Uk.exe (PID: 6848 cmdline: C:\Users\user\Desktop\60L3nw00Uk.exe MD5: 1E6EC142BA08C7DEAFD25BDEA76F32D4)
    - vbc.exe (PID: 7024 cmdline: 'C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe' /stext 'C:\Users\user\AppData\Local\Temp\tmp9B04.tmp' MD5: C63ED21D5706A527419C9FBD730FFB2E)
    - vbc.exe (PID: 5260 cmdline: 'C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe' /stext 'C:\Users\user\AppData\Local\Temp\tmp9795.tmp' MD5: C63ED21D5706A527419C9FBD730FFB2E)
- **cleanup**

Malware Configuration

No configs have been found

Yara Overview

Memory Dumps

Source	Rule	Description	Author	Strings
00000002.00000002.381558466.000000000398 7000.00000004.00000001.sdmp	MAL_HawkEye_Keylogger _Gen_Dec18	Detects HawkEye Keylogger Reborn	Florian Roth	• 0x15d586:$s1: HawkEye Keylogger • 0x15d5ef:$s1: HawkEye Keylogger • 0x1569c9:$s2: _ScreenshotLogger • 0x156996:$s3: _PasswordStealer
00000002.00000002.381558466.000000000398 7000.00000004.00000001.sdmp	JoeSecurity_HawkEye	Yara detected HawkEye Keylogger	Joe Security	
00000016.00000002.523503971.000000000040 0000.00000040.00000001.sdmp	APT_NK_BabyShark_KimJ oingRAT_Apr19_1	Detects BabyShark KimJongRAT	Florian Roth	• 0x147b0:$a1: logins.json • 0x14710:$s3: SELECT id, hostname, httpRealm, formSubmitURL, usernameField, passwordField, encryptedUsername, encryptedPassword FROM moz_login • 0x14f34:$s4: \mozsqlite3.dll • 0x137a4:$s5: SMTP Password

Copyright Joe Security LLC 2021

Source	Rule	Description	Author	Strings
00000016.00000002.523503971.000000000040 0000.00000040.00000001.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
00000006.00000002.605633875.0000000002E0 F000.00000004.00000001.sdmp	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
Click to see the 21 entries				

Unpacked PEs

Source	Rule	Description	Author	Strings
6.3.60L3nw00Uk.exe.4565bd5.0.unpack	JoeSecurity_WebBrowserPassView	Yara detected WebBrowserPassView password recovery tool	Joe Security	
6.3.60L3nw00Uk.exe.45bdbda.1.unpack	APT_NK_BabyShark_KimJoingRAT_Apr19_1	Detects BabyShark KimJongRAT	Florian Roth	• 0x11bb0:$a1: logins.json • 0x11b10:$s3: SELECT id, hostname, httpRealm, formSubmitURL, usernameField, passwordField, encrypteUsername, encryptedPassword FROM moz_login • 0x12334:$s4: \mozsqlite3.dll • 0x115a4:$s5: SMTP Password
6.3.60L3nw00Uk.exe.45bdbda.1.unpack	JoeSecurity_MailPassView	Yara detected MailPassView	Joe Security	
2.2.60L3nw00Uk.exe.3a5c958.1.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
2.2.60L3nw00Uk.exe.3a5c958.1.unpack	SUSP_NET_NAME_ConfuserEx	Detects ConfuserEx packed file	Arnim Rupp	• 0x85801:$name: ConfuserEx • 0x8450e:$compile: AssemblyTitle
Click to see the 39 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

Multi AV Scanner detection for dropped file

Key, Mouse, Clipboard, Microphone and Screen Capturing:

Yara detected HawkEye Keylogger

System Summary:

Malicious sample detected (through community Yara rule)

Data Obfuscation:

.NET source code contains potential unpacker

Boot Survival:

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

Copyright Joe Security LLC 2021

Malware Analysis System Evasion:

- Yara detected AntiVM3
- Tries to detect sandboxes and other dynamic analysis tools (process name or module or function)
- Queries sensitive network adapter information (via WMI, Win32_NetworkAdapter, often done to detect virtual machines)

HIPS / PFW / Operating System Protection Evasion:

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

Stealing of Sensitive Information:

- Yara detected MailPassView
- Yara detected HawkEye Keylogger
- Tries to steal Mail credentials (via file registry)
- Yara detected WebBrowserPassView password recovery tool
- Tries to steal Mail credentials (via file access)
- Tries to steal Instant Messenger accounts or passwords
- Tries to harvest and steal browser information (history, passwords, etc)

Remote Access Functionality:

- Yara detected HawkEye Keylogger
- Detected HawkEye Rat

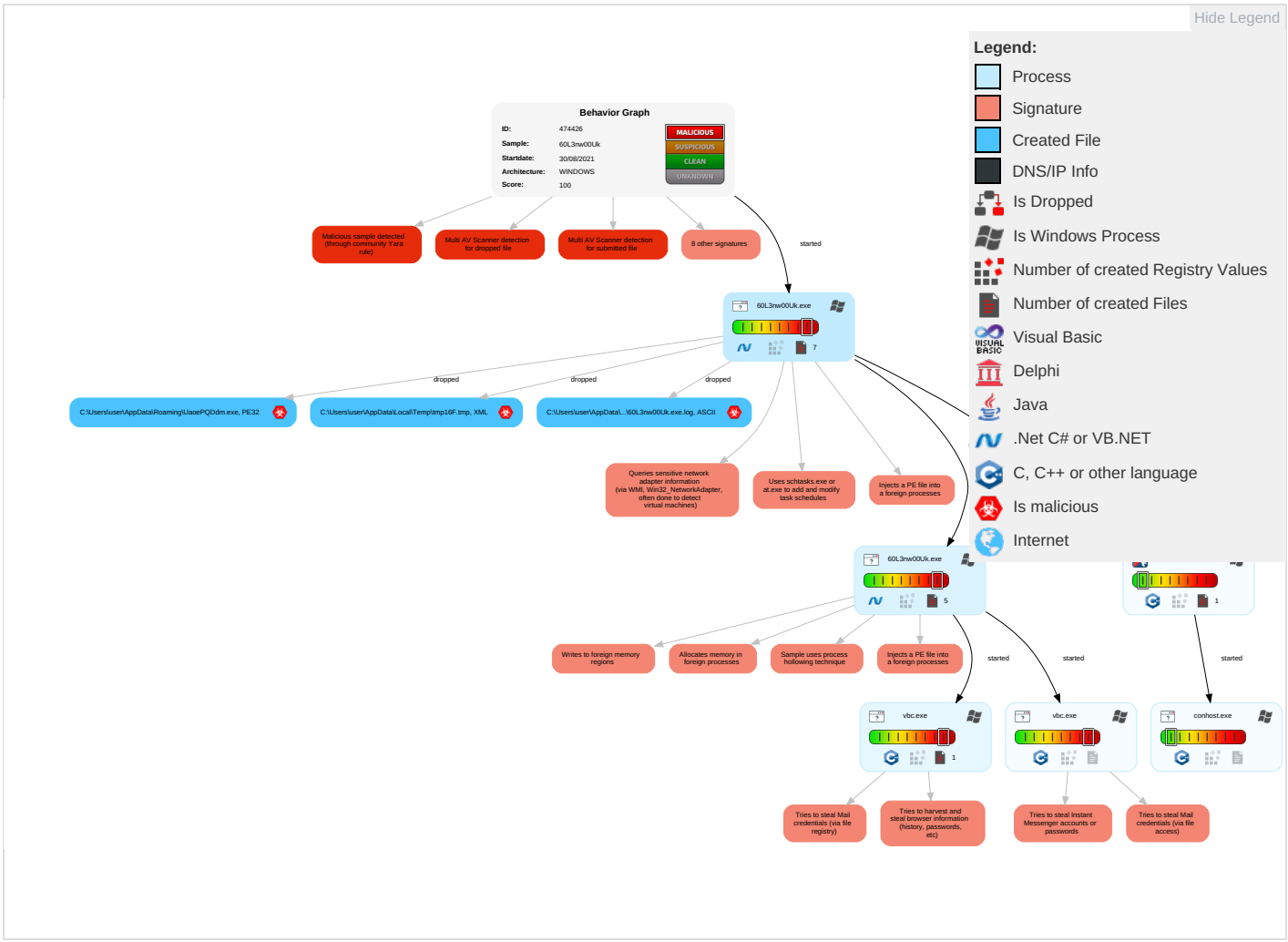
Mitre Att&ck Matrix

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	Application Shimming 1	Application Shimming 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	Scheduled Task/Job 1	Process Injection 4 1 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	Logon Script (Windows)	Scheduled Task/Job 1	Obfuscated Files or Information 3	Credentials In Files 1	File and Directory Discovery 2	SMB/Windows Admin Shares	Email Collection 1	Automated Exfiltration	Steganograp
Local Accounts	Scheduled Task/Job 1	Logon Script (Mac)	Logon Script (Mac)	Software Packing 1 3	NTDS	System Information Discovery 1 9	Distributed Component Object Model	Clipboard Data 1	Scheduled Transfer	Protocol Impersonatio
Cloud Accounts	Cron	Network Logon Script	Network Logon Script	Masquerading 1	LSA Secrets	Security Software Discovery 3 3 1	SSH	Keylogging	Data Transfer Size Limits	Fallback Channels
Replication Through Removable Media	Launchd	Rc.common	Rc.common	Virtualization/Sandbox Evasion 1 3 1	Cached Domain Credentials	Virtualization/Sandbox Evasion 1 3 1	VNC	GUI Input Capture	Exfiltration Over C2 Channel	Multiband Communicati
External Remote Services	Scheduled Task	Startup Items	Startup Items	Process Injection 4 1 1	DCSync	Process Discovery 3	Windows Remote Management	Web Portal Capture	Exfiltration Over Alternative Protocol	Commonly Used Port

Copyright Joe Security LLC 2021

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	Command and Scripting Interpreter	Scheduled Task/Job	Scheduled Task/Job	Indicator Removal from Tools	Proc Filesystem	System Owner/User Discovery 1	Shared Webroot	Credential API Hooking	Exfiltration Over Symmetric Encrypted Non-C2 Protocol	Application Layer Protoc

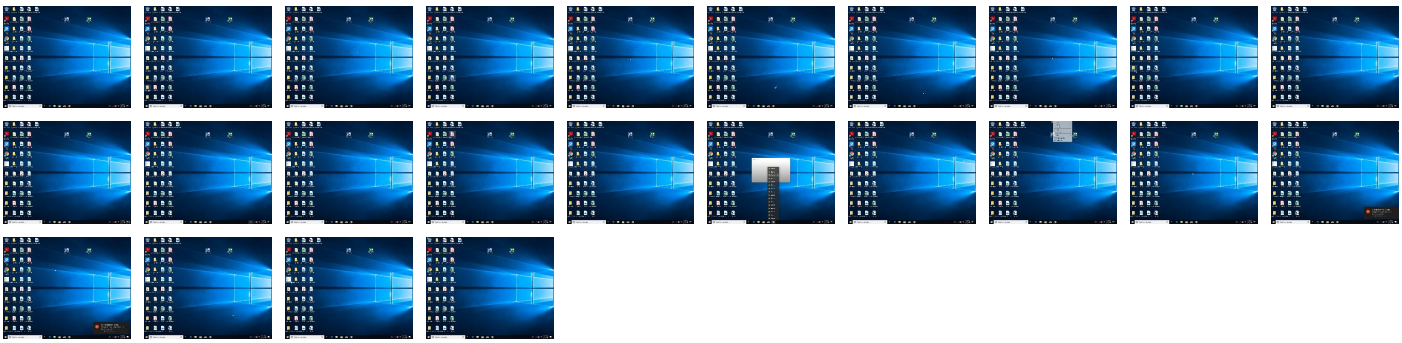
Behavior Graph



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
60L3nw00Uk.exe	26%	Metadefender		Browse
60L3nw00Uk.exe	65%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Dropped Files

Source	Detection	Scanner	Label	Link
C:\Users\user\AppData\Roaming\UaoePQDdm.exe	26%	Metadefender		Browse
C:\Users\user\AppData\Roaming\UaoePQDdm.exe	65%	ReversingLabs	ByteCode-MSIL.Trojan.AgentTesla	

Unpacked PE Files

Source	Detection	Scanner	Label	Link	Download
6.2.60L3nw00Uk.exe.400000.0.unpack	100%	Avira	TR/Dropper.Gen		Download File
7.2.vbc.exe.400000.0.unpack	100%	Avira	HEUR/AGEN.1125438		Download File

Domains

No Antivirus matches

Copyright Joe Security LLC 2021

URLs

Source	Detection	Scanner	Label	Link
http://https://deff.nelreports.net/api/report?cat=msn	0%	URL Reputation	safe	
http://https://mem.gfx.ms/me/MeControl/10.19168.0/en-US/meCore.min.js	0%	URL Reputation	safe	
http://www.sajatypeworks.com	0%	URL Reputation	safe	
http://www.founder.com.cn/cn/cThe	0%	URL Reputation	safe	
http://images.outbrainimg.com/transform/v3/eyJpdSI6Ijk4OGQ1ZDgwMWE2ODQ2NDNkM2ZkMmYyMGEwOTgwMWQ3MDE2Z	0%	Avira URL Cloud	safe	
http://https://a.pomf.cat/	0%	Avira URL Cloud	safe	
http://crl.pki.goog/GTS1O1core.crl0	0%	URL Reputation	safe	
http://www.fontbureau.com-	0%	Avira URL Cloud	safe	
http://www.galapagosdesign.com/DPlease	0%	URL Reputation	safe	
http://www.fontbureau.comuevaq	0%	Avira URL Cloud	safe	
http://www.urwpp.deDPlease	0%	URL Reputation	safe	
http://www.zhongyicts.com.cn	0%	URL Reputation	safe	
http://https://img.img-taboola.com/taboola/image/fetch/f_jpg%2Cq_auto%2Ce_sharpen%2Ch_311%2Cw_207%2Cc_fill%	0%	URL Reputation	safe	
http://images.outbrainimg.com/transform/v3/eyJpdSI6ImQ1Y2M3ZjUxNTk0ZjI1ZWI5NjQxNjllMjcxMDliYzA5MWY4N	0%	Avira URL Cloud	safe	
http://pki.goog/gsr2/GTS1O1.crt0	0%	URL Reputation	safe	
http://https://pki.goog/repository/0	0%	URL Reputation	safe	
http://https://mem.gfx.ms/meversion?partner=RetailStore2&market=en-us&uhf=1	0%	URL Reputation	safe	
http://www.carterandcone.coml	0%	URL Reputation	safe	
http://www.tiro.comn-u	0%	Avira URL Cloud	safe	
http://https://mem.gfx.ms/me/MeControl/10.19168.0/en-US/meBoot.min.js	0%	URL Reputation	safe	
http://crl.pki.goog/gsr2/gsr2.crl0?	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTSGIAG3.crt0)	0%	URL Reputation	safe	
http://pki.goog/gsr2/GTS1O1.crt0#	0%	URL Reputation	safe	
http://pomf.cat/upload.php&https://a.pomf.cat/	0%	Avira URL Cloud	safe	
http://www.founder.com.cn/cn/bThe	0%	URL Reputation	safe	
http://www.tiro.com	0%	URL Reputation	safe	
http://www.goodfont.co.kr	0%	URL Reputation	safe	

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:	474426
Start date:	30.08.2021
Start time:	23:48:21
Joe Sandbox Product:	CloudBasic
Overall analysis duration:	0h 11m 56s
Hypervisor based Inspection enabled:	false
Report type:	light
Sample file name:	60L3nw00Uk (renamed file extension from none to exe)

Copyright Joe Security LLC 2021

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:	26
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@10/7@0/0
EGA Information:	Failed
HDC Information:	• Successful, ratio: 97.4% (good quality ratio 94.5%) • Quality average: 85.8% • Quality standard deviation: 23%
HCA Information:	• Successful, ratio: 99% • Number of executed functions: 0 • Number of non-executed functions: 0
Cookbook Comments:	• Adjust boot time • Enable AMSI
Warnings:	Show All

Simulations

Behavior and APIs

Time	Type	Description
23:49:26	API Interceptor	2x Sleep call for process: 60L3nw00Uk.exe modified

Joe Sandbox View / Context

IPs

No context

Domains

No context

ASN

No context

JA3 Fingerprints

No context

Dropped Files

No context

Created / dropped Files

C:\Users\user\AppData\Local\Microsoft\CLR_v4.0_32\UsageLogs\60L3nw00Uk.exe.log	
Process:	C:\Users\user\Desktop\60L3nw00Uk.exe
File Type:	ASCII text, with CRLF line terminators
Category:	modified
Size (bytes):	1216
Entropy (8bit):	5.355304211458859
Encrypted:	false
SSDEEP:	24:MLUE4K5E4Ks2E1qE4qXKDE4KhK3VZ9pKhPKIE4oKFKHKoZAE4Kzr7FE4x84j:MIHK5HKXE1qHiYHKhQnoPtHoxHhAHKzr
MD5:	FED34146BF2F2FA59DCF8702FCC8232E
SHA1:	B03BFEA175989D989850CF06FE5E7BBF56EAA00A
SHA-256:	123BE4E3590609A008E85501243AF5BC53FA0C26C82A92881B8879524F8C0D5C
SHA-512:	1CC89F2ED1DBD70628FA1DC41A32BA0BFA3E81EAE1A1CF3C5F6A48F2DA0BF1F21A5001B8A18B04043C5B8FE4FBE663068D86AA8C4BD8E17933F75687C3178F F6
Malicious:	**true**
Reputation:	high, very likely benign file
Preview:	1,"fusion","GAC",0..1,"WinRT","NotApp",1..2,"System.Windows.Forms, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089",0..3,"System, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System\4f0a7eefa3cd3e0ba98b5ebddbbc72e6\System.ni.dll",0..2,"System.Drawing, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a",0..3,"System.Core, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Core\f1d8480152e0da9a60ad49c6d16a3b6d\System.Core.ni.dll",0..3,"System.Configuration, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Configuration\8d67d92724ba494b6c7fd089d6f25b48\System.Configuration.ni.dll",0..3,"System.Xml, Version=4.0.0.0, Culture=neutral, PublicKeyToken=b77a5c561934e089","C:\Windows\assembly\NativeImages_v4.0.30319_32\System.Xml\b219d4630d26b88041b59c21

C:\Users\user\AppData\Local\Temp\387de725-2380-e2bc-684f-2ef6ffc1f7f9	
Process:	C:\Users\user\Desktop\60L3nw00Uk.exe
File Type:	ASCII text, with no line terminators
Category:	dropped
Size (bytes):	64
Entropy (8bit):	5.06602441389348
Encrypted:	false
SSDEEP:	3:Bpx9fi2SE6ugiZkmrT:Bpx9fxS3vQ
MD5:	D2CB687CF3F90F69C9C5EE8E3232136C
SHA1:	B981B48FC19D78E43B28B3A8852C71CB1C8339B9
SHA-256:	F5F6C8372D06061D8670662374289B3B913BCB5C0FCC26F4C08556619C303ADA
SHA-512:	8C58595AB8ACF547F30A6EF386DDBD72A578ABC0018233D06C3E17F69A2D2DEF1C265437CE87BBD4D668EB4DACC24075B34692E75760206539B8F471AA2535F
Malicious:	false
Reputation:	low
Preview:	GTXq6lZGCzVwlrIPDHEkHHGVJ5dcMJa+E2adbYBKEGTTLAH5l2blnzzJ54Wymmv9

C:\Users\user\AppData\Local\Temp\bhv34B0.tmp	
Process:	C:\Windows\Microsoft.NET\Framework\v2.0.50727\vbc.exe
File Type:	Extensible storage user DataBase, version 0x620, checksum 0xe07be951, page size 32768, DirtyShutdown, Windows version 10.0
Category:	dropped
Size (bytes):	26738688
Entropy (8bit):	0.8752026016464309
Encrypted:	false
SSDEEP:	24576:kg+wP17f2sYFPHihgmKdTnjVccgeTaNX:esY5T
MD5:	E12C1D81734B65D7158F3564AE173818
SHA1:	57AB6A414A22AE6DD0D7A90F5F257F4BFBD2F9AC
SHA-256:	C18D5A6806F58730F504524416E484AB12A0FF2092F24CA3EC346776F9B1C8B5
SHA-512:	368C15D5E97211BB97A080537E6CF1FAD23EFA40EF8DFFF4358560F6A92B3ADE37245D48E3D9C39F60A18CF03AE1483CA43AF19842C052F61E268205A33B6E6E
Malicious:	false
Reputation:	low
Preview:	.{.Q... .....p.....Ef..4...w.....%.....1...y...1...y).h.'.....W.4...w.....[.....B..... ....1...y..... .....1...y.w...../..`.1...y)..... .....

C:\Users\user\AppData\Local\Temp\tmp16F.tmp	
Process:	C:\Users\user\Desktop\60L3nw00Uk.exe
File Type:	XML 1.0 document, ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	1654
Entropy (8bit):	5.155096980221409
Encrypted:	false
SSDEEP:	24:2dH4+SEqC/S7h2ulNMFp2O/rlMhEMjnGpwjpIgUYODOLD9RJh7h8gKB35tn:cbha7JlNQV/rydbz9I3YODOLNdq3h

C:\Users\user\AppData\Local\Temp\tmp16F.tmp	
MD5:	D366A6E1AB4A8F27DFEFC6E0B22E626B
SHA1:	9E3D3561C5EA98AB3874402375E1C106830509ED
SHA-256:	2345F5458DA189D397660707855E1F04880FB57D9DED065FC0FB9028907D389F
SHA-512:	4745C808EAAF878930E7831E413FFDB223A6D83DAFAA8A162A31620907857F3517EBC95B5900A63CC044CC5B7FB3A1282FB470E435363A82A2A9FCBCE836397D
Malicious:	**true**
Reputation:	low
Preview:	<?xml version="1.0" encoding="UTF-16"?>..<Task version="1.2" xmlns="http://schemas.microsoft.com/windows/2004/02/mit/task">.. <RegistrationInfo>.. <Date>2014-10-25T14:27:44.8929027</Date>.. <Author>computer\user</Author>.. </RegistrationInfo>.. <Triggers>.. <LogonTrigger>.. <Enabled>true</Enabled>.. <UserId>computer\user</UserId>.. </LogonTrigger>.. <RegistrationTrigger>.. <Enabled>false</Enabled>.. </RegistrationTrigger>.. </Triggers>.. <Principals>.. <Principal id="Author">.. <UserId>computer\user</UserId>.. <LogonType>InteractiveToken</LogonType>.. <RunLevel>LeastPrivilege</RunLevel>.. </Principal>.. </Principals>.. <Settings>.. <MultipleInstancesPolicy>StopExisting</MultipleInstancesPolicy>.. <DisallowStartIfOnBatteries>false</DisallowStartIfOnBatteries>.. <StopIfGoingOnBatteries>true</StopIfGoingOnBatteries>.. <AllowHardTerminate>false</AllowHardTerminate>.. <StartWhenAvail

C:\Users\user\AppData\Local\Temp\tmp9B04.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
Preview:	..

C:\Users\user\AppData\Roaming\UaoePQDdm.exe	
Process:	C:\Users\user\Desktop\60L3nw00Uk.exe
File Type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Category:	dropped
Size (bytes):	1222144
Entropy (8bit):	7.407764268193867
Encrypted:	false
SSDEEP:	12288:9ObrmTJfbAGG64rJr7MWUXApfe1l3ri7Ta8OFAzRfV/ZH1CFnws3uThJnaSFvpRH:l5NeJnNfe1uri725ID1G3uNMSFxHH/5
MD5:	1E6EC142BA08C7DEAFD25BDEA76F32D4
SHA1:	6B52334CA53B1C604C5865E2AB49056B870808C5
SHA-256:	E773F60AEB241F884B4F932D7DDD4E31C87F31781D5BD53D8583B3D54807A449
SHA-512:	70D7E937546384ECAFD26978C486F7626076DC403EE6B78051BF2A4F5CDA7A9733ABD566FACE813B93D1A6152494B9B57666BFAECD90122C0DFF126116BB492
Malicious:	**true**
Antivirus:	• Antivirus: Metadefender, Detection: 26%, Browse • Antivirus: ReversingLabs, Detection: 65%
Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....$'a.....6... ...@....@.. ....@.....5..W....`..x.....@..... ..... ..H.....text..... ..... ..`.reloc.....@.....@..B.rsr c...x....`.....@..@.....5.....H.....P...X9.....\h.....z.(.....}.....(....o....}....*..*...0.....{.....E.....8...Z...u.....*..}.....].4S }.....}.....*..}..... ..Q.}.....}.....*..}.....{.... Km.a}.....}.....*..}..... ,...}.....}.....*..}.....{.... ..=.a}.....}.....*..}..... ....}.....}.....*..}..... "G.R}.....}.....*..}.....*...{....*.s....z.2.{....5...*....0..<..... {.....3..{....(....o....3...}.....+..s.....{....}..

C:\Users\user\AppData\Roaming\UaoePQDdm.exe:Zone.Identifier	
Process:	C:\Users\user\Desktop\60L3nw00Uk.exe
File Type:	ASCII text, with CRLF line terminators
Category:	dropped
Size (bytes):	26
Entropy (8bit):	3.95006375643621
Encrypted:	false
SSDEEP:	3:ggPYV:rPYV
MD5:	187F488E27DB4AF347237FE461A079AD
SHA1:	6693BA299EC1881249D59262276A0D2CB21F8E64
SHA-256:	255A65D30841AB4082BD9D0EEA79D49C5EE88F56136157D8D6156AEF11C12309
SHA-512:	89879F237C0C051EBE784D0690657A6827A312A82735DA42DAD5F744D734FC545BEC9642C19D14C05B2F01FF53BC731530C92F7327BB7DC9CDE1B60FB21CD64
Malicious:	false
Preview:	[ZoneTransfer]....ZoneId=0

Static File Info

General

File type:	PE32 executable (GUI) Intel 80386 Mono/.Net assembly, for MS Windows
Entropy (8bit):	7.407764268193867
TrID:	• Win32 Executable (generic) Net Framework (10011505/4) 49.80% • Win32 Executable (generic) a (10002005/4) 49.75% • Generic CIL Executable (.NET, Mono, etc.) (73296/58) 0.36% • Windows Screen Saver (13104/52) 0.07% • Generic Win/DOS Executable (2004/3) 0.01%
File name:	60L3nw00Uk.exe
File size:	1222144
MD5:	1e6ec142ba08c7deafd25bdea76f32d4
SHA1:	6b52334ca53b1c604c5865e2ab49056b870808c5
SHA256:	e773f60aeb241f884b4f932d7ddd4e31c87f31781d5bd53d8583b3d54807a449
SHA512:	70d7e937546384ecafd26978c486f7626076dc403ee6b78051bf2a4f5cda7a9733abd566face813b93d1a6152494b9b57666bfaecd90122c0dff126116bb4928
SSDEEP:	12288:9ObrmTJfbAGG64rJr7MWUXApfe1l3ri7Ta8OFAzRfV/ZH1CFnws3uThJnaSFvpRH:l5NeJnNfe1uri725ID1G3uNMSFxHH/5
File Content Preview:	MZ.....@.....!..L.!This program cannot be run in DOS mode....$.....PE..L....$'a.....6... ...@....@.. .....@.....

File Icon

Icon Hash:	4545656561010309

Network Behavior

No network behavior found

Code Manipulations

Statistics

Behavior

Click to jump to process

System Behavior

Analysis Process: 60L3nw00Uk.exe PID: 312 Parent PID: 5792

General

Start time:	23:49:16
Start date:	30/08/2021
Path:	C:\Users\user\Desktop\60L3nw00Uk.exe
Wow64 process (32bit):	true
Commandline:	'C:\Users\user\Desktop\60L3nw00Uk.exe'
Imagebase:	0x420000
File size:	1222144 bytes
MD5 hash:	1E6EC142BA08C7DEAFD25BDEA76F32D4
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	.Net C# or VB.NET
Yara matches:	• Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000002.00000002.381558466.0000000003987000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000002.00000002.381558466.0000000003987000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_AntiVM_3, Description: Yara detected AntiVM_3, Source: 00000002.00000002.380209170.0000000002891000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000002.00000002.382445641.0000000003B17000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000002.00000002.382445641.0000000003B17000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: schtasks.exe PID: 6832 Parent PID: 312

General

Start time:	23:49:35
Start date:	30/08/2021
Path:	C:\Windows\SysWOW64\schtasks.exe
Wow64 process (32bit):	true
Commandline:	'C:\Windows\System32\schtasks.exe' /Create /TN 'Updates\UaoePQDdm' /XML 'C:\Users\user\AppData\Local\Temp\tmp16F.tmp'
Imagebase:	0x70000
File size:	185856 bytes
MD5 hash:	15FF7D8324231381BAD48A052F85DF04
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

File Activities

Show Windows behavior

Analysis Process: conhost.exe PID: 6880 Parent PID: 6832

General

Start time:	23:49:35
Start date:	30/08/2021
Path:	C:\Windows\System32\conhost.exe
Wow64 process (32bit):	false
Commandline:	C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
Imagebase:	0x7ff61de10000
File size:	625664 bytes
MD5 hash:	EA777DEEA782E8B4D7C7C33BBF8A4496
Has elevated privileges:	true
Has administrator privileges:	true
Programmed in:	C, C++ or other language
Reputation:	high

Analysis Process: 60L3nw00Uk.exe PID: 6848 Parent PID: 312

General

Start time:	23:49:36
Start date:	30/08/2021
Path:	C:\Users\user\Desktop\60L3nw00Uk.exe
Wow64 process (32bit):	true
Commandline:	C:\Users\user\Desktop\60L3nw00Uk.exe
Imagebase:	0x8b0000
File size:	1222144 bytes
MD5 hash:	1E6EC142BA08C7DEAFD25BDEA76F32D4
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: 00000006.00000002.605633875.0000000002E0F000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000006.00000003.379220023.0000000004565000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000006.00000003.379220023.0000000004565000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000006.00000002.603039803.0000000000402000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000006.00000002.603039803.0000000000402000.00000040.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000006.00000002.606069494.0000000003CF5000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000006.00000002.606069494.0000000003CF5000.00000004.00000001.sdmp, Author: Joe Security • Rule: MAL_HawkEye_Keylogger_Gen_Dec18, Description: Detects HawkEye Keylogger Reborn, Source: 00000006.00000002.604780389.0000000002D03000.00000004.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_HawkEye, Description: Yara detected HawkEye Keylogger, Source: 00000006.00000002.604780389.0000000002D03000.00000004.00000001.sdmp, Author: Joe Security • Rule: JoeSecurity_WebBrowserPassView, Description: Yara detected WebBrowserPassView password recovery tool, Source: 00000006.00000002.604780389.0000000002D03000.00000004.00000001.sdmp, Author: Joe Security
Reputation:	low

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: vbc.exe PID: 7024 Parent PID: 6848

General

Start time:	23:49:39
Start date:	30/08/2021
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\tmp9B04.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: 00000007.00000002.393358492.0000000000400000.00000040.00000001.sdmp, Author: Joe Security
Reputation:	high

File Activities

Show Windows behavior

File Created

File Deleted

File Written

File Read

Analysis Process: vbc.exe PID: 5260 Parent PID: 6848

General

Start time:	23:50:43
Start date:	30/08/2021
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\tmp9795.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: 00000016.00000002.523503971.0000000000400000.00000040.00000001.sdmp, Author: Florian Roth • Rule: JoeSecurity_MailPassView, Description: Yara detected MailPassView, Source: 00000016.00000002.523503971.0000000000400000.00000040.00000001.sdmp, Author: Joe Security

Reputation:	high

Disassembly

Code Analysis

Copyright Joe Security LLC

Copyright Joe Security LLC 2021