

#### Annual ADFSL Conference on Digital Forensics, Security and Law

2017 Proceedings

May 15th, 10:00 AM

# Kelihos Botnet: A Never-Ending Saga

Arsh Arora University of Alabama, Birmingham, ararora@uab.edu

Max Gannon University of Alabama, Birmingham, gannonm@uab.edu

Gary Warner University of Alabama, Birmingham, gar@uab.edu

Follow this and additional works at: https://commons.erau.edu/adfsl

Part of the Defense and Security Studies Commons, Forensic Science and Technology Commons, Information Security Commons, OS and Networks Commons, Other Computer Sciences Commons, and the Science and Technology Studies Commons

#### **Scholarly Commons Citation**

Arora, Arsh; Gannon, Max; and Warner, Gary, "Kelihos Botnet: A Never-Ending Saga" (2017). *Annual ADFSL Conference on Digital Forensics, Security and Law.* 4. https://commons.erau.edu/adfsl/2017/papers/4

This Peer Reviewed Paper is brought to you for free and open access by the Conferences at Scholarly Commons. It has been accepted for inclusion in Annual ADFSL Conference on Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.





# KELIHOS BOTNET: A NEVER-ENDING SAGA

Arsh Arora, Max Gannon, Gary Warner University of Alabama at Birmingham 1201 University Blvd, Birmingham, AL 35233 {ararora, gannonm, gar}@uab.edu

## ABSTRACT

This paper investigates the recent behavior of the Kelihos botnet, a spam-sending botnet that accounts for many millions of emails sent each day. The paper demonstrates how a team of students are able to perform a longitudinal malware study, making significant observations and contributions to the understanding of a major botnet using tools and techniques taught in the classroom. From this perspective, the paper has two objectives: encouragement and observation. First, by providing insight into the methodology and tools used by student researchers to document and understand a botnet, the paper strives to embolden other academic programs to follow a similar path and to encourage such discovery. Second, the paper shares observations and insights gathered about the botnet's recent spam activity showing evidence of the "spam as a service" model and demonstrating a variety of unique and dangerous spam campaigns conducted via the Kelihos botnet, including banking trojans, credential phishing, and ransomware attacks.

**Keywords**: Kelihos, Botnet, Malware, Spam, Ransomware, Banking Trojan, Pharma, Pump and Dump, Geo-Targeting

## 1. INTRODUCTION

While the Kelihos botnet first debuted in 2009, the current botnet is a functional derivative of two other famous botnets, Waledac, and the Storm Worm [Adair, 2012, Bureau, 2011]. The Kelihos botnet is known by a number of aliases in the community including Hlux and Slenfbot [Singh et al., 2014]. Kelihos evolved and became sophisticated over time, but no interruption could stop the working of Kelihos. Two widely celebrated takedowns of Kelihos have been performed by security companies. The first was Operation b79, conducted by Microsoft in September of 2009 [Nadji et al., 2013]. In March of 2012, CrowdStrike, Dell Secureworks, Kaspersky, and others sinkholed 100,000 nodes of the Kelihos.B malware [Kerkers et al., 2014]. At RSA Conference 2013, CrowdStrike demonstrated a repeat performance, targeted Kelihos.C [Rossow et al., 2013, Werner, 2013]. Despite these admirable attempts, Kelihos continues to send significant volumes of spam on a daily basis [Stringhini et al., 2014]. Even after all of the takedown attempts, Kelihos was still ranked as the top spam-sending botnet in 2015 and continues to yield a significant spam volume today [McAfee, 2016, Tech, 2016].

The Kelihos botnet utilizes a peer to peer

network infrastructure that hides the location of the true command and control server [Dietrich et al., 2013]. Kelihos-infected computers communicate with one another and are used in two primary ways, depending on whether they have a publicly reachable IP address or not. Nodes which cannot be addressed from the Internet just send spam. Internet addressable nodes help to anonymize the location of the C&C server by acting as a multi-tiered proxy, receiving requests for spam details from spamming nodes, and requesting those same details from other nodes, eventually leading to a job server which is leased infrastructure and communicates with the C&C server, as documented by Fortinet's Kyle Yang at BlackHat [Yang, 2012].

The most unique aspect of Kelihos is the diversity in its spam and its delivery mechanism. The spam diversity is primarily because Kelihos provides "spam as a service" offering the use of its spamming infrastructure for hire to deliver any messages for a sender who is willing to pay their fees. The spam messages are dominated by pharmaceutical spam, but are not limited to it. Pharma spam seems to be the fall-back position, when other higher paying customers have not hired the botnet to deliver something else. Kelihos has been observed sending spam for pump and dump manipulation of different stock symbols, money mule job applications, and credential phishing for Polish and French financial institutions. In the summer of 2016, Kelihos began geo-targeting for email delivery sending different messages and payloads based on the country-code Top Level Domain (ccTLD) of the email recipient ('.pl','.uk'). Malware, including ransomware and Zeus banking trojans, were delivered only to certain geographies using this technique. Kelihos has been seen spamming ransomware, sending Wild-Fire [Arora & Warner, 2016b], CryptFile2 [Arora & Warner, 2016a] and Troldesh [Arora & Warner, 2016f] encryption ransomware families.

Another addition to the spam campaign is sending links to a Word document that will drop a variant of Zeus, specifically, geotargeting for German and United Kingdom banks. In the current iteration, it uses stolen SMTP credentials to login as a legitimate user to a large number of mail servers and sends spam.



Figure 1. Courtesy: Kyle Yang outlining Kelihos distribution network [Yang, 2012]

Although the division of the botnet's operation appears to be clear in Figure 1, the path is actually complex. Starting from the bottom, the chart displays the worker or client nodes, which sends spam to the end user and only communicate to the servers at the proxy level. The proxy level is the most interesting one as it connects with other proxies, clients, and job servers. This 3-way communication makes it the most attractive and the one that contains maximum information. The proxy level receives templates from other proxies and also communicates with the job servers. While Kelihos-infected Windows computers serve as the proxy and worker nodes, job servers are leased hardware controlled by the criminals. Job servers are the ones that serve as the main operators to the command and control center. Job servers are often in disguise and try to be invisible under the shadow

of different proxies; thus, making detection extremely complex and difficult. Lastly, the command and control center is handled by the bot herder and provides the information, spam templates, and updates needed to be distributed across the botnet.

# 3. INITIALIZATION

In this section, researchers will describe the pattern that is followed by the Kelihos binary to initiate, then communicate to its command and control center and eventually send spam. The process will be illustrated with screen captures from OllyDbg and Wireshark. The details are shared so that they can be easily replicated by any individual who has expertise with OllyDbg. The following analysis was performed in a virtual environment (VMWare) operating in NAT network mode.

#### 3.1 Processes

In the subsequent section, researchers will describe the process of how a Kelihos binary performs when we try to self-infect. The preliminary observations can be viewed with the help of programs such as Wireshark, Process Hacker, and OllyDbg 2.0 version. Next, we will explain the process of self-infecting with a complete description of the process as depicted in Figure 2. As soon as we launch the binary, it initiates and starts a child process. Once the child process gets fully activated, it terminates the parent process and starts the communication process. Initially, it tries to make a TCP connection with several Internet Protocol (IP) addresses which are hard-coded in the binary. There is a unique identifier in the message that helps to authenticate the communication coming from the Kelihos binary. Once a connection is established, it makes a request for configuration (config) files. The config files contain the information about the spam template and the email addresses to be used for sending spam messages.



Figure 2. Architecture of Kelihos Malware

#### 3.1.1 Parent Process

In the following sub-section, researchers will demonstrate some breakpoints in OllyDbg that are helpful in performing the analysis. To attain optimum results, the following steps should be followed in the order mentioned.

After introducing a Kelihos binary into the virtual environment, start Process Hacker and OllyDbg as an administrator. Next, open the Kelihos binary in OllyDbg. Now, one can see a process being activated in Process Hacker. The following breakpoints should be enabled under the Executables (E) tab of OllyDbg:

- 1. Ntdll.dll
  - (a) RtlReportSilentProcessExit
  - (b) NtTeminateProcess
  - (c) NtResumeThread
- 2. kernel32.dll
  - (a) Resume Thread

B INT3 brea	kpoints			
Address	Module	Status	Disassembly	Comment
75C80F1C	kerne132	Active	MOV EDI,EDI	UINT kernel32.ResumeThread(Thread)
778364A8	ntdll	Active	MOV EAX,130	ntdll.NtResumeThread(guessed Arg1,Arg2)
77836808	ntdll	Active	MOU EAX,172	ntdll.NtTerminateProcess(guessed Arg1,Arg2)
7784DFDC	ntdll	Active	MOV EDI,EDI	ntdll.RtlReportSilentProcessExit(guessed Arg1,Arg2)

Figure 3. Breakpoints for Parent Process

The researchers provide the specific breakpoints in Figure 3, so that the results may be easily replicated. Once we start debugging the program, it will stop at the breakpoints in the following manner:

- 1. RtlReportSilentProcessExit
- 2. NtTerminateProcess
- 3. RtlReportSilentProcessExit
- 4. NtTerminateProcess
- 5. ResumeThread
- 6. NtResumeThread

The process is complicated, but this method seems to obtain the maximum information from the parent process before moving to the child process. This child process can be observed in Process Hacker. The timing of when to attach to the child process is crucial, if one does it before or after the following steps mentioned above, the desired result may not be obtained. Next, we attach the child process in a new OllyDbg window with administrative rights.

#### 3.1.2 Child Process

Once the child process is attached successfully, we check the Executables (E) box and set a breakpoint in the child process at the following location displayed in figure 4.

- 1. kernel32.dll
  - (a) Virtual Protect



Figure 4. Breakpoints for Child Process

By setting a breakpoint on kernel32.VirtualProtect, we can pause the malware execution only after the code has been unpacked. One way to understand this unpacking is to observe the DLLs listed in the Executables window in OllyDBG. Before running to the next breakpoint, there are only four DLLs under the Executable section, as shown in Figure 5.

After the execution pauses at the Virtual Protect breakpoint, we can see in figure 6, that the number is significantly greater than what was observed previously.

E Executab	le modules						- 8
Base	Size	Entry	Name	Туре	File version	Static links	Path
00400000	00245000	0063E000	5dec	)		KERNEL32	C:\Users\carbona Desktop\
75A50000	00044000	75A57DE0	KERNELBASE		6.1.7688.16385	ntdll	C:\Windows\system32\KERNELBASE.dll
75040000	88804888	75C8BDE4	kerne132		6.1.7688.16385	API-HS-Win-Core-Debug-L1-1-8, API-HS-Wi	C:\Windows\system32\kernel32.dll
777F 0000	0013C000		ntdll		6.1.7688.16385		C:\Windows\SYSTEM32\ntdl1.dll

Figure 5. Pre-loaded Dlls at Virtual Protect

E Executal	ble modules						
Base	Size	Entry	Name	Туре	File version	Static links	Path
8848888	00245000	8863E888	5dec			KERNEL32	C:\Users\Desktop\5dec
7418088	00007000	74181280	VINNSI		6.1.7608.16385 (1	API-MS-Win-Core-ErrorHandling-L, API-MS	C:\Windows\susten32\WINNSI.DLL
7428088	00010000	74288431	IPHLPAPI		6.1.7608.16385 (	API-MS-Vin-Core-DelayLoad-L1-1-, API-MS	C:\Windows\system32\IPHLPAPI.DLL
7510088	00844008	751E63F9	DNSAPI		6.1.7608.16385 (1	API-HS-Vin-Core-Debug-L1-1-0, API-HS-Win	C:\Windows\system32\DNSAPI.dll
7530000	00030000	75301450	HSWSOCK		6.1.7608.16385 ()	API-HS-Win-Core-Debug-L1-1-0, API-HS-Win	C:\Windows\system32\MSWSOCK.dll
7598000	00000000	7598238E	HSASH1		6.1.7601.17514 (1	API-MS-Win-Core-ErrorHandling-L, API-MS-	C:\Windows\system32\MSASN1.dll
7565000	00844008	75A57DE0	KERNELBASE		6.1.7608.16385 (1	ntdll	C:\Windows\system32\KERNELBASE.dll
75AC000	) 0011D000	75AC158A	CRYPT32		6.1.7608.16385 (1	API-MS-Win-Core-LocalRegistry-L, API-MS	C:\Windows\system32\CRYPT32.dll
7504000	88804888	75C8BDE4	kerne132		6.1.7608.16385 (1	API-HS-Win-Core-Debug-L1-1-0, API-HS-Wi	C:\Windows\system32\kernel32.dll
7508000	00000000	7508168B	HSCTF		6.1.7608.16385 (1	API-MS-Win-Core-LocalRegistry-L, API-MS	C:\Windows\system32\MSCTF.dll
75E5000	00000000	75E5A472	nsvert		7.8.7688.16385 (1	API-MS-Win-Core-Console-L1-1-0, API-MS-	C:\Windows\system32\msvcrt.dll
75F 0000	00835000	75F0145D	WS2_32		6.1.7600.16385 (1	API-MS-Win-Core-DelayLoad-L1-1-, API-MS	C:\Windows\system32\WS2_32.dll
75F4000	00090000	75F73F07	USP10		1.8626.7681.1751	GD132, KERNEL32, mswcrt, USER32	C:\Windows\system32\USP10.dll
75FE000	0001F000	75FE1355	INN32		6.1.7601.17514 (1	API-MS-Win-Core-LocalRegistry-L, API-MS	C:\Windows\system32\IMM32.DLL
7688888	) 0008F000	76003FB1	OLEAUT32		6.1.7601.17514	API-MS-Win-Core-LocalRegistry-L, API-MS	C:\Windows\system32\OLEAUT32.dll
7616000	) 0084E008	76169089	GD132		6.1.7601.17514 (1	API-MS-Win-Core-LocalRegistry-L, API-MS	C:\Windows\system32\GDI32.dll
7618088	001FB000	76182209	iertutil		8.88.7681.17514	ADVAPI32, KERNEL32, msvcrt, ntdll, SHLW	C:\Windows\system32\iertutil.dll
7638000	00150000	763F8A3D	ole32		6.1.7600.16385 ()	API-HS-Vin-Core-Debug-L1-1-0, API-HS-Wi	C:\Windows\system32\ole32.dll
7651000	00136000	76511835	urlmon		8.00.7600.16385	ADVAPI32, CRYPT32, iertutil, KERNEL32, I	C:\Windows\system32\urlmon.dll
7665000	00001000	76682433	RPCRT4		6.1.7600.16385 ()	API-MS-Win-Core-DelayLoad-L1-1-, API-MS	C:\Windows\system32\RPCRT4.dll
7670000	) 00C4A000	76781681	SHELL32		6.1.7601.17514 (1	API-HS-Vin-Core-Debug-L1-1-0, API-HS-Wi	C:\Windows\system32\SHELL32.dll
7735000	000000000	773649E5	ADVAP132		6.1.7608.16385 ()	API-MS-Vin-Core-LocalRegistry-L, API-MS	C:\Windows\system32\ADVAPI32.dll
773F000	) 000F5000	773F1865	VININET		8.00.7600.16385	ADVAPI32, iertutil, KERNEL32, msvcrt, m	C:\Windows\system32\WININET.dll
7772000	00000000	77730711	user32		6.1.7601.17514 (1	GDI32, KERNEL32, ntdll	C:\Windows\system32\user32.dll
777F 000	00130000		ntdll		6.1.7600.16385 (1		C:\Windows\SYSTEM32\ntdll.dll
7793000	00005000	77931438	PSAPI		6.1.7600.16385 (1	KERNEL32	C:\Windows\system32\PSAP1.DLL
7794000	0000A000	77941360	LPK		6.1.7608.16385 (1	API-MS-Vin-Core-ErrorHandling-L, API-MS	C:\Windows\system32\LPK.dl1
7798000	1 00006000	77981782	N21		6.1.7600.16385 (1	API-MS-Vin-Core-ErrorHandling-L, API-MS	C:\Windows\system32\NSI.dll
7799088	00019000	77994975	sechost		6.1.7608.16385 (1	API-HS-Vin-Core-Debug-L1-1-0, API-HS-Wi	C:\Windows\SYSTEH32\sechost.dll
7790000	00057000	77909886	SHLWAPI		6.1.7600.16385 (1	API-MS-Win-Core-LocalRegistry-L, GDI32,	C:\Windows\system32\SHLWAPI.dll

Figure 6. New DLLs loaded shown in Red

Next, the binary will decrypt itself and then proceed towards its communication channel.

## 3.2 Preparing for Take-Off

This section demonstrates a decoding loop that is run across the code within the binary. Figure 7 displays a certain memory address with non-human readable content.



Figure 7. Encrypted Text

After applying this decoding function at the same memory location, displayed in Figure 8, now the same memory location contains readable ASCII code that will be used to request a configuration file from a peer node, displayed in Figure 9. The request is accompanied by NET\_SERVER\_WORKER ID and an IP address.

After decrypting and activating itself, the binary again stops at Virtual Protect to take

		····· -····, ·
0063BEB8 🔶	1DB	ADD EBX,EBX
0063BEBA 🗸 7	5 07	JNE SHORT 0063BEC3
0063BEBC 8	B1E	MOV EBX,DWORD PTR DS:[ESI]
0063BEBE 8	SEE FC	SUB ESI,-4
0063BEC1 1	1DB	ADC EBX,EBX
0063BEC3 1	100	ADC EAX,EAX
0063BEC5	11DB	ADD EBX,EBX
0063BEC7 🗸 7	3 OB	JAE SHORT 0063BED4
0063BEC9 🗸 7	5 28	JNE SHORT 0063BEF3
0063BECB 8	B1E	MOV EBX,DWORD PTR DS:[ESI]
0063BECD 8	SEE FC	SUB ESI,-4
0063BED0 1	1DB	ADC EBX,EBX
0063BED2 🗸 7	'2 1F	JB SHORT 0063BEF3
0063BED4 4	8	DEC EAX
0063BED5	11DB	ADD EBX,EBX
0063BED7 🗸 7	5 07	JNE SHORT 0063BEE0
0063BED9 8	B1E	MOV EBX,DWORD PTR DS:[ESI]
0063BEDB 8	SEE FC	SUB ESI,-4
0063BEDE 1	1DB	ADC EBX,EBX
0063BEE0 1	100	ADC EAX,EAX
0063BEE2 ^LE	B DJ	IMP SHORT 0063RER8

Figure 8. Function Call used for Decryption



Figure 9. Decrypted text of the binary

care of some unfinished business. It loads nine new DLLs to perform internet related activities, as displayed in Figure 10. This behavior can be inferred because downloaded DLLs are related to wpcap, dhcp, and tcpip. Wpcap provides network intercept capabilities to the Kelihos binary, which is part of the method for gathering new user ID and password pairs for FTP and SMTP email traffic that are later used by other nodes for spamming and creating temporary internet file storage on stolen web servers.



Figure 10. Nine new DLLs loaded by Binary © 2017 ADFSL

To reiterate, there has not been any internet communication or activity so far in the process.

#### 3.3 Communication

In this segment, the communication channel will be discussed in detail; reaching out to its peers, establishing a connection, getting the config files, decrypting the config files and preparing them to send spam messages.

#### 3.3.1 First Communication

From now on, we will require simultaneous monitoring of the network traffic which will be performed by Wireshark in the demo case. The initial communication starts immediately after the child process takes control of the operation after loading the required DLLs for proper working of the malware. During our research, it was found that the binary uses a particular command at a precise location to communicate with its peers. We concluded that there were approximately 145 hard-coded Internet Protocol (IP) addresses that the malware tries to reach out in sets of five each. The precise location can be found under the Memory (M) tab as shown in figure 11 and 12.

- 1. MSWsock.dll under second section
  - (a) NtDeviceIOControlFile at location - 7530616E

75300000	00001000	MSWSOCK		PE header	Ing	R	RWE	CopyOnWr
75301000	00035000	MSWSOCK	.text,SANONTCP	Code,imports,exports	Ing	RE	RWE	CopyOnWr
75336000	00002000	MSWSOCK	.data		Ing	RV Copi	RWE	CopyOnWr
75338000	00001000	MSWSOCK	.rsrc	Resources	Ing	R	RWE	CopyOnWr
75339000	00003000	MSWSOCK	.reloc	Data,relocations	Inq	R	RWE	CopyOnWr

Figure 11. Location under MSWsock

ADD'ess Midule	Status	Olsastenbly	Commit
CHEMILE MINSBOK	Active	CALL DWERP FIR #5;[Cantdl1.HtDeviceInControlFile>]	Brok - 8, Arob - 12815, Bros - 18, Aros - 8, Broth - 1
750 M HE HEVEDIX	Rellur	CALL DANKS FTH 05:[(Anid11.HtievicvinEentral/1107]	Aru7 - 0, Aru1 - 0, Aru4 - 17907, Aru18 - 8

Figure 12. Breakpoints under MSWsock

The location may vary due to using different machines, but the last four digits will remain constant. When performing the steps one can add 616E at the end of the location of the starting point of the MSWsock.dll. Once you set the breakpoint at the following address, debug the program. The program will stop at the place with the function call:

MOV EBX, EAX

This is the location where the IP address gets stored before making a Transmission Control Protocol (TCP) connection. The value is stored in hex in the EAX registry and can be confirmed with Wireshark. As soon as the call is made, Wireshark displays a TCP connection request to the IP in the EAX registry. This can be viewed in Figure 13.



Figure 13. Proof of Hard-coded IP address

Since we knew the IP address from the Wireshark connection (77.123.63.149) it can be safely assumed that the IP is hardcoded in the binary. When we visited the hex address in the EAX Registry and checked for the value in '0E76D1F8' location it contained:

Hex 4D 7B 3F 95 to IP 77.123.63.149

This is the first check done by Kelihos binary to the following IP address, based on the hard-coded IPs in the binary. The binary attempts to establish the connection with the IP addresses one by one in the hope of securing a connection with one of them. In almost all cases, the binary is able to establish connection with one of the 145 IP addresses. If it is not able to establish the connection, it falls back to a list of hard coded domains to try and establish a connection. A list of these domains are shown in the figure 14.

The dominant ones are 'gorodkoff.com' and 'goloduha.info.' During the past year, Pas-

•	2014br.biz	•	goloduha.info	•	niwrebsa.info
•	abrora.biz	•	gorodkoff.com	•	pasbuyr.info
•	avroran.biz	•	gorotza.biz	•	pookagyx.info
•	bayermun.biz	•	hockelen.info	•	segbuktem.info
•	bypomsa.info	•	ibayermun.biz	•	usdivqo.info
•	chemp14.biz	•	jagesxij.info	•	omyxiglet.info
•	demyator.biz	•	jiqnipun.ru	•	onabgitry.info
•	ecuad69.biz	•	meuvbayt.info	•	ggabwav.info
•	ekidjop.info	•	mydear.name	•	zadofadsun.info
•	fahhtaz.biz	•	newcounter.biz		
•	fucmethev.info	•	niggawhat.net		

Figure 14. List of the Fast Flux domain names

sive DNS systems at Internet Identity (IID) recorded 3,261 distinct IP addresses used by goloduha.info. The researchers' monitoring station was observed by IID resolving gorodkoff.com, goloduha.info, and zavodchikshop.com at least once during each month from July 2016 through December 2016, proving that our "proxy node" was being used as part of the Fast Flux hosting.

#### 3.3.2 Second Communication

Once the initial TCP connection is established with one of the IP addresses, the binary tries to initiate a 164 bytes encrypted conversation with the IP address. The consistent thing in the communication is the presence of string 'lUUE..H@' at the starting of the message in the first 12 bytes, as depicted in Figure 15. This is the unique identifier that is used to confirm that Kelihos binary indeed sends the communication. Before this communication gets sent, it makes the following call:

Nt Device IO Control File 753044EE

The location can be found by the same manner as you found the previous location. In this case, you add '44EE' to the MSWsock.dll location and put a breakpoint at the following address. One may notice that the function call is the same, but it is the address which is the key here. Therefore, one has to be careful about the address because the function call is mentioned in ten other places in the binary when searched in OllyDbg. Once the call is made, it uses 'WSA Send' to send the initial communication.

topJents0    http	Expression_ Clear Apply Save
Time         Source         Definition           59         48. 1067930 192, 168, 120, 128         188, 220, 58, 89           124         25590 188, 230, 58, 89         192, 168, 120, 128           62         48, 2566320 188, 230, 58, 89         192, 168, 120, 128	Protocol Length Mro TCP 216 34912-80 [PSH, ACK] Seq=1 ACk=1 win=64240 Len=164 TCP 106 90-54912 [PSH, ACK] Seq=1 ACk=165 win=64240 Len=106 TCP 62 80-54912 [FIN, PSH, ACK] Seq=107 ACk=165 win=64240 Len=10
Follow TCP Stream (top.stream eq 13)	107 107
Stream Content	
$\begin{array}{c} \begin{array}{c} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 $	0 40 5 40 5 40 5 - 50 168 - 74 5 4 - 74 5 1 - 74 5 1 4 - 74 5 1 - 74 5 1 4 - 74 5 1 -

Figure 15. Initial communication with unique identifier 'lUUE..H@'

Next, it waits for a reply from the connected IP; in case it does not receive a response, it moves on to the next IP and performs the same process over and over again. Finally, it uses 'WSA Receive' when the binary can establish a connection and then it receives a consistent string of 227 bytes.



Figure 16. Olly Socket Trace displaying the back and forth communication

Next step, the binary sends a reply and communicates back and forth exchanging pertinent information with the established IP connection about how to obtain the config files. The information is encrypted, but the network communication can be viewed in Wireshark and can be confirmed with a special plugin named 'Olly Socket Trace,' being displayed in Figure 16.

#### 3.3.3 Third Communication

This is the most important section of the communication cycle. The section includes the process of receiving the encrypted config files and then displaying the decryption of the config files into the various fields of 'To,' 'From,' 'Subject' and 'Email Body' for the spam template.

After the above communication is established, the binary requests to receive config files. For the following, we would need to continuously monitor Wireshark and for better results of the experiment use the filter 'http.request.method == GET.' The binary uses HTTP protocol, as shown in Figure 17, to request for config files with the usage of the 'GET' command.

GET /file.htm HTTP/1.1

Info		Protocol
GET	/start.htm HTTP/1.1	HTTP
GET	/start.htm HTTP/1.1	HTTP
GET	/home.htm HTTP/1.1	HTTP
GET	/home.htm HTTP/1.1	HTTP
GET	/main.htm HTTP/1.1	HTTP
GET	/search.htm HTTP/1.1	HTTP
GET	/login.htm HTTP/1.1	HTTP
GET	/login.htm HTTP/1.1	HTTP
GET	/search.htm HTTP/1.1	HTTP
GET	/file.htm HTTP/1.1	HTTP
GET	/default.htm HTTP/1.1	HTTP
GET	/default.htm HTTP/1.1	HTTP
GET	/file.htm HTTP/1.1	HTTP

Figure 17. Some examples of GET config file request

Figure 18 displays a list of different '.html' file names that are used to obtain various GET config files:

•	default	•	install	•	search
•	file	•	login	•	setup
•	home	•	main	•	start
•	index	•	online	•	welcome

Figure 18. GET config files

After the files are received, the process of decrypting the data starts. Multiple levels of decoding, involving six to seven permutations, are used to convert the encrypted text into readable text. Figures 19 and 20 will give a more picturesque view of the commands use to decrypt the files and the decoded text.

1	115	C37	7E	4 62	2 72	61	73	óВ	ó1	2E	63	Fó	Dó	C4	73	77	50	50	6	Có	b	ra	5k	a.c	ÖÖÄ	swU	ÆÆ	
1	115	C37	7FJ	4 73	: 40	77	69	C6	46	62	C6	57	56	2E	Εó	56	- 43	7 8	4	68	s	aw:	iÆ	Fba	WU	æVG	∎h.	
1	115	038	B Ø1	4 F6	i D6	56	F5	66	69	E6	61	E6	63	69	61	Cć	7:	3 F	6	C6	ö	ÖVí	ŏf	iæa	æci	aÆs	öÆ	
1	115	038	811	4 57	47	69	Fó	Εó	73	40	79	61	68	Fó	Fó	28	6	3 F	6	Dó	W	Gii	öæ	s@y	ahö	ö.c	:ÖÖ	
1	115	038	82	4 45	76	61	73	69	Fó	72	Fó	77	73	óВ	69	13	1 31	+ 4	10 61 Evasiör					örö	röwski‼4@a			
1	115	038	831	4 F6	i C6	2E	63	F6	Dó	48	47	F6	69	C6	Fδ	Eć	i 51	54	0	62	2 öÆ.cöÖHGöiÆöæV@							
1	115	038	841	4 61	6B	2E	72	72	2E	63	Fó	Dó	40	73	72	23	23	3 1	3	35	5 ak.rr.cöÖ@sr##‼5							
1	115	038	851	4 48	9 47	56	Có	57	73	2E	Εó	56	47	48	77	72	6	17	9	Dó	0	@GVÆWs.æVGHwray				ıyÖ		
1	115	038	86	4 D6	40	67	56	72	69	7A	Fó	E6	2E	Еó	56	47	0	2 6	1	72	Ö	۵q۱	Ur	izö	æ.æ	VG	ār	
1	115	038	871	4 67	69	Еó	46	2E	72	61	67	69	73	68	57	Εđ	6	3 6	1	72	g	iæ	F.	rag	ish	Wæk	ar	
1	115	038	881	4 46	) 66	61	69	72	63	68	69	<b>C6</b>	46	73	56	Dć	69	2	E.	63	ē	Fa	ir	chĩ	ÆFs	vöi	c	
1	115	038	891	4 F 6	i D6	C5	72	69	63	68	40	73	47	72	56	56	- 43	74	17	72	ö	ÖÅI	ri	ch@	sGr	VVG	Gr	
1	115	038	BAJ	4 61	69	Еó	69	E6	76	2E	63	F6	Dó	08	Dó	61	7:	2 6	в	2E	a	iæ:	iæ	v.c	öÖם	Öar	ĸ.	
1	115	038	BB1	4 63	69	63	68	Fő	Εó	73	óВ	69	40	62	61	Eć	61	3 F	6	66	C	ic	hö	<del>e</del> sk	i@b	aæk	öf	
	F	ia		iro	1(	)	$\mathbf{F}$	nc	rt	m	to	А	$\mathbf{T}_{\prime}$	77	ŧ.,	of	C	n	•	m	r	$\mathbf{T}$	01	m	ոե	ht.	0	
i.		19		цe	- 1.2	7.		110	. 1. 1	/ 1 )	ьc	<u> </u>	1.0	- X	L			1.7	a.			1.1			110	1.1.	<u> </u>	
	881-9	7000	· ·	67		-DIIC	U CDI						1.00															
I	0843	782F 7838	2	57 8BCF		L HOI	H EDI	123			A	ddress	Hex	dunp			10.0	- 70					70	AS	CII			
	0843 0843 0843	782F 7830 7832	)	57 8BCE E8 74	2AFEFF	HOU	H EDI ECX,I L AR4	ESI 1828b			<u>A</u>	idress	Hex 4 6F	dunp	6	1 75	6C 2	73	74	65 6 75 7	5 64	48	70	68 0	CII Ul	.stee	3ph	
	0043 0043 0043	782F 7830 7832 7837	>	57 8BCE E8 74: 8A10	2AFEFF	FPUS Hou Cal	H EDI ECX,I L 004 DL.B	ESI 1a2ab Yte P1	IR DS:	[EAX]	A 1 1	<b>Idress</b> 15031E 150310	Hex 4 6F 4 61	dunp 72	0	1 75	<mark>60</mark> 21	73 61	74 72	65 6 74 6 79 4	5 <mark>64</mark> 9 73	40 2E	70 63	68 0 6F ai	CII ul	.stee va i	igph s.co	
	0043 0043 0043 0043 0043 0043	782F 7830 7832 7837 7837 7839	>	57 8BCE E8 74: 8A10 8ACA	2AFEFF	PUS HOU Cal Hou Hou	H EDI ECX,I 1 004 DL,B CL,DI	ESI 1a2ab Yte P1 L	IR DS:	[EAX]	A 1 1 1	ddress 150318 150310 150310 150310	Hex 4 6F 4 61 4 60 5 25	dunp 72 48	60 2	1 75 E 64	60 21 61	73 61	74 72 48 72	65 6 74 6 73 6	5 <mark>64</mark> 9 73 8 61	40 2E 77	70 63 75	AS 68 0 6F an 73 mi 25 4	Ul ul d nda	.stee va i @sh	igh s.co avus	
	0943 0943 0943 0943 0943 0943 0943	782F 7830 7832 7837 7837 7839 7838	>	57 8BCE E8 74: 8A10 8ACA 80E1	2AFEFF 44	PUS HOU CAL HOU HOU	H EDI ECX,I 004 DL,B CL,DI CL,4	ESI 1A2AB Yte P1 L	IR DS:	[EAX]	A) 1 1 1 1 1	ddress 15031E 150310 150310 15031E 15031E	Hex 4 6F 4 61 4 60 4 2E 4 63	dunp 72 48 63 6F 6F 60	60 8	175 E64 8	6C 21 61 32 3	73 61	74 72 40 72 61	65 6 74 6 73 6 6F 4 6F 6	5 64 9 73 8 61 8 61 6 2F	48 2E 77 6F 63	70 63 75 60 6F	AS 68 0 6F ar 73 nl 2E .0	CII ul nda con8 in 2	.stee va i @sh ro@ 1Ran1	9ph s.co awus aol.	
	0043 0043 0043 0043 0043 0043 0043 0043	782F 7830 7832 7837 7839 7838 7838 7838	>	57 8BCE E8 74: 8A10 8ACA 80E1 80F9	2AFEFF 44 44	FPUS HOU Cal Hou Hou And CmP	H EDI ECX,I 084 01,8 01,8 01,0 01,0 01,4 01,4	ESI 1A2AB Yte P1 L 4	IR DS:	[EAX]	A 1 1 1 1 1 1	ddress 150318 150310 150310 150318 150318 150328	Hex 4 6F 4 61 4 60 4 2E 4 63 4 48	dunp 72 48 63 6F 6F 6D 73 72	60 2 32	1 75 E 64 8 73	6C 21 61 32 3	73 61 48 68	74 72 48 72 61 6F	65 6 74 6 73 6 6F 4 6F 6 6	5 64 9 73 8 61 8 61 0 61 C 2E D 61	40 2E 77 6F 63 69	70 63 75 6C 6F	AS 68 0 6F ar 73 ni 2E .0 6D co 2E HS	CII ul nda con8 n 2 r2 1	.stee va i Øsh ro@ 1@aol Øho p	9ph s.co avus aol. .con ai .	
	0943 0943 0943 0943 0943 0943 0943 0943	782F 7838 7832 7837 7838 7838 7838 7838 7838	> • • • •	57 8BCE E8 74: 8A10 8ACA 80E1 80F9 74 84	2AFEFF 44 44	FPUS Hou Cal Hou Hou And Chp Je	H EDI ECX,I DL,8 CL,0 CL,4 CL,4 SHORT	ESI 1A2AB Yte Pi L 4 80437	TR DS: 7847	[EAX]	A 1 1 1 1 1 1 1 1 1 1 1 1 1 1	ddress 15C310 15C310 15C310 15C310 15C310 15C320 15C320	Hex 4 6F 4 61 4 60 4 2E 4 63 4 48 4 63	dunp 72 48 63 6F 6F 6D 73 72 6F 6D	60 2 32 48 2	1 75 E 64 8 73 0 6E	6C 21 61 32 3	73 61 48 68	74 72 48 72 61 6F 64	65 6 74 6 73 6 6F 4 6F 6 6F 7	5 64 9 73 8 61 8 61 0 61 0 61 2 48	40 2E 77 6F 63 69 60	70 63 75 60 6F 73	At 68 0 6F ar 73 m 2E .0 6D co 2E H 6E co	CII ul nda :om8 in 2 :r2 1 in2pns	.stee va i @sh ro@ 1@aol @ho # or	9ph s.co avus aol. .con ai . @nsn	
	0843 0843 0843 0843 0843 0843 0843 0843	782F 7838 7832 7837 7838 7838 7838 7838 7841 7843 7843	> • • • •	57 8BCE E8 74: 8A10 8ACA 80E1 80F9 74 84 84C9	2AFEFF 44 44	PUS Hou Cal Hou And Chp Je Tes	H EDI ECX,I DL,B CL,D CL,4 CL,4 SHORT T CL,I	ESI 1A2AB Yte Pi L 4 80437 CL	TR DS: 7847	[EAX]	A 1 1 1 1 1 1 1 1 1 1 1 1 1 1	ddress 150316 150310 150310 150316 150316 150326 150321 150321	Hex 4 6F 4 61 4 60 4 2E 4 63 4 63 4 63 4 63 4 63 4 63 4 2E	dunp 72 48 63 6F 6F 6D 73 72 6F 6D 63 6F	60 3 32 40 3 60 3	1 75 E 64 8 73 0 6E 4 64	6C 21 61 32 3 61 6	73 61 48 68	74 72 48 72 61 6F 64	65 6 74 6 73 6 6F 4 6F 6 6F 7 6	5 64 9 73 8 61 8 61 0 61 0 61 2 48 1 6F	48 2E 77 6F 63 69 60 60	70 63 75 6C 6F 73 2E	A1 68 0 6F ar 73 m 2E .0 6D co 2E H 6E co 63 .0	CTT UL I nda con8 in 2 ir2 1 ir2pns con4d	.stee Va i Osh ro@ 1@aol 2ho r 0r 0a	9ph s.co avus aol. .con ai . Qnsn ol.c	
	0943 0943 0943 0943 0943 0943 0943 0943	782F 7838 7832 7837 7838 7838 7838 7838 7841 7843 7843 7845 7845	> · · · ·	57 8BCE E8 74: 8A18 8ACA 80E1 80F9 74 84 84C9 75 0F	2AFEFF 44 44	PUS Hou Cal Hou And Chp Je Tes Jn2	H EDI ECX,I DL,B CL,D CL,4 CL,4 SHORT T CL,I SHORT	ESI 1A2AB YTE P1 L 4 80437 CL T 0043	TR DS: 7847 87856	[EAX]	A) 111111111111111111111111111111111111	ddress 15C31E 15C31C 15C31C 15C31E 15C31E 15C32E 15C32E 15C322 15C322	Hex 4 6F 4 61 4 60 4 2E 4 63 4 63 4 63 4 63 4 63 4 63 4 63 4 63 4 63 4 65	dunp 72 48 63 6F 67 60 73 72 6F 60 63 6F 60	60 2 60 2 40 2 60 2	1 75 E 64 8 73 0 6E 4 64	6C 21 61 32 3 61 61 48 6	73 61 48 68 74	74 72 48 72 61 6F 64 65	65 6 74 6 73 6 6F 4 6F 6 6F 7 6 2E 6	5 64 9 73 8 61 8 61 0 61 2 40 1 6F E 65	48 2E 77 6F 63 69 60 60 60 74	70 63 75 60 6F 73 2E 50	A3 68 0 6F an 73 ni 2E .0 6D co 2E H9 6E co 63 .0 6A or	CTT ul on8 on8 in 2 in2 f in2pns on4d i Q	.stee va i @sh ro@ 1@aol 2ho r @a gte.n	9ph s.co avus aol. .con ai Qnsn ol.c etPj	
	0943 0943 0943 0943 0943 0943 0943 0943	782F 7838 7832 7837 7838 7838 7838 7838 7845 7843 7845 7847 7849	> • • • • • • • • • • • • • • • • • • •	57 8BCE E8 74: 8A18 8ACA 80E1 - 80F9 - 74 84 84C9 75 8F 8ACA	2AFEFF 44 44	PUS HOU CAL HOU AND CHP JE TES JNZ HOU	H EDI ECX,I DL,84 CL,01 CL,44 CL,44 CL,44 CL,44 SHORT T CL,14 SHORT CL,01	ESI 1A2AB YTE P1 4 60437 CL CL T 0043	TR DS: 7847 87856	[EAX]	A 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Idress 150310 150310 150310 150310 150310 150321 150321 150323 150323 150323	Hex 4 6F 4 61 4 6D 4 2E 4 63 4 48 4 63 4 2E 4 63 4 2E 5 6F 5 6F	dunp 72 48 63 6F 6F 6D 73 72 6F 6D 63 6F 6D	60 3 32 48 3 60 3	1 75 E 64 8 73 0 6E 4 64	6C 21 61 32 3 61 61 48 6 63 7	73 61 48 68 74 65	74 72 48 72 61 6F 64 65 72	65 6 74 6 73 6 6F 4 6F 6 6F 7 6 2E 6 76	5 64 9 73 8 61 8 61 0 61 2 2E 0 61 2 48 1 6F E 65	40 2E 77 6F 63 69 60 60 60 74	70 63 75 60 6F 73 2E 50 73	AS 68 0 6F at 73 pt 2E .0 6D CO 2E HS 6E CO 63 .0 6A 01 2E 0	icii ul onda ion8 in 2 ir2 i in2pns ion4d i @jc:	.stee va i @sh ro@ 1@aol 1@aol 1@aol 0 1@aol 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	9ph s.co avus aol. .con ai. Qnsn ol.c etPj s.	
	0043 0043 0043 0043 0043 0043 0043 0043	782F 7838 7832 7837 7839 7838 7838 7838 7845 7843 7845 7845 7845 7849 7849		57 8BCE E8 74: 8A18 8ACA 80E1 80F9 74 84 84C9 75 8F 8ACA C0F9 8ACA	2AFEFF 44 44 84	PUS HOU CAL HOU AND CMP JE TES JN2 HOU SAR	H EDI ECX,I DL,8 CL,01 CL,44 CL,44 CL,44 SHORT T CL,1 SHOR CL,01 CL,41	ESI 1A2AB YTE P1 4 60437 CL T 0043 L	TR DS: 7847 87856	[EAX]	A 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Idress 150316 150310 150316 150316 150326 150321 150323 150323 150324 150324 150324	Hex 4 6F 4 61 4 60 4 2E 4 63 4 48 4 63 4 2E 4 63 4 63 4 65 4 65 4 63	dunp 72 48 63 6F 67 60 73 72 6F 60 63 6F 60 6F 60	60 3 32 48 3 60 3 54	1 75 E 64 8 73 8 6E 4 64 8 67	6C 21 61 32 3 61 61 48 6 63 7: 62 4	73 61 48 68 74 3 65 9 67	74 72 48 72 61 6F 64 65 72 72	65 6 74 6 73 6 6F 4 6F 6 6F 7 6 6F 7 6 2E 6 76 69 6	5 64 9 73 8 61 0 61 C 2E D 61 2 40 F E 65 6 66	48 2E 77 6F 63 69 60 60 74 69	70 63 75 60 6F 73 2E 50 73	A3 68 0 6F ar 73 pl 2E .0 6D C0 2E H5 6E C0 63 .0 6A 01 2E 0 C0 C0 C0 C0 C0 C0 C0 C0 C0 C	icii ul i nda ion8 in 2 ir2 i in2 i in2 i in2 i in2 i i in2 i i i i i i i i i i i i i i i i i i i	.stee va i @sh ro@ 1@aol 1@aol 1@aol 2ho m @a gte.n serv Bgrif	<pre>3ph s.co auus aolcon ai . @nsn ol.c etPj s. fi</pre>	
	0043 0043 0043 0043 0043 0043 0043 0043	782F 7838 7832 7837 7838 7838 7838 7838 7845 7843 7845 7845 7845 7845 7845 7845 7845		57 8BCE E8 74: 8A10 8ACA 80E1 74 84 84C9 75 8F 8ACA C0F9 80E1 C0F2	2AFEFF 44 44 84 84 86 86	PUS Hou Cal Hou And Chp JE TES JN2 Hou SAR AND	H EDI ECX,I DL,B CL,DI CL,44 CL,44 SHORT T CL,4 SHORT CL,4 SHORT CL,0 CL,0 CL,4 CL,0 CL,4 CL,0 CL,4 CL,0 CL,4 CL,0 CL,4 CL,0 CL,4 CL,0 CL,4 CL,0 CL,4 CL,0 CL,4 CL,0 CL,4 CL,0 CL,4 CL,0 CL,4 CL,0 CL,4 CL,0 CL,4 CL,0 CL,4 CL,0 CL,4 CL,4 CL,0 CL,4 CL,4 CL,0 CL,4 CL,4 CL,4 CL,4 CL,4 CL,4 CL,4 CL,4	ESI 1A2AB YTE P1 4 80437 60437 CL T 0043 L	TR DS: 7847 87856	[EAX]	A 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Idress 150310 150310 150310 150310 150321 150321 150323 150323 150324 150324 150324	Hex 4 6F 4 61 4 60 4 2E 4 63 4 63 4 2E 4 63 4 6F 4 63 4 63 4 63 4 63 4 63 4 63 4 63 4 63 4 63 5 65 6 7 6 7 6 7 6 7 6 7 6 7 6 7 6 7	dunp 72 48 63 6F 6D 73 72 6F 6D 63 6F 60 6F 60 6C 65	60 2 32 48 7 60 2 54 61 6	1 75 E 64 8 73 8 6E 4 64 8 67 E 2E	6C 21 61 32 3 61 61 49 6 63 7: 62 4 63 61	73 61 48 68 774 365 774 60	74 72 48 72 61 6F 64 65 72 72 58	65 6 74 6 73 6 6F 4 6F 6 6F 7 6 76 69 6 39 3	5 64 9 73 8 61 8 61 0 61 2 40 0 61 2 40 1 6F E 65 6 66 2 35	48 2E 77 6F 63 69 60 60 60 60 74 69 34	70 63 75 60 6F 73 2E 50 73 30	A3 668 0 667 at 773 nb 22E .c 660 cc 660 cc 663 .c 664 or 663 .c 663 .c 663 .c 663 .c 663 .c 663 .c 664 or 665 .c 665	iciii ul inda ion8 in 2 ir2 i in2pns ion4d i Qgc int bi ean.co	.stee Va i Osh ro@ 1@aol 2ho m 0r 0a gte.n gte.n Serv Bgrif onX92	<pre>3ph s.co avus aol. .con ai . @nsn ol.c etPj s. fi 5408</pre>	
	0043 0043 0043 0043 0043 0043 0043 0043	782F 7838 7832 7837 7838 7838 7838 7838 7845 7843 7845 7845 7845 7845 7845 7845 7845 7845	> ·	57 8BCE E8 74: 8A10 8ACA 80E1 74 84 84C9 75 8F 8ACA C0F9 8ACA C0F9 80E1 C0E2 8ACA	2AFEFF 44 44 84 84 84	PUS HOU CAL HOU AND CMP JE TES JNZ HOU SAR AND SHL OR	H EDI ECX, DL,8 CL,0 CL,4 CL,4 CL,4 SHORT CL,4 SHORT CL,0 CL,0 CL,4 CL,4 CL,0 CL,4 CL,4 CL,0 CL,4 CL,4 CL,4 CL,4 CL,4 CL,4 CL,4 CL,4	ESI 1A2AB YTE P1 L % 00437 CL CL T 0043 L	TR DS: 7847 87856	[EAX]	A + + + + + + + + + + + + + + + + + + +	Idress 150316 150310 150316 150316 150316 150328 150323 150323 150323 150324 150325 150326 150326 150326	Hex 5 6F 5 61 5 60 5 2E 5 63 5 48 5 63 5 6F 5 63 5 65 5 63 5 65 5 7 5 7 5 7 5 7 5 7 5 7 5 7 5	dunp 72 48 63 6F 67 60 73 72 6F 60 63 6F 60 6F 60 6C 65 33	60 2 60 2 40 2 60 2 54 61 6 2 70 2	1 75 E 64 8 73 8 6E 4 64 8 67 E 2E 8 63	6C 21 61 32 3 61 61 49 6 63 7: 62 4 63 61 6F 61	73 61 48 68 74 3 65 3 67 60 63 67	74 72 48 72 61 6F 64 65 72 72 58 61	65 6 74 6 73 6 6F 4 6F 6 6F 7 6 76 69 6 39 3	5 64 9 73 8 61 0 61 2 40 1 6F E 65 6 66 2 35 2E	48 2E 77 6F 63 69 60 60 60 60 60 60 60 60 60 60 60 60 60	70 63 75 6C 6F 73 2E 50 73 30 65	A5 68 0 66 at 73 nt 22 .c 60 cc 22 H5 66 cc 63 .c 64 or 66 cc 63 .c 63 .c 73 nt 74 or 74 or 74 or 75 or 76 or	CTT ul onda cons in 2 in2 T in2pns con4d Qgc inT bl ean.co 3 Bco	.stee va i Osh ro@ 1@aol 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	<pre>3ph s.co auus aol. .con ai. @nsn ol.c etPj s. fi 5408 .net</pre>	
	0043 0043 0043 0043 0043 0043 0043 0043	782F 7830 7832 7837 7839 7838 7838 7838 7838 7843 7843 7845 7844 7845 7847 7846 7847 7846 7845 7852 7854	> ·	57 8BCE E8 74: 8A18 8ACA 80E1 80E1 80E1 74 84 84C9 75 8F 8ACA C0F9 80E1 C0E2 8ACA 8888	2AFEFF 44 44 84 84 84	-PUS Hou Call Hou And Chp Je Tes Jn2 Jn2 Sar And Sar And Sar And Sar Hou Dr	H EDI ECX, DL,8 CL,0 CL,4 CL,4 CL,4 SHORT CL,4 SHORT CL,4 CL,0 CL,4 CL,0 CL,4 CL,9 CL,4 CL,9 CL,4 CL,9 CL,4 CL,9 CL,4 CL,9 CL,4 CL,4 CL,4 CL,4 CL,4 CL,4 CL,4 CL,4	ESI 1A2AB YTE P1 L 4 8 80431 CL T 8043 L F F	IR DS: 7847 87856 95:[EA	[EAX]	A 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Idress 15C31E 15C31C 15C31C 15C31E 15C32E 15C32E 15C323 15C323 15C323 15C325 15C326 15C326 15C326 15C326	Hex 4 6F 4 61 4 62 2E 63 4 63 4 63 4 63 4 63 4 63 4 63 4 63 4 65 64 65 65 65 65 65 65 63 8 8 8 8 8 8 8 8 8 8 8 8 8	dunp 72 48 63 6F 60 73 72 6F 60 63 6F 60 6F 60 6F 60 73 72 6F 60 73 72 8 72 73 72 73 72 73 72 73 72 73 72 73 72 73 72 73 72 74 74 75 72 75 7	60 2 32 48 7 60 2 54 61 6 1 73 7 60 2	1 75 E 64 8 73 8 6E 4 64 8 67 E 2E 8 63 3 63	6C 21 61 32 3 61 61 48 6 63 7: 62 4 63 61 6F 61 6F 61 6F 6	73 61 48 68 74 68 74 68 74 68 67 60 63 72 60	74 72 48 72 61 6F 64 65 72 72 72 58 61 60 60	65 6 74 6 73 6 6F 4 6F 6 6F 7 6 76 6 76 6 76 6 79 6 39 3 39 3	5 64 9 73 8 61 0 61 2 48 1 6F E 65 6 66 2 35 2 25 2 25 2 61 6 61 6 65	40 2E 77 6F 63 69 60 60 60 60 60 60 74 69 34 69 34 68	70 63 75 6C 6F 73 2E 50 73 30 65	A5 68 0 6F at 73 nd 2E .6 60 ct 60 ct 66 ct	CII ul ons ons nepos on4d egc: nT bi ean.co 3 Bco iissco	.stee Qsh ro@ 1@aol 2@ho r Qa 2@c.n 2@c.n 2@c.n 2@c.n 2@c.n 2@c.n 2@c.n 2@c.n 2@c.n 200 200 200 200 200 200 200 200 200 20	Paph s.co avus auus ai ensn ol.c etPj s. fi 5408 .net ah	
	0043 0043 0043 0043 0043 0043 0043 0043	782F 7830 7832 7837 7839 7838 7838 7838 7838 7838 7843 7843 7845 7844 7845 7844 7845 7845 7845 7855	· · · · · · · · · · · · · · · · · · ·	57 8BCE E8 74: 8A10 8ACA 80E1 80E9 74 84 84C9 75 8F 8ACA C0F9 8ACA C0F9 80E1 C0E2 80E1 80E1 80E1 80E1 80E2 8ACA 8888 47	2AFEFF 44 44 44 84 84 84	-PUSUA HOU Call Hou And Chp Je Jie Jie Jie Jie Jie Sar And Sar And Sar And Sar Hou Ince	H EDI ECX,I CL,04 CL,04 CL,44 CL,44 CL,44 CL,44 CL,44 CL,44 CL,01 CL,44 CL,01 CL,44 CL,01 CL,44 CL,01 DL,4 CL,01 BYTE EDI	ESI 142AB Yte P1 L 4 4 60437 Cl T 00437 L T 00437 F F	IR DS: 1847 87856 95:[EA	(EAX) X],CL	A 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	150310 150310 150310 150310 150310 150321 150321 150323 150323 150323 150323 150323 150323 150323 150325 150326 150326 150326 150326	Hex 4 6F 4 61 4 60 2E 63 4 63 4 63 4 63 4 63 4 63 4 63 4 63 4 63 64 65 63 63 63 63 63 63 63 63 63 63	dunp 72 48 63 6F 60 67 60 63 6F 60 66 65 33 64 69 63 6F 63 6F 63 6F	60 2 48 2 48 2 60 2 54 61 6 54 61 6 54	1 75 E 64 8 73 8 6E 4 64 8 67 E 2E 8 63 3 63 3 63 4 60 8 62	6C 21 61 32 3 61 61 49 6 63 7: 62 4 63 61 6F 61 6F 61 6F 6 69 6:	73 61 48 68 774 865 60 63 772 868	74 72 48 72 61 6F 64 65 72 72 58 61 6C 61 54	65 6 74 6 73 6 6F 4 6F 6 6F 7 6 6F 7 6 76 69 6 39 3 39 3 48 7 56 C	5 64 9 73 8 61 0 61 2 48 1 6F E 65 6 66 2 35 2E 2 2 2 4 6 1 6 1 6 2E	40 2E 77 67 63 69 60 60 74 69 34 65 68 68 68	70 63 75 6C 6F 73 2E 50 73 30 65 2E 72	AS 68 0 6F at 73 nf 72 60 ct 62 ct 63 64 or 74 ct 38 ct 74 ct 62 62 64 or 65 ct 66 or 75 ct 75	CII ul on8 in 2 in2 1 in2pns on4d Qgc in1 bl ean.co 3 Qco issco issco issco	.stee Qsh ro@ 1@aol 2@ho rro@ 0 2@ 0 2@ 2 0 2 0 0 2 0 0 0 2 0 0 0 2 0 0 0 2 0 0 0 2 0	aph s.co avus laol. .con ol.c etPj s. .net ah .j.b	
	0043 0043 0043 0043 0043 0043 0043 0043	782F 7830 7832 7837 7838 7838 7838 7838 7838 7845 7845 7845 7845 7845 7845 7845 784	· · · · · · · · · · · · · · · · · · ·	57 8BCE E8 74: 8A10 8ACA 80E1 80E9 74 84 84C9 75 8F 8ACA C0E9 80E1 C0E2 8ACA 8808 47 3BFB	2AFEFF 44 44 84 84 84	-PUS HOU Call Hou And Chp Je Tes Jn2 Jn2 Sar And Sar And Sar Hou Incc	H EDI ECX, B044 L 004 CL,01 CL,01 CL,01 CL,01 CL,01 CL,01 L,01 L,01 EL,01 L,01 EL,01 L,0	ESI 142AB Yte P1 L 4 4 60437 CL 7 0043 L F F PTR I EBX	IR DS: 1847 87856 95:[EA	(EAX) X],CL	A 1 1 1 1 1 1 1 1 1 1 1 1 1	ddress 150318 150318 150310 150310 150318 150320	Hex 4 6F 4 61 4 62 2E 63 48 48 48 48 48 48 48 48 48 48	dunp 72 48 63 6F 60 73 72 6F 60 63 6F 60 6F 60 66 65 33 64 69 63 6F 77 7 61 25	60 2 32 48 1 60 2 54 61 6 73 7 60 8 E6 1 63 8	1 75 E 64 8 73 8 6E 4 64 8 67 E 2E 8 63 3 63 3 63 3 63 8 62 6 06	6C 21 61 32 3 61 61 49 6 63 7: 62 4 63 61 6F 61 6F 61 6F 6 69 6: 61 E1	73 61 48 68 74 68 74 8 65 67 60 63 72 8 68 68 68 65 65 65 65 65 65 65 65 65 65 65 65 65	74 72 48 72 61 6F 64 65 72 72 58 61 6C 61 F6 62	65 6 74 6 73 6 6F 4 6F 6 6F 6 6F 7 6 6 76 6 6 9 6 39 3 39 3 48 7 56 C 56 6 56 6 57 7	5 64 9 73 8 61 0 61 2 48 1 6F E 65 2 35 2 2E 2 61 6 1 06 3 68	48 2E 77 6F 63 69 60 60 60 60 60 60 60 60 60 60 60 60 60	70 63 75 6C 6F 73 2E 50 73 30 65 2E 72 72	AS 668 0 667 al 667 al 660 c 600 c 60	ul u	.stee Qsh ro@ 1@ao1 2@ho r @a 2@ho r @a 2 gte.n 2 gte.n 2 gr1@y gr1@y cchaU# zeköfa böb s	Aph S.CO avus taol. .con ol.c etPj S. fi 5488 .net ah .j.b ÖVri baa0	

Figure 20. Encrypted text being decrypted with the function call

#### 3.3.4 Fourth Communication

```
Received: from unknown (HELO localhost) (%^C0%^Fnames^%@%^Fdomains^%^%@%^C6%^I^%.%^I^%.%^I^%.%^I^%.%
by %^A^% with ESMTPA; %^D%^R20-300^%^%
From: %^V0%
To: %^0%
Subject:
```

Subject: Date: %^D-%^R30-600^%^%

Figure 21. Spam template formation

Spam Template obtains information of the spam to be sent from different parts, as can be viewed in Figure 21 . The executable assembles everything and packages it before sending it out. The different categories that the executable stores information are:

- Fnames From username
- Fdomains From domain name
- From and To email addresses

Once the spam template is created, the executable sends an SMTP message in order to check whether it is allowed to send email or whether it is being blocked.

#### 3.3.5 Fifth Communication

After all the procedures are verified, the malware is ready to spam and spread evil to the entire world. The spam volume is quite high, often sending 1,000 emails in less than 15 to 20 minutes.

# 4. SPAM PRODUCTS

This section outlines the individual spam campaigns and explains the purpose and target market of the spam messages. Figure 22 helps in explaining it properly.

### 4.1 Pharma Spam

Pharma spam is the most dominant spam type sent by Kelihos and is the most consistent. It is spammed for ninety percent of the time during the year. During 2015, Kelihos started initially with the "Dr. OZ & Oprah Winfrey" spam, where it promised the best performance enhancement pills for men and skin care and weight loss products for women. None of this proved to be true as the sellers were distributing fake pills and the Federal Trade Commission took legal action against the company that was using Kelihos for advertising at that time, leading to a \$43 Million settlement against Sale Slash, LLC [Commission, 2016].

This was the time when it was thought that Kelihos, known as Waledac at that time, was dead. As the saying goes "the game is not finished until the final bell", Kelihos returned stronger and continued to spam people all over the world.

In 2009, when Waledac was a dominant force, it started to shift its spam pattern from SMS spy cam to Canadian Health & Care Mall and Canadian Pharmacy. These were websites where the user can buy Viagra pills for less than a dollar, but these were fake pills.

After the takedown of the Waledac botnet in 2011 by Microsoft and Kaspersky, Kelihos came into existence [Meisner, 2011]. A press release alleging a Russian citizen can be seen in Figure 23.

The attribute that related both Waledac and Kelihos is the similarity between the source code and the product being spammed. Since 2009, Kelihos is spamming links to





Since taking down the Kelihos botnet with our partners Kyrus Inc. and Kaspersky Labs in September, the Microsoft Digital Crimes Unit has continued to actively investigate the case and pursue new leads with the goal of holding the perpetrators behind the botnet accountable for their actions.

In an amended complaint filed today with the U.S. District Court for the Eastern District of Virginia, Microsoft alleges that Andrey N Sabelnikov, a citizen of Russia, is responsible for the operations of the Kellhös bothet.

Figure 23. Sabelnikov alleged to operate and control the Kelihos botnet

Canadian Health & Care Mall for the majority of its spam.



Figure 24. Snapshot of Canadian Health & Care Mall

#### 4.1.1 Domain Names

When the Kelihos botnet is spamming URLs for pharmaceutical products, the URL used in the spam does not point directly to the pharmaceutical website, but rather to a redirector site. However some domains have been used consistently over a period of many months, including those listed in Figure 25 25. Researchers used these domain names as beacons to identify spam-sending IP addresses infected with Kelihos.

The domains displayed in Figure 25 are different and recurring at times in the spam campaign.

asvhpwti[.]ru bleguzjn[.]ru blvqekte[.]ru canadianrxsale[.]ru curativebestcompany[.]ru curativebestinc[.]ru curativeonlinedeal[.]ru curingfamilymall[.]ru curingfamilytrade[.]ru curingfirsttrade[.]ru curinghotpurchase[.]ru curingonlineservice[.]ru dgwghslr[.]ru familydrugsreward[.]ru firstdruginvestment[.]ru

curativeonlinegroup[.]be gnhwigmd[.]be bestpillmart[.]com canadianherboutlet[.]com curativepillshop[.]com fasthealingelement[.]com organicremedyreward[.]com perfectcuringshop[.]com secureorganictrade[.]com smartpharmacymarket[.]com sveuxfrd[.]com thepillpurchase[.]com onlineremedymart[.]eu abargainingassociation[.]ru arbjubfn[.]ru

Figure 25. Domain names spammed by Kelihos

## 4.2 Pump and Dump Spam

The second most dominant spam affiliated to Kelihos botnet is pump & dump spam. These types of campaigns last a couple of weeks on average. The pump & dump operators trick people into buying penny stocks advertised in the spam messages [Bouraoui, 2015] [Nelson et al., 2013]. The spam promises that the stock is on the rise and its value will increase drastically, often with fraudulent or misleading statements about a new contract, patent, or discovery that is about to make the company much more valuable. Generally, these stocks are priced for less than 50 cents while some are 10-12 cents. The spam messages promise closing prices of 3-4 dollars in a short period of time. Stock symbols spammed by Kelihos over the last year or so were:

- GRYN Green Hygienes Holdings Inc.
- APTY APT Systems Inc.

- FZRO FlashZero Corp.
- CWTC Clearwave Telecommunication Inc.
- UPOT Indie Growers Association, Inc.
- SNXG Sunx Energy

Most of the stock symbols were spammed for a couple of weeks, but a few of them came back after taking a break. For example, APTY was first seen on January 22, 2016 and then seen frequently in January, February, and March. It was the most consistent symbol that was being spammed by Kelihos botnet for a long period.

### 4.3 Money Mule Spam

The Kelihos botnet also often sends spam for money mule or work at home position vacancies. The targets are mostly based on language and location. In this particular spam, the operators seek for unemployed workers or people looking for a job. They urge the reader to reply back to an email address with his/her personal information, promising to pay handsomely with flexible work hours. One of the biggest factors for this spam campaign was that the employee would have the option to work from home, which allowed readers to reply back with their information promptly. Different languages such as English, French, Italian, Spanish, Portuguese, and Dutch have been noted in this particular spam campaign. Notable organizations like Apple and Walmart were also used in some spam campaigns to attract readers.

## 4.4 Credential Phish Spam

Frequently, we encounter multi-language credential phish. In recent months, the Kelihos botnet targets mostly Polish and French banks, and attempts to steal user credentials by asking the victim to verify their information via clicking a link. The link leads to a phishing website and tries to steal the victims username and password. An example of such an email was documented in April 2016 and can be seen in the figure 26:

Deta: 20.04.2016 r. <htps: 0000000000000000000000000000000<="" 10.0016="" doi.org="" td=""><td>×</td><td>Date: 04.20.2016 / <h3> Access to your account inteligo is blockedf </h3></td></htps:>	×	Date: 04.20.2016 / <h3> Access to your account inteligo is blockedf </h3>
$q_{\rm T} M$ to consider that the second second biodistic CM is relative weighting the second		$\label{eq:product} \begin{array}{l} \Phi^{-}  is believed of a customer blocket account is the system FKO. The reason is unantituted accounts by paracoact-data is unantituted accounts by paracoact-data. To regar access, please with the owner of the account by togong into the account by togong intothe account by togong intot$
-to- Surdiczne pozdtawany -to- ZenpARQ3, 84522, PKO Bank Polisk-go- -go-et-W pozgodku jakchkoliwek pytakti24, prosiny o kontakt z informa 001 307 307-et-sp- -go-et-sp- -go-et-spgo- -go-ban - anal- count-8122, wyporenoweny automátyczne. Prosiny sa nego ne- op-bank - anal-count-8124, wyporenoweny automátyczne. Prosiny sa nego ne- dop-ban - anal-count-8124, wyporenoweny automátyczne. Prosiny sa nego ne- dop-bank - zene-bank - zene-bank - zene-bank - zene-bank - zene- bank - zene-bank - zene-bank - zene-bank - zene-bank - zene-bank - zene- sku - zene-bank - zene-bank - zene-bank - zene-bank - zene-bank - zene- sku - zene-bank - zene-bank - zene-bank - zene-bank - zene- sku - zene-bank - zene-bank - zene-bank - zene-bank - zene- sku - zene-bank - zene-bank - zene-bank - zene-bank - zene-bank - zene- kt - zene-bank - zene-bank - zene-bank - zene-bank - zene-bank - zene- sku - zene-bank		-to- Greetings, -to- Team PKO Foliah Bark  $dP \rightarrow \Phi^+ p_0$ have any spectrum, parase contact the hotme 801.507.507.40 $d \to d p_0$ -to- $d p_0$ -to- $d p_0$ -to- $d p_0$ - $d p_0$ - Those - and size generated automatically. Pease do not notice the hotmess of a D-matrix 0.50.535. Nimes-angle of the Barder Could for a manual of a D-matrix 0.50.535. Nimes-angle of the Barder Could for the matrix of a D-matrix 0.50.555. Nimes-angle of the Barder Could for the matrix of a D-matrix 0.50.555. Nimes-angle of the Barder Could for the matrix of the D-matrix 0.50.555. Nimes and the D-matrix 0.50.555. Nimes and the matrix 0.50.555. Nimes and the matrix 0.50.555. Nimes and the matrix 0.50.555. Nimes and the Nimes and the Nimess of
28868/322.adowy (kapita68/322, wp68/322.acony) 1 250 000 000 z8#322, ~(p= 		는 전 40 <

Figure 26. Polish Bank Phish Email

## 4.5 Kronos Banking Trojan

An interesting thing that was observed on November 9, 2016 was that, in addition to spamming the world, the Kelihos binary behaved covertly and dropped Microsoft Word document on the infected machines desktop[Arora & Warner, 2016e]. The document name can be viewed in Figure 27.



Figure 27. Pictorial view of the document link on the infected user's desktop

The intention was to surprise the user and hope that the document will be viewed out of curiosity. As expected, the 'oldversion.doc' was a malicious document and after clicking 'Enable Content,' it downloaded Kronos banking trojan malware. This was confirmed with Figure 28 that contains a string found in Ollydbg

Figure 28. Confirmation of Kronos malware with the help of OllyDbg

4B 72 6F 6E 6F 73 00 00 25 00 77 00 73 00 00 00 Kronos

# 5. RANSOMWARE

### 5.1 WildFire Ransomware

The latest addition to the Kelihos botnet was WildFire Ransomware. On July 8, 2016, a Kelihos sample was encountered that was sending a Dutch-language spam with a link to a Microsoft Word document [Arora & Warner, 2016b]. The behavior has never been seen before and it was the first time that Kelihos botnet was distributing links to ransomware. Ransomware has evolved drastically and seems to be the most profitable form of malware distributed by malware authors. Through a single click on a malicious link or enabling a macro script, the malware has the ability to encrypt all the files on a victim's machine and requests a payment in return for decrypted files. Figures 29 and 30 display the original email in the Dutch language and its translation to English.

Subject: Mislukte afleverpoging BT-32084	
Transportbødri ()f. Butterink. B.V. Westkamald (B) 1060 3542. DA utrecht	
Geachte heer / mevrouw,	
op donderdag 7 jull heeft een van onze chauffeurs onstrekt 11,00 opprokeett om een pakket af te leveran Angezien dit niet is op luikt villen wij ur gang versoeken om op sopkoelt mogelijk een nituew af byraak te maken u kont een nieuw afprisak maken door het volgende formulier te downloaden, in te vullen an retour te malien naar infordrangoordheil liberitig al. <u>Buennen</u> of volgende Somalier formulier het op infordatie is het de lavering	
Met vriendelijke groet,	
Anna Dorst	
De informatie verzonden in dit e-mail bericht is automatisch gegenereerd en uitsluitend bestemd voor de geaddresseerde. van deze informatie door anderen dan de geadresseerde is verboden.	Geb

Figure 29. Word document link being distributed in the email

When translated to English, the message states:
Subject: Unsuccessful delivery attempt BT-32084
Transport Buitink B.V.
Westkanaaldijk 160
3542 DA Utrecht
Dear Sir / Madam,
On Thursday, July 7th at about 11:30 our drivers tried to deliver a package.
Since this was not successful, we would like to request to make a new appointment as soon
as possible.
You can create a new appointment by downloading the following form to complete and
return by email to info@transportbedrijfbuitink.nl
http://bestandend.transport[redacted].nl/BT-32084.doc
(This form also contains delivery HINTS)
Sincerely,
Anna Dorst
The information contained in this email message is automatically generated and intended
solely for the addressee. Use of this information by anyone other than the addressee is
prohibited.

Figure 30. Word document email translated in English

In this particular case, the message informs the user of an unsuccessful package delivery. The user is required to fill a form in order to reschedule the delivery and is requested to click the embedded link to download a Microsoft Word document. Once the Word document opens, the document is presented in "Protected View" and requires "Enable Editing".



Figure 31. Word document in protected view

Once enabled, it followed a similar process required by most hostile macro scripts "Enable Content". After fulfilling all requirements by the Word document, the macro leverages a connection with its command and control center in order to encrypt the files on the machine. The process can be better understood with help of Figures 31, 32 and 33



Figure 32. Word document asking to enable content

YOUR FILES ARE ENC BY WILDFIRE LOCK	RPTED IR
The price for unlocking is \$2	19
Navigate to one of the websit #c2_url_0#/#uid# #c2_url_0#/#uid# #c2_url_0#/#uid# #c2_url_0#/#uid# folder for more information of	is below to unlock your files me_(muldi).tet located (n your documents n for to unlock your files
You have 7 days before the pr	ice increases to \$/
All your files have been enc. All your files have been enc. The only way to get your file The decryption password will fou have until Bayment, dead file of the second second second because the second second second Visit one of the wesites bei a target "_BLANG" herf "sc2 a target "_BLANG" herf "sc2 a target "_BLANG" herf "sc2 a target "_BLANG" herf "sc2 a target "_BLANG" herf "sc2 fit these websites don't work 1. Dominds the TOB Fromer D' 2. Intail and then open the 3. Intaile the for Broase Bhu	<pre>opted by Ultrice Looser Untel alton and Ultrice Looser is back is by purchasing the decryption passand's list (is by purchasing the decryption passand's list (is by purchasing the price locates) to bollies/(Neuros)9991 a site to receive your files! The only may to recover your files is by purchasing the decryption passand's is to purchas your decryption passand's in the norther your decryption passand's interference of the price locates and the price of the site of the purchasing interference of the price of the price of the price of the price interference of the price of the price of the price of the price interference of the price of the price of the price of the price interference of the price of the price of the price of the price of the price of the price of the price of the price of the price of the pr</pre>
Antivirus software will NOT b Personal ID: #uid# Visit one of the websites bel #c2_wr1_8/#uid# #c2_wr1_1#/#uid# #c2_wr1_1#/#uid# #c2_wr1_1#/#uid#	+ able to recover your files! The anly way to recover your files is by purchasing the decryption bassword, no to purchase your decryption password!
If these websites don't work 1. Download the TOR Browser B 2. Install and then open the 3. Inside the Tor Browser Bun	Valler be steps below much http://www.torwnject.org/projects/torbrowser.html.en#downloads for Browser bundle. Ei enwiget to st_context muld#
http://exithub1.su http://exithub2.su http://exithub-sug.su	

Figure 33. Wildfire Encryption Ransomware ransom note

Different payment sites are listed where the user can pay the ransom amount in Bitcoin and receive the decryption key. This was a significant change for the Kelihos botnet given that it normally targets victims with less aggressive methods. The introduction of ransomware made the long lasting Kelihos botnet extremely treacherous.

## 5.2 CryptFile2 Ransomware

On August 4, 2016, another interesting addition to the long-lasting Kelihos spam was that American Airlines themed spam messages delivered Microsoft Word documents, which eventually delivered CryptFile2 ransomware [Arora & Warner, 2016a]. The ransom note is mentioned in Figure 34



Figure 34. CryptFile2 Encryption Ransomware ransom note

## 5.3 No\_More\_Ransom Ransomware

On November 30, 2016, Kelihos spammed a wide variety of payloads, including a banking trojan, credential phishing, and a new ransomware variant. The criminals altered their malware to change the extension of encrypted files to ".nomoreransom" poking fun at the "No More Ransomware" campaign [No More Ransom, 2016] started by National High Tech Crime Unit of the Netherlands police, Europol's European Cybercrime Centre, Kaspersky Lab, and Intel Security. Rather than being cowed by the new public service campaign, the criminals challenged them. This particular spam campaign was geo-targeting Australian email addresses ending in '.au' with a lure impersonating Bank of America to trick the users to believe that the spam is legitimate and coming from a well-established corporation.

### 5.3.1 Inauguration of JavaScript

In this campaign, the infection vector changed from a Microsoft Word document to a JavaScript file. Clicking the link in the email downloaded a zip file which contained a small JavaScript program [Arora & Warner, 2016f]. The necessary details of the zip file are visible in Figure 35



Figure 35. Downloaded zip file containing Java Script

After the JavaScript is executed, the malware contacts the command and control center and encrypts the file system. Afterwards, it displays the following ransom note, noted in Figure 36, in Russian as well as in English.



Figure 36. Ransom note of Troldesh ransomware in Russian and English

As can be seen in the ransom note, the extension of the file is changed to 'no\_more\_ransom'. On further analysis, it was found that it was 'Troldesh' ransomware.

### 5.3.2 Pony Info Stealer Malware

After encrypting the files on the victim's machine with the Troldesh ransomware, the malware also downloaded the Pony information stealer malware. This behavior is unique and has never been associated with Kelihos malware. Even though the files are encrypted, the malware still wants to acquire additional information from the victim's computer. Figure 37 depicts the admin page of Pony malware.

🚱 💭 🔹 🖂 http://ipieceofcake.com/wprconter	uptoads.	+ 4 × 2 Bing
🛉 Fevorites 🛛 🙀 🙋 Suggested Sites 🔹 🙆 Web	ce Gallery 🕶	
🔏 Авторизация		0 · 0 · • •
	Авторизация	
		-
	Пароль	-
	I Jatomerre napote	
	Second Second	6

Figure 37. Pony Info Stealer Malware Admin Panel

# 6. GEO-TARGETED SPAM

## 6.1 Europe Geo-Targeted with Panda Zeus

Perhaps the clearest example of geo-targeting comes from a set of spam campaigns conducted on August 12, 2016 by Kelihos. The botnet was geo-targeting based on the top level domain of the recipient's email addresses [Arora & Warner, 2016d]. Some examples of the specific targeted spam campaigns were:

- If you are a ".de" you get "German banking" spam that drops a Word doc that leads to a Panda Zeus infection
- If you are a ".co.uk" you get "British banking" spam that drops a Word doc that leads to a Panda Zeus infection
- If you are a ".it" you get invited to start a romance with lyudmilafedoji@gmail[.]com
- If you are anyone else, you get pill spam.

The Zeus banking trojan is well-known among the information security community. Zeus is a form of malware that targets various operating systems and tries to steal financial data; especially, banking information, credit card, social security, and so on [Kaspersky, 2010]. While this seemed a dramatic change in the Kelihos botnet spamming techniques, it is merely a sign of the "Spam as a Service" model used by Kelihos. Any malware actor can hire the Kelihos spammers to deliver their message or payload. The same mechanism, as previously mentioned, was used to spread several different malware campaigns and target the geographies desired by the customer.

## 6.2 Canada Geo-Targeted with Desjardins Phish

On August 16, 2016, another example of geotargeting was observed. Email addresses ending with ".ca" were targeted with a French language spam message for one of many Desjardins phishing websites [Arora & Warner, 2016c]. The link advertised in the spam went was of a credential phishing form, intended to steal the username and password of users of Desjardins Bank. The spam message in French and English is shown in Figure 38.

ubject: Solutions en ligne Desjardins 🕺 🕷	Subject Desjardins Online Solutions
her membre AccesD, ors de votre dermiere connexion dans le service en ligne Desjardins, notre steme a decele une erreur de avigation.	Dear AccesD member, During your last connection to the online service Desjardins, our system detects an error of navigation.
ous trouverez ci-joint les causes probables :	You will find the probable cause attached:
Vous n'avez pas ferme votre navigateur. La deconnection de votre session du service en ligne n'a pas ele faite apres ilitation. Vous avez terme votre navigateur avant de completer votre operation. Votre anvigeture neropont pas aux evigences minimales. ette enreur n'affecte en aucun cas votre comple et son fonctionnement, vous devez utelois reactiver ter service en ligne. Desjardins en sulvant les etapes ci-dessous . eulleis sulvar les bratuctions sulvantes afin de neactiver votre service en ligne. puyer i ci pour commence: .the plimembre acceed com-page-reactivation-5354- cost-desjardins comivninge.	You do not close your browser.     The deconnection your session online service has not been made after use.     The deconnection your session online service has not been made after use.     Your drowser does not meet the minimum requirements.     This error does not after this may case your account and its operation, however, you must reactivate     Desjardins your online service by following the steps below.     Please follow the instructions to reactivate your service online.     Cick here to get started this limitmem accessd com-page-reactivation-5354-accesd-desjardins convientigne     (c) tham 1996 to 2015, Desjardins Group, All rights reserved.
) 1996-2010, Mouvement des casses bespirations : rous drots reserves. IFORMATION ET DES-BOINNEMENT AU COURRIEL esjardins - Sege social 85, boulever (Daebec) 85, boulever (Daebec) 84, 148 332-245 bou 1 686 261-5133 alec: 418 833-4550 met	INFORMATION AND EMAIL TO UNSUBSCRIBE Degiardins - Head Office Sp. budievard Alphone-Degiardins Levis (Disehec) Geo/WM7 Sub1.: 48 833-2215 or 1 866 281-5133 Tele:: 418 833-253 Tele:: 418 833-253 Tele:: 418 833-253 Status - 418 83-253 Status - 418 83
ealaran alfacalaran a com	

Figure 38. French Desjardins Phishing Email; Google Translate

### 6.3 United States of America Geo-Targeted with Nymaim

On August 30, 2016, Kelihos began geotargeted US based emails ending with the top level domain .us by spamming the online shopping site Amazon. The Kelihos botnet was delivering Nymaim banking trojan with an Amazon Gift Card theme [Arora et al., 2016]. In this case, the link in the spam body downloaded a Word document, which downloaded a Nullsoft Installer, and eventually executed the Nymaim banking trojan.

# 7. BEHAVIOR

It is well known that the Kelihos botnet behaves differently based on the network connection type [Yang, 2012]. The behavior changes in accordance to the network communication and ability to send spam. The network connections that will be referred in the following section are:

- 1. Network Address Translation (NAT) Private IP and internal facing
- 2. Bridged Mode Public IP and external facing

## 7.1 Network Address Translation

When the Virtual Machine or the infected computer is in NAT mode, with an IP address that is not directly reachable from the Internet, the Kelihos botnet behaves like a client or work server. It connects to a single node and receives the information. This means that it receives a single spam template and sends out the same spam message to everyone with an identical subject and message content. A single URL and similar text is used in the spam message that is distributed in a single run.

## 7.2 Bridged

When the Virtual Machine or infected computer is in bridged mode, meaning that it requests or is assigned a publicly addressable IP number, the Kelihos botnet drastically changes its behavior. Kelihos acts as a proxy server, where it receives not one but many spam templates and send them in different directions. Other Kelihos nodes approach the server to obtain various spam messages for them to send. In bridged mode, it acts as a proxy as well as a client; thus, receiving spam templates and forwarding them to various other clients or servers.

## 7.2.1 Credential Exchange

Each Kelihos-infected computer has the capacity to steal userids and passwords from the user logged in at that station, particularly focusing on email and FTP credentials. Stolen credentials are passed upstream to the C&C server. When a node is in bridge mode, Kelihos receives some of these stolen credentials to test and logs into various targets using the FTP addresses and checking for the ability to write files. The SMTP credentials are tested and, if they work, are used to send spam disguising itself as the user whose credentials were used. Kelihos receives a list that includes 'Username', 'Password', 'From'. and 'To' to be used for the spam message. After a successful establishment of connection and logging into the machine as the user, the spam is sent out using the same email address within one or two seconds. Another interesting observation is that the same server IP address is used for different username and password logins. Once the email is sent, the malware logs in with a different account and keeps on repeating the process. On average, for a 30 minute run it exchanges approximately 700-800 FTP and SMTP credentials combined. With the given quantity, one can imagine how many credentials are being circulated across the globe. This is one of the main reasons why Kelihos is considered to be the most poisonous and resilient spam botnet in the entire world.

# 8. FUTURE WORK

While the Kelihos botnet has successfully endured through multiple take-down attempts, the researchers share everything they learn about the botnet with law enforcement and the greater anti-virus community. We will continue to document the Kelihos botnet's regular spam campaigns and seek a greater understanding of its infection and communication methodologies as we train additional team members and begin to pursue other botnets in a similar fashion. We would welcome contact with other researchers who would like to see similar programs adopted in their research or teaching curriculum.

## REFERENCES

Adair, S. (2012, December). Could it be storm worm 3.0/ waledac 2.0? Retrieved from http://www.shadowserver.org/ wiki/pmwiki.php/Calendar/20101230

Arora, A., Gannon, M., & Warner, G. (2016, August). Amazon gift card from kelihos! garwarner.blogspot.com. Retrieved from http://garwarner.blogspot.com/ 2016/08/ amazon-gift-card-from-kelihos.html

Arora, A., & Warner, G. (2016a, August). American airlines spam from kelihos delivers ransomware. garwarner.blogspot.com. Retrieved from http://garwarner.blogspot.com/ 2016/08/american-airlines-spam -from-kelihos.html

Arora, A., & Warner, G. (2016b, July). Kelihos botnet delivering dutch wildfire ransomware. garwarner.blogspot.com. Retrieved from http://garwarner.blogspot.com/ 2016/07/kelihos-botnet-delivering -dutch.html

Arora, A., & Warner, G. (2016c, August). Kelihos botnet sending geo-targeted desjardins phish to canadians. garwarner.blogspot.com. Retrieved from http://garwarner.blogspot.com/ 2016/08/kelihos-botnet-sending-geo -targeted.html

Arora, A., & Warner, G. (2016d, August). Kelihos botnet sending panda zeus to german and uk banking customers. garwarner.blogspot.com. Retrieved from http://garwarner.blogspot.com/ 2016/08/kelihos-botnet-sending -panda-zeus-to.html Arora, A., & Warner, G. (2016e, November). Kronos banking trojan and geo-targeting from kelihos. garwarner.blogspot.com. Retrieved from http://garwarner.blogspot.com/ 2016/11/kronos-banking-trojan-and -geo-targeting.html

Arora, A., & Warner, G. (2016f, November). Nomoreransom aka troldesh ransomware delivered by kelihos. garwarner.blogspot.com. Retrieved from http://garwarner.blogspot.com/ 2016/11/nomoreransom-ransomware-by -kelihos.html

Bouraoui, T. (2015). Does pump and dump affect stock markets? International Journal of Trade Economics and Finance, 45.

Bureau, P.-M. (2011). Same botnet, same guys, new code. Virus Bulletin International Conference.

Commission, F. T. (2016, February). Cases
and proceedings: Sale slash, llc. Retrieved
from https://www.ftc.gov/
enforcement/cases-proceedings/
142-3247/sale-slash-llc

Dietrich, C. J., Rossow, C., & Nobert, P. (2013). Cocospot: Clustering and recognizing botnet command and control channels using traffic analysis. *Elsevier*, 475-486.

Kaspersky. (2010). Kaspersky lab. Retrieved from https://usa.kaspersky.com/ internet\-security\-center/ threats/zeus\-trojan\-malware\# .V97n0vArKM8

Kerkers, M., Santanna, J. J., & Sperotto, A. (2014). Characterisation of the kelihos. b botnet. Springer Berlin Heidelberg: IFIP International Conference on Autonomous Infrastructure, Management and Security.

McAfee. (2016, June). Mcafee labs threats report. Retrieved from http://www.mcafee.com/us/ resources/reports/ rp-quarterly-threats-may-2016.pdf

Meisner, J. (2011, September). Microsoft neutralizes kelihos botnet, names defendant in case. Microsoft. Retrieved from http://blogs.microsoft.com/ blog/2011/09/27/ microsoft-neutralizes-kelihos -botnet-names-defendant-in-case-2/ #sm.0000i7mgzgrjpfddy8k1vahomseh5

Nadji, Y., Antonakakis, M., Perdisci, R., Dagon, D., & Lee, W. (2013). Beheading hydras: performing effective botnet takedowns. New York, NY, USA: ACM SIGSAC Conference.

Nelson, K. K., Price, R. A., & Rountree, B. R. (2013). Are individual investors influenced by the optimism and credibility of stock spam recommendations? *Journal* of Business Finance & Accounting, 1155-1183.

No more ransom. (2016, July). Retrieved from https://www.nomoreransom.org/

Rossow, C., Andriesse, D., & Werner, T.
(2013). Sok: P2pwned-modeling and evaluating the resilience of peer-to-peer botnets. Security and Privacy (SP), 2013 IEEE Symposium.

Singh, K., Guntuku, S. C., Thakur, A., & Hota, C. (2014). Big data analytics framework for peer-to-peer botnet detection using random forests, information sciences. *Elsevier*, 278(0020-0255), 488-497. Stringhini, G., Hohlfeld, O., Kruegel, C., & Vigna, G. (2014). The harvester, the botmaster, and the spammer: on the relations between the different actors in the spam landscape. New York, NY, USA: 9th ACM symposium on Information computer and communications security (ASIA CCS '14).

Tech, M. (2016, August). Significant increase in kelihos botnet activity. Retrieved from https://www.malwaretech.com/2016/ 08/significant-increase-in-kelihos -botnet-activity.html

Werner, T. (2013, February). Kelihos botnet taken down live on stage. Retrieved from http://www.h-online.com/security/ news/item/Kelihos-botnet-taken -down-live-on-stage-1813580.html

Yang, K. (2012, July). Fighting against kelihos botnet. BlackHat. Retrieved from https://media.blackhat.com/ad-12/ Yang/bh-ad-12-the-endless-game -yang-slides.pdf