

dissectingmalwa.re/picking-locky.html

Tue 30 July 2019 in Ransomware

Back in 2016 Locky was (one of) the first to commercialize the "art" of holding data for ransom. I picked this strain because I would like a bit more of a challenge in terms of obfuscation and anti-disassembly techniques, so strap in for this OG Ransomware

Locky (at least the first few versions) is said to be created by the makers of the Dridex/Cridex banking trojans. For example the spreading mechanism via macros in Word or Excel documents sent out via carefully crafted spear-phishing emails is exactly the same for both of these strains.

A general disclaimer as always: downloading and running the samples linked below will lead to the encryption of your personal data, so be f\$cking careful. Also check with your local laws as owning malware binaries/ sources might be illegal depending on where you live.

Todays samples are brought to you by:

Locky #1 available @ https://github.com/ytisf/theZoo/tree/master/malwares/Binaries/Ransomware.Locky sha256 bc98c8b22461a2c2631b2feec399208fdc4ecd1cd2229066c2f385caa958daa3

Locky.AZ available @ https://dasmalwerk.eu/ sha256 2e4319ff62c03a539b2b2f71768a0cfc0adcaedbcca69dbf235081fe2816248b

🖳 Pro	cess Hacker [Il	E9WIN7\IE	User]								x	
Hacker	r View Too	ols Users	s Help)								
🤣 Ref	resh 🛛 🎲 Opt	ions 🛗	🗄 Find I	handles or	DLLs 💡	🖋 System inf	ormation	🗆 🗔 🗙 👘		Search Processes (Ctrl+K)	Q	
Process	ses Services	Network	Disk									
Name				PID	CPU	I/O total	Private b	User name		Description	-	Running
	vmicsvc.exe			1444			1 MB			Virtual Machine Integration C		
4 🥫	explorer.exe			1480	0.05		23.65 MB	IE9WIN7\IEUser	0	Windows Explorer		
	🥳 VBoxTray.	exe		1964			1.34 MB	IE9WIN7\IEUser	3	VirtualBox Guest Additions Tr		
	🏙 Locky.exe			1004			4.17 MB	IE9WIN7\IEUser				

this first Locky Sample was pretty unspectacular since nothing really happend 🤔. Let's take a look at the binary first:

	Import Results Summary						
Project File Name:	LOCKY Tue Jul 30 00:07:36 CEST 2010						
Readonly:	false						
Program Name:	Locky						
 Language ID:	x86:LE:32:default (2.8)						
 Compiler ID:	windows						
Processor:	x86						
Endian:	Little						
Address Size:	32						
Maximum Address:	00400000						
# of Bytes:	3988554						
# of Memory Blocks:	6						
# of Instructions:	0						
# of Defined Data:	830						
# of Functions:	Θ						
# of Symbols:	183						
# of Data Types:	5						
# Of Data Type Categories: CompanyName:	s FileSee.com						
Compiler:	visualstudio:unknown						
Created With Ghidra Version	:9.0.4						
Date Created:	Tue Jul 30 00:07:35 CEST 2019						
Executable Format:	Portable Executable (PE)						
Executable Location:	/home/f0wl/Malware/Locky/Locky						
Executable MD5:	b06d9dd1/c69ed2ae/5d9e40b2631b42						
FSKL: FileVersion:	TILE:///NOME/TUWI/Malware/Locky/Locky?MDS=D06d9dd1/C69ed2ae/Sd9e40D2631D42						
LegalConvright.	Intend (C) 2013						
ProductName:	Lipreading Fenced						
ProductVersion:	0.144.212.113						
Relocatable:	false						
SectionAlignment:	4096						
Additional Information							
Loading /home/f0wl/Malware/Locky/Locky							
Locky: failed to create IconResource at 007b9630: Conflicting data exists at address 007b8df0 to 007b							
Locky: failed to create IconResource at 007ba6b0: Conflicting data exists at address 007b9e70 to 007b							
Locky: failed to create MenuResource at 007b7b78: Conflicting data exists at address 007b7b28 to 007b							
Locky: failed to create GroupIconResource at 007b9618: Conflicting data exists at address 007b8df0 to							
Locky: failed to create Gro	hupiconkesource at 00/ba698: Conflicting data exists at address 00/b9e/0 to						
Unable to find external lib	Dialy: USER32.DLL						
Searching for referenced li	brary: BASAPT32.DLL						
4							
	OK						



Т

you look at that! We found ourselves some poor mans obfuscation :D A whole bunch of random strings to make the analyst's life just a little bit harder. We'll come back to this later to see if we can simplify our strings output a bit.

alue Gather Gather ent S2.dll n SLakeside ean Lynx Lynx Liticultural enetic Founts oppicMagnetisation eoonate ionsMountains idenFillip ther dHeighten Multiprocessors	String Represen Data Type "WriteFileGather" ds "PulseEvent" ds "KERNEL32.dll" ds "HubLenin" ds "HydrantsLakesi ds "GrimeOcean" ds "LightensLynx" ds "LuckyMulticult ds "OverlandFounts" ds "MacroscopicMa ds "FoundationsMo ds "HandmaidenFill ds "InstitutedHeig ds
alue Gather Gather Gather S2.dll S2.d	String Represen Data Type "WriteFileGather" ds "PulseEvent" ds "KERNEL32.dll" ds "HubLenin" ds "HydrantsLakesi ds "GrimeOcean" ds "LightensLynx" ds "LysineGenetic" ds "MotorsNeonate" ds "FoundationsMo ds "HandmaidenFill ds "KindleLather" ds "InstitutedHeig ds
Gather Ga	"WriteFileGather" ds "PulseEvent" ds "PulseEvent" ds "KERNEL32.dll" ds "HubLenin" ds "HydrantSLakesi ds "GrimeOcean" ds "LightensLynx" ds "LuckyMulticult ds "LuckyMulticult ds "UysineGenetic" ds "OverlandFounts" ds "MacroscopicMa ds "MotorsNeonate" ds "FoundationsMo ds "HandmaidenFill ds "KindleLather" ds "InstitutedHeig ds
ent 32.dll n sLakeside ean Lynx eant Lynx liticultural enetic infounts opicMagnetisation eonate eonate ionsMountains idenFillip ther dHeighten Multiprocessors	"PulseEvent" ds "KERNEL32.dll" ds "HubLenin" ds "HydrantsLakesi ds "GrimeOcean" ds "LightensLynx" ds "LuckyMulticult ds "UysineGenetic" ds "OverlandFounts" ds "MotorsNeonate" ds "FoundationsMo ds "HandmaidenFill ds "InstitutedHeig ds
32.dll n sLakeside ean Lynx Lynx liticultural enetic Founts oppicMagnetisation eoonate ionsMountains idenFillip ther dHeighten Multiprocessors	"KERNEL32.dll"ds"HubLenin"ds"HydrantsLakesids"GrimeOcean"ds"LightensLynx"ds"LuckyMulticultds"LysineGenetic"ds"OverlandFounts"ds"MacroscopicMads"FoundationsMods"FoundationsMods"KindleLather"ds"InstitutedHeigds
n sLakeside ean Lynx Lynx liticultural enetic Founts opicMagnetisation eonate ionsMountains idenFillip ther dHeighten Multiprocessors	"HubLenin" ds "HydrantsLakesi ds "GrimeOcean" ds "LightensLynx" ds "LuckyMulticult ds "LuckyMulticult ds "OverlandFounts" ds "MacroscopicMa ds "FoundationsMo ds "FoundationsMo ds "KindleLather" ds
Lakeside ean Lynx Lynx Iticultural enetic IFounts opicMagnetisation eonate ionsMountains idenFillip ther dHeighten Multiprocessors	"HydrantsLakesi ds "GrimeOcean" ds "LightensLynx" ds "LuckyMulticult ds "LysineGenetic" ds "OverlandFounts" ds "MacroscopicMa ds "MotorsNeonate" ds "FoundationsMo ds "FoundationsMo ds "KindleLather" ds "InstitutedHeig ds
ean Lynx Lynx Ilticultural IFounts opicMagnetisation oonate ionsMountains idenFillip ther dHeighten Multiprocessors	"GrimeOcean" ds "LightensLynx" ds "LuckyMulticult ds "LysineGenetic" ds "OverlandFounts" ds "MacroscopicMa ds "MotorsNeonate" ds "FoundationsMo ds "FoundationsMo ds "FoundationsMi ds "FoundationsMi ds "InstitutedHeig ds
Lynx Ilticultural Inetic IFounts oppicMagnetisation eonate ionsMountains idenFillip ther dHeighten Multiprocessors	"LightensLynx" ds "LuckyMulticult ds "LysineGenetic" ds "OverlandFounts" ds "MacroscopicMa ds "MotorsNeonate" ds "FoundationsMo ds "KindleLather" ds "InstitutedHeig ds
Iticultural enetic IFounts oppicMagnetisation eonate ionsMountains idenFillip ther dHeighten Multiprocessors	"LuckyMulticult ds "LysineGenetic" ds "OverlandFounts" ds "MacroscopicMa ds "MotorsNeonate" ds "FoundationsMo ds "HandmaidenFill ds "KindleLather" ds "InstitutedHeig ds
enetic IFounts IFounts eonate ionsMountains idenFillip ther dHeighten Multiprocessors	"LysineGenetic" ds "OverlandFounts" ds "MacroscopicMa ds "MotorsNeonate" ds "FoundationsMo ds "HandmaidenFill ds "KindleLather" ds "InstitutedHeig ds
Founts opicMagnetisation eonate ionsMountains idenFillip ther dHeighten Multiprocessors	"OverlandFounts" ds "MacroscopicMa ds "MotorsNeonate" ds "FoundationsMo ds "HandmaidenFill ds "KindleLather" ds "InstitutedHeig ds
ppicMagnetisation eonate ionsMountains idenFillip ther dHeighten Multiprocessors	"MacroscopicMa ds "MotorsNeonate" ds "FoundationsMo ds "HandmaidenFill ds "KindleLather" ds "InstitutedHeig ds
oonate oonstountains idenFillip ther dHeighten Multiprocessors	"MotorsNeonate" ds "FoundationsMo ds "HandmaidenFill ds "KindleLather" ds "InstitutedHeig ds
ionsMountains idenFillip ther dHeighten Multiprocessors	"FoundationsMo ds "HandmaidenFill ds "KindleLather" ds "InstitutedHeig ds
idenFillip ther dHeighten Multiprocessors	"HandmaidenFill ds "KindleLather" ds "InstitutedHeig ds
ther dHeighten Multiprocessors	"KindleLather" ds "InstitutedHeig ds
dHeighten Multiprocessors	"InstitutedHeig ds
Multiprocessors	
	"HolidaysMultipr ds
Interlocks	"LocativeInterlo ds
stMicrophones	"InnermostMicr ds
ket	"OffsetJacket" ds
atesFind	"InterrogatesFin ds
antries	"MadridGantries" ds
edLice	"GravitatedLice" ds
d	"FivesMeld" ds
angar	"LibeledHangar" ds
Finality	"LeaguesFinality" ds
tionsOvereat	"IntersectionsO ds
reasing	"HastedGreasing" ds
erForearms	"LiquidiserForea ds
a a F F	ket tesFind Intries dLice I angar iinality ionsOvereat reasing (Forearms

After a couple of seconds it spawns a new svchost.exe process with the same icon as Locky.exe had previously. Of course we'll dump the process memory to a file (just right-click the listing in Process Hacker and choose *Create dump* from the

	5		0		0		,
contoxt monu)	🜉 ProcessHacker.exe		5068	1.28	7 MB	IE9WIN7\IEUser	Process Hacker
context menu).	📉 svchost.exe		1928		5.23 MB	IE9WIN7\IEUser	
Looking at the p	roperties of the new s	vchost.	exe pi	rocess we	can see that it	is actually run from	I

C:\Users\IEUser\AppData\Local\Temp\ and it's unsigned as well.

	emory	Environment	Handles	Commen		
General S	tatistics	Performance	Threads	Toker		
File						
N/A						
UNVER	IFIED)					
Version: 0.170.1	6.207					
Image file name:						
C:\Users\IEUser	\AppData\L	ocal\Temp\svchost.ex	e			
Process						
Command line:	C:\User	s\IEUser\AppData\Loo	cal\Temp\svcho	ost.exe 🔍		
Command line: Current directory:	C:\User	s \IEUser \AppData \Loo s \IEUser \Downloads \F	cal\Temp\svcho Ransomware.Lo	ost.exe 🔍 ocky\		
Command line: Current directory: Started:	C:\User	s\IEUser\AppData\Loo s\IEUser\Downloads\F e and 37 seconds ano	cal\Temp\svchc Ransomware.Lo	ost.exe		
Command line: Current directory: Started:	C:\User C:\User	s\IEUser\AppData\Loo s\IEUser\Downloads\F e and 37 seconds ago	cal\Temp\svchc Ransomware.Lo (12:08:51 PM	ost.exe		
Command line: Current directory: Started: PEB address:	C:\User C:\User a minute 0x7ffdc	s\IEUser\AppData\Loo s\IEUser\Downloads\F e and 37 seconds ago 000	cal\Temp\svchc Ransomware.Lo (12:08:51 PM	ost.exe		
Command line: Current directory: Started: PEB address: Parent:	C:\User C:\User a minute 0x7ffdc Non-exi	s\IEUser\AppData\Lo s\IEUser\Downloads\F e and 37 seconds ago 000 stent process (1004)	cal\Temp\svchc Ransomware.Lo (12:08:51 PM	ost.exe		
Command line: Current directory: Started: PEB address: Parent: Mitigation policies:	C:\User C:\User a minute 0x7ffdc Non-exi	s\IEUser\AppData\Loo s\IEUser\Downloads\F e and 37 seconds ago 000 istent process (1004)	cal\Temp\svchc Ransomware.Lc (12:08:51 PM	ost.exe		
Command line: Current directory: Started: PEB address: Parent: Mitigation policies: Protection: None	C:\User C:\User a minute 0x7ffdc Non-exi	s\IEUser\AppData\Loo s\IEUser\Downloads\F e and 37 seconds ago 000 stent process (1004)	cal\Temp\svchc Ransomware.Lc (12:08:51 PM	ost.exe		

Trojan.Ransom.Locky.AZ

Computer		
Recycle Bin	RunDLL There was a problem starting C:\ran.dll Invalid access to memory location.	×
Reader DC	OK	
📀 🏉 🚞		▲ 🔀 🖬 🏎 1:49 PM 5/10/2019

https://www.hybrid-

analysis.com/sample/2e4319ff62c03a539b2b2f71768a0cfc0adcaedbcca69dbf235081fe2816248b/5cd5813d028838383d3ab408

<pre>Project File Name: 2e4319ff2203539b2b771768a0cf0dacaedbcca69dbf235081fe2816248b Headonly: false Program Name: 2e4319ff2203539b2b771768a0cf0dacaedbcca69dbf235081fe2816248b Language ID: 2e4319ff2203539b2b771768a0cf0dacaedbcca69dbf235081fe2816248b Mainum Address: 00431449 # of Bytes: 187476 # of Memory Blccks: 8 0 # of Defined Data: 0860 # of Function: 0 # of Defined Data: 0860 # of Defined Data: 0860 # of Symbol: 04 # of Bata Type Categories: 3 # of Data Type Categories: 3 # of Data Type Categories: 0 # of Data Type C</pre>		Import Results Summary V A					
Last Modified: Tue Jul 30 23:35:24 CET 2019 Program Name: Language ID: Kompiler ID: Processor: Kell:32:default (2.8) Compiler ID: Processor: Kell:32:default (2.8) Compiler ID: Minium Address: ORAD0000 Maximum Address: Minium Addre	Project File Name:	2e4319ff62c03a539b2b2f71768a0cfc0adcaedbcca69dbf235081fe2816248b					
<pre>Feedonly: false Freqern Name: 2e4319f62c03a539b2b2f71768a0cfc0adcaedbcca69dbf235081fe2816248b Language ID: x86:LE:32:default (2.8) Compiler ID: windows Frocessor: x86 Endia: Little Address Size: 32 Winium Address: 00400000 Maximm Address: 00400000 Created With Ghidra Version: 9, 0.4 Date Created: Tue Jul 30 23:35:23 CEST 2019 Executable Location: //home/f0wl/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b2711768a4 Executable HoCs: 004070 InternalWame: Alert LegalCopyright: 004000 InternalWame: Alert LegalCopyright: 004000 InternalWame: Alert LegalCopyright: 00400 Maxime Alert ProductVersion: 2.01.0007 Relocatable: Tue SectionAlignment: 4006 Translation: 4000409</pre>	Last Modified:	Tue Jul 30 23:35:24 CEST 2019					
<pre>Program Name: 2e4319ff62c03a539b2b2f71768a0cfc0adcaedbcca69dbf235081fe2816248b Language ID: xwindows Processor: x X66 Endian: Little Address: 00400000 Maximum Address: 00400000 Maximum Address: 004400000 Maximum Address: 00440000 Maximum Address: 00440000 Maximum Address: 004400000 Maximum Address: 00440000 Maximum Address: 0044000 Max</pre>	Readonly:	false					
Language ID: x86:LE:32:default (2.8) Compiler ID: windows Processor: x86 Endian: Little Address Size: 32 Minimum Address: 00400000 Maximum Address: 00431449 # of Bytes: 107476 # of Memory Blocks: 8 # of Defined Data: 8620 # of Defined Data: 8620 # of Functions: 0 # of Data Type Categories: 3 CompanyName: Bluefive software Compiler: visualstudio:unknown Created With Ghidra Version: 9.0.4 Date Created: Tue Jul 30 23:35:23 CEST 2019 Executable Format: Portable Executable (PE) Executable Information: 0 Executable Horize: 00226f3aaa157edff9c0235f298850c2 Filebescription: Alert clock FileVersion: 2.01.0007 Filebescription: Alert clock FileVersion: 2.01.0007 Filebescription: Alert clock Filedescription: Alert clock Filedescription: 2.01.0007 Filebescription: Alert clock Firefultion: Alert dit ProductName: Alert ProductName: Alert ProductName: Alert ProductVame: Alert	Program Name:	2e4319ff62c03a539b2b2f71768a0cfc0adcaedbcca69dbf235081fe2816248b					
Compiler ID: windows Processor: x X86 Endian: Little Address Size: 32 Minimum Address: 00400000 Maximum Address: 00400000 Maximum Address: 00431449 * of Bytes: 187476 * of Memory Blocks: 8 * of Instructions: 0 * of Defined Data: 820 * of Defined Data: 820 * of Data Types: 43 * of Data Types: 43 * of Data Types: 43 * of Data Types: 43 * of Data Types: 0.4 Date Created: Tue Jul 30 23:35:23 CEST 2019 Executable Location: //home/fowL/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b2f71768a1 Executable Location: //home/fowL/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b2 FileDescription: Alert clock FileVersion: 2.01.0007 InternalName: Alert LegalCrademarks: David De Groot LegalTrademarks: David De Groot LegalTrademarks: David De Groot SectionAlignment: 40966 Translation: 4b00409 * Additional Information Translation: 4b00409 * Maximum Address: 2001.0007 Redocatable: true SectionAlignment: 40966 Translation: 4b00409 * Maximum Address: 2001.0007 Redocatable: true SectionAlignment: 40066 Translation: 4b00409 * Maximum Address: 2001.0007 Redocatable: true SectionAlignment: 4b00409 * * Maximum Address: 2001.0007 Redocatable: 1007 Redocatable: 1007 SectionAlignment: 4b00409 * * Maximum Address: 2001.0007 Redocatable: 1007 Redocatable: 1007 Red	Language ID:	x86:LE:32:default (2.8)					
Processor: x86 Endian: Little Address Size: 32 Minimum Address: 00400000 Maximum Address: 00431449 # of Bythes: 1047476 # of Memory Blocks: 8 # of Instructions: 0 # of Defined Data: 8620 # of Functions: 0 # of Symbols: 43 # of Data Type Categories: 3 CompanyName: Bluefive software Compiler: visualstudio:unknown Created With Ghidra Version: 9.0.4 Date Created: Tue Jul 30 23:35:23 CEST 2019 Executable Format: Portable Executable (PE) Executable Iofmat: Portable Executable (PE) Executable Hormat: Portable Executable (PE) Executable Hormat: Portable Executable (PE) Executable Hormat: Alert One/fow/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b2f71768a4 FileDescription: Alert clock FileDescription: Alert clock Herd alert. 01 OrginaTelenarks: David De Groot OrginaTelenarks: David De Groot OrginaTelenarks: David De Groot OrginaTelenarks: David De Groot OrginaTelenarks: Alert ProductName: Alert. ProductName: Alert. ProductVarsion: 2.01.0007 Relocatable: true SectionAlignment: 4096 Translation: 4000409 Additional Information True Loading /home/fow/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b2f71768a0cfc0adcaedbccd Searching for referenced library: USER32.DLL Searching for referenced library: WINMM.DLL Unable to find external Library: WINMM.DLL #	Compiler ID:	windows					
Endian: Little Address Size: 32 Minimum Address: 00400000 Maximum Address: 00431449 # of Bytes: 187476 # of Memory Blocks: 8 # of Instructions: 0 # of Symbols: 35 # of Data Types: 43 # of Data Type Categories: 3 CompanyName: Bluefive software Compiler: visualstudio:unknown Created with Ghidra Version: 9.0.4 Date Created: Tue Jul 30 23:35:23 CEST 2019 Executable Format: Portable Executable (PE) Executable Location: //home/fowl/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b2f71768at Executable Mo5: 0026df3aaa15redf960237290850c2 FileBescription: Alert clock FileVersion: 2.01.0007 InternalName: Alert LegalTrademarks: David De Groot LegalTrademarks: David De Groot LegalTrademarks: David De Groot LegalTrademarks: David De Groot SectonAlignment: 4096 Translation: 4b00409 Additional Information Additional Information Addi	Processor:	x86					
Address Size: 32 Minimum Address: 00400000 Maximum Address: 00400000 Maximum Address: 00400000 # of Bytes: 104776 # of Memory Blocks: 8 # of Defined Data: 8620 # of Functions: 0 # of Data Type Categories: 3 CompanyName: Bluefive software Compiler: visualstudio:unknown Created With Chidra Version: 9.0.4 Date Created: Tue Jul 30 23:35:23 CEST 2019 Executable Format: Portable Executable (PE) Executable Format: Portable Executable (PE) Executable Location: //one/f0wl/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b2f71768a0 Executable Isomat: file://home/f0wl/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b2 FSRL: fileDescription: Alert clock FileVersion: 2.01.0007 InternalName: Alert.dll ProductName: Alert.dll Produc	Endian:	Little					
Minimum Address: 00400000 Maximum Address: 00401449 # of Bytes: 187476 # of Memory Blocks: 8 # of Instructions: 0 # of Symbols: 3 # of Data Types: 43 # of Data Types: 40 30 23:35:23 CEST 2019 Executable Location: //home/fowl/Malware/Trojan.Ransom.Locky.AZ/Ze4319ff62c03a539b2b2f71768a4 Executable MDS: 0026df3aaa157edff9c03257098505C FSRL: filePersini: 2.01.0007 InternalName: Alert LegalCopyright: David De Groot LegalTrademarks: Alert difter the SectionAlignment: 400607 Relocatable: true SectionAlignment: 4006409 # # # # # # # # # # # # #	Address Size:	32					
<pre>Maximum Address: 00431449 # of Bytes: 1187476 # of Memory Blocks: 8 # of Instructions: 0 # of Defined Data: 8620 # of Functions: 3 # of Data Types: 43 # of Data Types: 43 # of Data Types: 43 # of Data Types: 9 CompanyName: Bluefive software Compiler: visualstudio:unknown Created With Ghidra Version:9.0.4 Date Created: Tue Jul 30 23:35:23 CEST 2019 Executable Format: Portable Executable (FE) Executable format: Portable Executable (FE) Executable Cocation: //home/fow/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b2f71768a4 Executable MD5: 0826df3aaa157edff9c0325f298850c2 FERL: file://home/fow/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b2 FileDescription: Alert Clock FileVersion: 2.01.0007 InternalName: Alert LegalCopyright: David De Groot LegalTrademarks: David De Groot LegalTrademarks: Alert ProductVersion: 2.01.0007 Relocatable: true SectionAlignment: 4096 Translation: 4b00409</pre>	Minimum Address:	0040000					
<pre># of Bytes: 18/40 # of Hemory Blocks: 8 # of Instructions: 0 # of Defined Data: 8620 # of Functions: 0 # of Symbols: 3 CompanyName: Bluefive software Compiler: visualstudio:unknown Created With Ghidra Version: 9.0.4 Date Created: Tue Jul 30 23:35:23 CEST 2019 Executable Coration: /home/fowl/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b2f71768a0 Executable Location: /home/fowl/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b2f71768a0 Executable PDS: 08260f3aaa157edff9c0325f290850c2 FSRL: file://home/fowl/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b2f71768a0 Executable: true SectionAlignment: 4096 Translation: 4b00409</pre>	Maximum Address:	00431449					
<pre># 01 Memory BiotKs:</pre>	# of Bytes:	18/4/0					
<pre># of lanside LDMs: 0 # of Functions: 0 # of Functions: 0 # of Functions: 0 # of Symbols: 35 # of Data Types: 43 # of Data Types: 43 # of Data Type Categories: 3 CompanyName: Bluefive software Compiler: visualstudio:unknown Created With Ghidra Version:9.0.4 Date Created: Tue Jul 30 23:35:23 CEST 2019 Executable Format: Portable Executable (PE) Executable Location: //home/f0wl/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b2f71768ad Executable Location: Alert clock FileVersion: 2.01.0007 InternalName: Alert clock Corpiler: 2.001.0007 InternalName: Alert Clock ProductName: Alert Clock ProductName: Alert ProductVersion: 2.01.0007 Relocatable: true SectionAlignment: 4096 Translation: 4b00409 Additional Information Additional Informat</pre>	# of Thetructions:	8					
<pre># of Functions: 0 # of Symbols: 35 # of Data Type Categories: 3 CompanyName: Bluefive software Compiler: visualstudio:unknown Created With Ghidra Version: 9.0.4 Date Created: Tue Jul 30 23:35:23 CEST 2019 Executable Format: Portable Executable (PE) Executable Format: Portable Executable (PE) Executable Costion: //home/fowl/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b2f71768a4 Executable MD5: 00226df3aaa157edff9c0325f298850c2 FSRL: fileVersion: 2.01.0007 InternalName: Alert LegalCopyright: David De Groot LegalTrademarks: David De Groot LegalTrademarks: David De Groot Relocatable: true SectionAlignment: 4096 Translation: 4000409 Additional Information Additional Information Additional Information Additional Information Additional Information Additional Unformation Additi</pre>	# of Defined Data	0 9620					
<pre>d f unitions: 0 f of Symbols: 35 f of Data Types: 43 f of Data Types: 43 f of Data Type Categories: 3 CompanyName: Bluefive software Compiler: visualstudio:unknown Created With Ghidra Version: 9.0.4 Date Created: Tue Jul 30 23:35:23 CEST 2019 Executable Format: Portable Executable (PE) Executable Location: //home/fowl/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b2f71768at Executable MD5: 0026df3aaa157edff9c0325f298850c2 FSRL: filee/scription: Alert clock FileVersion: 2.01.0007 InternalName: Alert LegalCopyright: David De Groot LegalTrademarks: David De Groot CriginalFilename: Alert ProductVersion: 2.01.0007 Relocatable: true SectionAlignment: 4096 Translation: 4000409 Additional Information Additional Information</pre>	# of Eurotions,	0					
<pre># of Jymous: 35 # of Data Types: 43 # of Data Types: 43 # of Data Types: 8 CompanyName: Bluefive software Compiler: visualstudio:unknown Created With Ghidra Version: 9.0.4 Date Created: Tue Jul 30 23:35:23 CEST 2019 Executable Format: Portable Executable (PE) Executable Location: //home/fowl/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b2f71768ad Executable MD5: 00226f3aaa157edff9c0325f298850c2 FSRL: file://home/fowl/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b2 FileDescription: Alert clock FileVersion: 2.01.0007 InternalName: Alert LegalCopyright: David De Groot OriginalFilename: Alert.dll ProductName: Alert.dll ProductVersion: 2.01.0007 Relocatable: true SectionAlignment: 4096 Translation: 4b00409</pre>	# of Symbols.	25					
<pre>d) dut Type Categories: 3 companyName: Bluefive software Compiler: visualstudio:unknown Created With Ghidra Version:9.0.4 Date Created: Tue Jul 30 23:35:23 CEST 2019 Executable Format: Portable Executable (PE) Executable Location: //home/fowl/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b2f71768ad Executable MDS: 0826df3aa157edff0c0325f298850c2 FSRL: file:///home/fowl/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b2f71768ad Executable MDS: 0826df3aa157edff0c0325f298850c2 FSRL: file/ersion: 2.01.0007 InternalName: Alert LegalCopyright: David De Groot LegalTrademarks: David De Groot UrginalFilename: Alert ProductVersion: 2.01.0007 Relocatable: true SectionAlignment: 4096 Translation: 4b00409 Additional Information</pre>	# of Data Types:	43					
CompanyName: Bluefive software Compiler: visualstudio:unknown Created With Ghidra Version:9.0.4 Date Created: Tue Jul 30 23:35:23 CEST 2019 Executable Format: Portable Executable (PE) Executable Location: //nome/fowl/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b2f71768a1 Executable MD5: 00226f3aa157edff9c0325f298850c2 FSRL: file0escription: Alert clock File0escription: Alert clock File0escriptin: Alert clock File0escriptin: David De Groot LegalTrademarks: David De Groot LegalTrademarks: David De Groot Relocatable: true SectionAlignment: 4096 Translation: 4000409 Additional Information Model of find external library: USER32.DLL Unable to find external library: USER32.DLL Unable to find external library: SHEL132.DLL Unable to find external library: SHEL132.DL Searching for referenced library: SHEL132.DL Unable to find external library: SHEL132.DL Searching for referenced library: SHEL132.DL Searching for referenced library: SHEL132.DL Searching for searching for searchin	# of Data Types. # of Data Type Categories.	45					
Computer: visualstudio:unknown Created With Ghidra Version:9.0.4 Date Created: Tue Jul 30 23:35:23 CEST 2019 Executable Format: Portable Executable (PE) Executable Location: //home/fowl/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b2f71768ai Executable MD5: 0826df3aaa157edff9c0325f298850c2 FSRL: filebescription: Alert clock FileVersion: 2.01.0007 InternalName: Alert LegalCopyright: David De Groot LegalTrademarks: David De Groot OriginalFilename: Alert ProductName:	CompanyName:	Bluefive software					
Created With Ghidra Version:9.0.4 Date Created: Tue Jul 30 23:35:23 CEST 2019 Executable Format: Portable Executable (PE) Executable MD5: 0020df3aaal57edf9c0325f208850c2 FSRL: fileScription: Alert clock FileDescription: Alert clock FileVersion: 2.01.0007 InternalName: Alert LegalCopyright: David De Groot OriginalFilename: Alert ProductWarsion: 2.01.0007 Relocatable: true SectionAlignment: 4096 Translation: 4006409 Additional Information Additional Information Aditional Inf	Compiler.	visualstudio:unknown					
Date Created: Tue Jul 30 23:35:23 CEST 2019 Executable Format: Portable Executable (PE) Executable Location: //ome/fOWL/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b271768ai Executable MD5: 0826df3aaa157edff9c0325f298850c2 FSRL: fileDescription: Alert clock FileVersion: 2.01.0007 InternalName: Alert LegalCopyright: David De Groot LegalTrademarks: David De Groot LegalTrademarks: David De Groot LegalTrademarks: David De Groot Relocatable: True SectionAlignment: 4096 Translation: 40960 Translation: 40960 Translation: 40960 Translation: 40960 Translation: 40960 Translation: 40960 David De Groot LegalTrademarks: Searching for referenced library: USER32.DLL Unable to find external library: USER32.DLL Unable to find external library: SER32.DLL Searching for referenced library: SER32.DLL Unable to find external library: SER32.DLL Searching for referenced library: SER32.DLL Unable to find external library: SER32.DLL Unable to find external library: SER32.DLL Searching for referenced library: SHEL32.DLL Unable to find external library: SHEL32.DLL Unable to find external library: SHEL32.DLL Unable to find external library: SHEL32.DLL Searching for referenced library: SHEL32.DLL Unable to find external library: SHEL32.DLL Unable to find external library: SHEL32.DLL Unable to find external library: SHEL32.DLL Searching for referenced library: SHEL32.DLL Unable to find external library: SHEL32.DLL Searching for referenced library: SHEL32.DLL Unable to find external library: SHEL32.DLL Searching for referenced library: SHEL32.DLL Unable to find external library: WINMM.DLL The Searching for referenced library: WINMM.DLL T	Created With Ghidra Version	:9.0.4					
Executable Format: Portable Executable (PE) Executable Location: //home/fGW1/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b2f71768ai Executable MDS: 0826df3aaa1576298550c2 FSRL: file:///home/fGW1/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b2 FileDescription: Alert clock FileVersion: 2.01.0007 InternalName: Alert LegalCopyright: David De Groot LegalTrademarks: David De Groot OriginalFilename: Alert.dll ProductName: Alert ProductVarsion: 2.01.0007 Relocatable: true SectionAlignment: 4096 Translation: 4b00409 Additional Information Additional Information Additional Information Additional Information Additional Information Muable to find external library: USER32.DLL Unable to find external library: SHEL132.DLL Unable to find external library: WINMM.DLL	Date Created:	Tue Jul 30 23:35:23 CEST 2019					
Executable Location: /home/f0wl/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b2f71768ad Executable MDS: 0026df3aaa157edff9c0325f298850c2 FSRL: file:///home/f0wl/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b2 FileDescription: Alert clock FileVersion: 2.01.0007 InternalName: Alert LegalCopyright: David De Groot LegalTrademarks: David De Groot UrginalFilename: Alert.dll ProductName: Alert ProductVersion: 2.01.0007 Relocatable: true SectionAlignment: 4096 Translation: 4b00409 Imable to find external library: USER32.DLL Searching for referenced library: USER32.DLL Searching for referenced library: ADVAPI32.DL Unable to find external library: SHEL132.DLL Searching for referenced library: SHEL132.DLL Searching for referenced library: SHEL132.DLL Searching for referenced library: SHEL132.DLL Searching for referenced library: SHEL132.DLL Searching for referenced library: SHEL132.DLL Searching for referenced library: SHEL132.DLL Searching for referenced library: SHEL132.DLL Searching for referenced library: SHEL132.DLL <td< td=""><td>Executable Format:</td><td>Portable Executable (PE)</td></td<>	Executable Format:	Portable Executable (PE)					
Executable MD5: 0826df3aaa157edff9c0325f298850c2 FSRL: file:///home/f0wl/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b2 FileDescription: Alert clock FileVersion: 2.01.0007 InternalName: Alert LegalCopyright: David De Groot LegalTrademarks: David De Groot OriginalFilename: Alert.dll ProductName: Alert ProductVame: Alert ProductVersion: 2.01.0007 Relocatable: true SectionAlignment: 4096 Translation: 4b00409 Additional Information Loading /home/f0wl/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b2f71768a0cfc0adcaedbccc Searching for referenced library: USER32.DLL Searching for referenced library: ADVAPI32.DLL Searching for referenced library: ADVAPI32.DLL Unable to find external library: SHEL132.DLL Searching for referenced library: SHEL132.DLL Unable to find external library: WINMM.DLL 	Executable Location:	/home/f0wl/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b2f71768a0c					
FSRL: file:///home/f0wl/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b2' FileDescription: Alert clock FileDescription: 2.01.0007 InternalName: Alert LegalCopyright: David De Groot OriginalFilename: Alert LegalTrademarks: David De Groot OriginalFilename: Alert.dll ProductName: Alert ProductVersion: 2.01.0007 Relocatable: true SectionAlignment: 4096 Translation: 4b00409 Additional Information unable to find external library: USER32.DLL Unable to find external library: USER32.DLL Unable to find external library: SHELI32.DLL Unable to find external library: WINM.DLL Unable to find external library: WINM.D	Executable MD5:	0826df3aaa157edff9c0325f298850c2					
<pre>FileDescription: Alert clock FileVersion: 2.01.0007 InternalName: Alert LegalCopyright: David De Groot LegalTrademarks: David De Groot OriginalFilename: Alert.dll ProductName: Alert ProductVersion: 2.01.0007 Relocatable: true SectionAlignment: 4096 Translation: 4b00409 Additional Information Loading /home/f0wl/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b2f71768a0cfc0adcaedbcc: Searching for referenced library: USER32.DLL Searching for referenced library: ADVAPI32.DLL Searching for referenced library: SHEL132.DLL Searching for referenced library: SHEL132.DLL Searching for referenced library: SHEL132.DLL Searching for referenced library: WINMM.DLL ADDE to find external library: SHEL132.DLL Searching for referenced library: WINMM.DLL ADDE to find external library: WINMM.DLL ADDE to find ex</pre>	FSRL: file:///home/f0wl/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b2f7176						
FileVersion: 2.01.0007 InternalName: Alert LegalCopyright: David De Groot LegalTrademarks: David De Groot OriginalFilename: Alert. ProductVersion: 2.01.0007 Relocatable: true SectionAlignment: 4096 Translation: 4b00409 Additional Information Loading /home/f0wl/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b2f71768a0cfc0adcaedbcc: Searching for referenced library: USER32.DLL Unable to find external library: USER32.DLL Unable to find external library: ADVAPI32.DLL Unable to find external library: SHELL32.DLL Unable to find external library: SHELL32.DLL Unable to find external library: SHELL32.DLL Unable to find external library: WINMM.DLL Unable to find external library: WINMM.DLL Unable to find external library: WINMM.DLL Unable to find external library: WINMM.DLL	FileDescription:	Alert clock					
InternalName: Alert LegalCopyright: David De Groot LegalTrademarks: David De Groot OriginalFilename: Alert.dll ProductVersion: 2.01.0007 Relocatable: true SectionAlignment: 4096 Translation: 4b00409 Additional Information Loading /home/f0wl/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b2f71768a0cfc0adcaedbccc Searching for referenced library: USER32.DLL Unable to find external library: USER32.DLL Unable to find external library: USER32.DLL Unable to find external library: SHEL132.DLL Unable to find external library: SHEL132.DLL Unable to find external library: SHEL132.DLL Unable to find external library: WINMM.DLL Unable to find external library: WINMM.DLL	FileVersion:	2.01.0007					
LegalCopyright: David De Groot LegalTrademarks: David De Groot OriginalFilename: Alert. ProductName: Alert ProductVersion: 2.01.0007 Relocatable: true SectionAlignment: 4096 Translation: 4b00409 Additional Information Loading /home/f0wl/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b2f71768a0cfc0adcaedbcca Searching for referenced library: USER32.DLL Unable to find external library: USER32.DLL Unable to find external library: SHELI32.DLL Unable to find external library: WINMM.DLL Unable to find external library: WINMM.DLL	InternalName:	Alert					
LegalTrademarks: David De Groot OriginalFilename: Alert.dll ProductName: Alert ProductVersion: 2.01.0007 Relocatable: true SectionAlignment: 4096 Translation: 4b00409 Additional Information Loading /home/f0wl/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b2f71768a0cfc0adcaedbcca Searching for referenced library: USER32.DLL Unable to find external library: USER32.DLL Unable to find external library: USER32.DLL Unable to find external library: SHEL132.DLL Searching for referenced library: SHEL132.DLL Searching for referenced library: SHEL132.DLL Searching for referenced library: SHEL132.DLL Searching for referenced library: WINMM.DLL Unable to find external library: WINMM.DLL	LegalCopyright:	David De Groot					
OriginalFilename: Alert.dll ProductName: Alert ProductVersion: 2.01.0007 Relocatable: true SectionAlignment: 4096 Translation: 4b00409 Additional Information Additional Information Additional Information Additional for referenced library: USER32.DLL Unable to find external library: USER32.DLL Unable to find external library: ADVAPI32.DLL Searching for referenced library: SHELL32.DLL Searching for referenced library: SHELL32.DLL Unable to find external library: SHELL32.DLL Searching for referenced library: SHELL32.DLL Searching for referenced library: SHELL32.DLL Lunable to find external library: SHELL32.DLL Searching for referenced library: WINMM.DLL Unable to find external library: WINMM.DLL	LegalTrademarks:	David De Groot					
ProductName: Alert ProductVersion: 2.01.0007 Relocatable: true SectionAlignment: 4096 Translation: 4b00409 Additional Information Loading /home/f0wl/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b2f71768a0cfc0adcaedbcc: Searching for referenced library: USER32.DLL Unable to find external library: USER32.DLL Unable to find external library: USER32.DLL Unable to find external library: ADVAPI32.DLL Searching for referenced library: SHELL32.DLL Unable to find external library: SHELL32.DLL Unable to find external library: SHELL32.DLL Unable to find external library: WINMM.DLL Unable to find external library: WINMM.DLL Unable to find external library: WINMM.DLL	OriginalFilename:	Alert.dll					
ProductVersion: 2.01.0007 Relocatable: true SectionAlignment: 4096 Translation: 4b00409 Additional Information Loading /home/f0wl/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b2f71768a0cfc0adcaedbcc: Searching for referenced library: USER32.DLL Unable to find external library: USER32.DLL Unable to find external library: USER32.DLL Unable to find external library: ADVAPI32.DLL Unable to find external library: SHELL32.DLL Unable to find external library: WINMM.DLL Unable to find external library: WINMM.DLL Unable to find external library: WINMM.DLL	ProductName:	Alert					
Relocatable: true SectionAlignment: 4096 Translation: 4b00409 Additional Information Loading /home/f0wl/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b2f71768a0cfc0adcaedbcc: Searching for referenced library: USER32.DLL Unable to find external library: USER32.DLL Unable to find external library: ADVAPI32.DLL Searching for referenced library: SHELL32.DLL Unable to find external library: SHELL32.DLL Unable to find external library: SHELL32.DLL Unable to find external library: WIMM.DLL Unable to find external library: WIMM.DLL Unable to find external library: WIMM.DLL	ProductVersion:	2.01.0007					
SectionAlignment: 4096 Translation: 4b00409 Additional Information Loading /home/f0wl/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b2f71768a0cfc0adcaedbcc: Searching for referenced library: USER32.DLL Unable to find external library: USER32.DLL Unable to find external library: ADVAPI32.DLL Unable to find external library: ADVAPI32.DLL Unable to find external library: SHEL132.DLL Unable to find external library: SHEL132.DLL Unable to find external library: SHEL132.DLL Unable to find external library: WINMM.DLL Unable to find external library: WINMM.DLL Unable to find external library: WINMM.DLL	Relocatable:	true					
Transtation: 4000409 Additional Information Additional for referenced library: USER32.DLL Unable to find external library: USER32.DLL Unable to find external library: ADVAPI32.DLL Unable to find external library: ADVAPI32.DLL Unable to find external library: SHELL32.DLL Unable to find external library: SHELL32.DLL Unable to find external library: SHELL32.DLL Unable to find external library: SHELL32.DLL Unable to find external library: SHELL32.DLL Unable to find external library: SHELL32.DLL Unable to find external library: SHELL32.DLL Unable to find external library: SHELL32.DLL Unable to find external library: SHELL32.DLL Unable to find external library: SHELL32.DLL Unable to find external library: WINMM.DLL Unable to find external library: WINMM.DLL Unable to find external library: WINMM.DLL OK	SectionAlignment:	4096					
Additional Information Loading /home/f0wl/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b2f71768a0cfc0adcaedbcc: Searching for referenced library: USER32.DLL Unable to find external library: ADVAPI32.DLL Unable to find external library: ADVAPI32.DLL Unable to find external library: SHELL32.DLL Unable to find external library: SHELL32.DLL Unable to find external library: WINMM.DLL Unable to find external library: WINMM.DLL Unable to find external library: WINMM.DLL	Translation:	4000409					
Additional Information Loading /home/f0wl/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b2f71768a0cfc0adcaedbcc: Searching for referenced library: USER32.DLL Unable to find external library: OSER32.DLL Searching for referenced library: ADVAPI32.DLL Searching for referenced library: SHELL32.DLL Searching for referenced library: SHELL32.DLL Searching for referenced library: SHELL32.DLL Searching for referenced library: WINMM.DLL Unable to find external library: WINMM.DLL Mobile to find external library: WINMM.DLL	-	7					
Aduitonal minormation Loading /home/f0wl/Malware/Trojan.Ransom.Locky.AZ/2e4319ff62c03a539b2b2f71768a0cfc0adcaedbcc: Searching for referenced library: USER32.DLL Unable to find external library: ADVAPI32.DLL Searching for referenced library: ADVAPI32.DLL Searching for referenced library: SHELL32.DLL Unable to find external library: SHELL32.DLL Searching for referenced library: WINMM.DLL Searching for referenced library: WINMM.DLL Unable to find external library: WINMM.DLL Mable to find external library: WINMM.DLL Mable to find external library: WINMM.DLL	Additional Information						
Searching for referenced library: USER32.DLL Unable to find external library: USER32.DLL Searching for referenced library: ADVAPI32.DLL Unable to find external library: ADVAPI32.DLL Searching for referenced library: SHELL32.DLL Unable to find external library: SHELL32.DLL Searching for referenced library: WINMM.DLL Unable to find external library: WINMM.DLL Mobile to find external library: WINMM.DLL	Additional information Loading /home/f0wl/Malware/Trojan.Ransom.Lockv.AZ/2e4319ff62c03a539b2b2f71768a0cfc0adcaedbcca60						
Unable to find external library: USER32.DLL Searching for referenced library: ADVAPI32.DLL Unable to find external library: ADVAPI32.DLL Searching for referenced library: SHELL32.DLL Unable to find external library: WINMM.DLL Unable to find external library: WINMM.DLL Unable to find external library: WINMM.DLL	Searching for referenced library: USER32.DLL						
Searching for referenced library: ADVAPI32.DLL Unable to find external library: ADVAPI32.DLL Searching for referenced library: SHELL32.DLL Unable to find external library: SHELL32.DLL Unable to find external library: WINMM.DLL Unable to find external library: WINMM.DLL	Unable to find external library: USER32.DLL						
Unable to find external library: ADVAPI32.DLL Searching for referenced library: SHELL32.DLL Unable to find external library: SHELL32.DLL Searching for referenced library: WINMM.DLL Unable to find external library: WINMM.DLL	Searching for referenced library: ADVAPI32.DLL						
Searching for referenced library: SHELL32.DLL Unable to find external library: SHELL32.DLL Searching for referenced library: WINMM.DLL Unable to find external library: WINMM.DLL	Unable to find external library: ADVAPI32.DLL						
Unable to find external library: SHELL32.DLL Searching for referenced library: WINMM.DLL Unable to find external library: WINMM.DLL	Searching for referenced library: SHELL32.DLL						
Searching for referenced library: WINMM.DLL Unable to find external library: WINMM.DLL	Unable to find external library: SHELL32.DLL						
Unable tō find external library: WINMM.DLL	Searching for referenced li	brary: WINMM.DLL					
	Unable to find external lib	rary: WINMM.DLL					
OK	•						
		OK					

This article is a work in progress, updates going to follow soon

IOCs

Locky (SHA256)

 $2e4319ff62c03a539b2b2f71768a0cfc0adcaedbcca69dbf235081fe2816248b\\5ed2f09e648dca8f0ca75466b1442f6e599afddc80777e0559fb6881c6cd9ff3\\3b60fde281d91cc3e7ea3e343ee5b13a31def564903c0136ae928f70e25c3c02\\6afc78b5630726c907a69d62a6c8a7d86326e21383fe3aae1efc715342238e02\\$