## AutoIt Hata Ayıklaması

written by Mert SARICA | 1 February 2017 Hem Pi Hediyem Var oyununun altıncısına hem de AutoIt Bankacılık Zararlı Yazılımı başlıklı blog yazıma konu olan zararlı yazılımı/betiği incelediğimizde, AutoIt'in son yıllarda zararlı yazılım geliştiriciler tarafından sıklıkla kullanıldığını görebiliyoruz. APT gibi hedeflenmiş siber saldırılarda da AutoIt ile geliştirilmiş zararlı yazılımların kullanılıyor olması, zararlı yazılım analistleri ve zararlı yazılım analizi becerisine sahip siber güvenlik uzmanları tarafından analiz edilebilmesini ihtiyaç haline getirmektedir.

Wikipedia'dan alıntı yapacak olursak, "AutoIt, Microsoft Windows için ücretsiz bir otomasyon yazılımıdır. Yazılımın ilk versiyonları tamamen otomasyona yönelik hazırlanmış olsa da sonradan kapsamı genişletilerek hemen her türlü uygulamanın geliştirilebileceği bir programlama aracı haline gelmiştir. Bir AutoIt betiği, AutoIt yorumlayıcısının yüklü olmadığı bilgisayarlarda çalışabilecek şekilde, sıkıştırılmış bir EXE programı haline getirilebilir."

Eğer "AutoIt Bankacılık Zararlı Yazılımı" başlıklı blog yazımdaki gibi şanslıysak, elimizdeki AutoIt betiğini (script) çeşitli hata ayıklama (debug) araçları ile analiz edebiliriz. Eğer derlenmiş, exe uzantılı bir AutoIt dosyası ile karşı karşıya isek bu durumda yapacağımız ilk iş, derlenmiş AutoIt dosyasını, betiğe çevirmek olacaktır.

Derlenmiş AutoIt dosyasını betiğe çevirmek için Exe2aut aracından faydalanabiliriz. Exe2aut aracını çalıştırdıktan sonra exe uzantılı AutoIt dosyasını araca sürükledikten sonra betik dosyasına kolaylıkla ulaşabiliyoruz.



Peki betiğe ulaştık, şimdi ne yapacağız ? AutoIt'in web sayfasında yer alan Sıkça Sorulan Sorular sayfasına bakacak olursak, hata ayıklama için çeşitli araçlardan faydalanabileceğimizi görebiliyoruz.

6. Pi Hediyem Var oyununda kimilerinin safe betiğini analiz ederken hata ayıklama araçları yerine ConsoleWrite(), MsgBox() gibi ekrana değişkenlerin sahip olduğu değerleri yazmak için kullanılan fonksiyonlardan faydalandığını gördüm. Her ne kadar bu da bir yöntem olsa da işleri kolaylaştırmak ve daha hızlı ilerlemek için hata ayıklama araçlarından faydalanmanızı tavsiye ederim. Tabii kimi zaman hata ayıklama araçlarından faydalanmanızı tavsiye ederim. Tabii kimi zaman hata ayıklama araçlarından faydalanmanızı da olasıdır. Örneğin yine 6. Pi Hediyem Var oyununda, hata ayıklama araçlarından olan Dbug aracını AutoIt programının son sürümü ile kullanarak safe betiğini analiz etmeye çalışanlar, #comments-start ile #comments-end takıları arasında yer alan gizlenmiş (obfuscated) verilerin hatalı olarak çözülerek diske yazıldığına şahit oldular. Bu ve benzer sorunlarla karşılaşmama adına, zararlı yazılımın geliştirildiği AutoIt sürümü ile betiği analiz ederseniz, sorun yaşama ihtimaliniz oldukça düşecektir. AutoIt sürümünü bulmak için ise betik ile birlikte gelen AutoIt programının karakter dizilerini (strings) incelemeniz yeterli olacaktır.

Ħ	H	lex W	ork	shop -	[C:\U	sers\N	lert\De	esktop	\lsass	s.exe]									X
PT 002 Bå	2	File	Edit	Disk	Opti	ons	Tools	Plug-	Ins V	Vindo	w He	elp		5				-	e x
iie	7	38	8	3	' 🖣 🕻	🕄 🖙	126	#1	<b>A A</b>	<b>2</b>	3		▼ 🖡	₽ %	15 🐼 🐷				
1		<b>16</b>	6	🕺 🍫	• 🐁 😸	1		Legac	y ASC	II •	-	• •	<b>•</b> •••		•				
7		2			0	1	2	3	4	5	6	7	8	012	3456 <mark>7</mark> 8		Data Inspector	offset 0x0	<sup>+</sup> • × 000020
)ata		000	00	201	00	00	00	00	00	00	00	2E	74		<mark>.</mark> t		int8	46	
Vis		000	00	20A	65	78	74	00	00	00	45	BF	08	ext	E		uint8	46	
2		000	00	213	00	00	10	00	00	00	C0	08	00				int16	29742	
Zer		000	00	21C	00	04	00	00	00	00	00	00	00				uint16	29742	
•		000	00	225	00	00	00	00	00	00	00	20	00				int32	2019	
		000	00	22E	00	60	2E	72	64	61	74	61	00	• `•	rdata.		uint32	2019	-
		000	00	237	00	52	CC	02	00	00	DO	08	00	.R.			Expression Cal	c	<b>↓ • ×</b>
		000	00	240	00	CE	02	00	00	C4	80	00	00				Signed	▼ 3	2 b 🔻
	l	<u></u>	00	249	0.0	00	00	00	$\cap \cap$	00	00	$\cap \cap$	00				1		
	I.	lsa 🛍	ISSS.							1.2									
*	St	ructu	ires		•			1 <del>01</del> E	24			2	2362	instand	ces of 'string	gs' found in <sup>,</sup>	C:\Users\M	lert\Desk	top\lsa
#	Ν	lemb	er 🛙	9		Valu	ie (dec	)	Valu	e (hex	) / :	Siz	Add	ress 🖻	Length 🖻	Length 🖻			-
													000	BFC90	23	17 🔶	AutoIt3	.exe	
										000	BFCAE	23	17	Produc	tName				
											000	BFCC8	33	21	AutoIt	v3 Script			
												000	BFCF2	29	1D 🔪	Produc	tVersion		
fiewer													000	BFD10	23	17	3, 3, 12	, 0	=
cture \														זרחזנ	<u></u>	17		nfa	-
Stru	•					111							≝ ∰C	ompare	Checksu	m 🛅 Find 🖣	Bookmar	ks   🖪 Out	put
Fir	d	AL C	om	olete.					Cu	rsor:	00000	568	Car	et: 0000	00208 9	34400 byte	5 O'	VR MOD	READ
	0	9	6	0	He	Work	sh										No 12	<b>(</b> )) 11	:45

Hata ayıklama araçları (betikleri) arasında Dbug aracı, diğer araçlara kıyasla daha kullanışlı olduğu için onunla ilerleyebilirsiniz.

Dbug aracını kullanmak için öncelikle Auto IT script editörü olan SciTE aracını yüklememiz gerekiyor. Dbug aracının kurulum paketinden çıkan \_Dbug.au3 dosyasını, analiz etmek istediğimiz safe betiği ile aynı klasöre koyduktan sonra safe betiğinin ilk satırına #Include "\_Dbug.au3" satırını ekliyoruz. Bu işlemi gerçekleştirdikten sonra Dbug hata ayıklama aracını/betiğini çalıştırmak için başka bir eksiğimiz kalmıyor.

safe betiğini SciTE ile açtıktan sonra ilk olarak F5 (run/resume execution) tuşuna basarak Dbug aracının devreye girmesini sağlıyoruz. Fakat betiği çalıştırdığımızda, AutoIt kütüphanesindeki değişkenler ve fonksiyonlar ile betiktekiler çakıştığı için soruna yol açan bu değişkenleri ve fonksiyonları silmemiz gerekiyor.



To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Betiği sorunsuz bir şekilde çalıştırdıktan sonra gözümüze kestirdiğimiz bir satırın üzerine gelip F9 (run to cursor) tuşuna basarak program akışının o satıra kadar ilerlemesini sağlıyoruz. 3711. satıra geldiğimizde farenin imlecini (cursor) bir üst satırda yer alan \$lc70652o3373 değişkenin üzerine getirdiğimizde, o değişkenin hangi değere (http://149.202.206.57) sahip olduğunu görebiliyoruz. OllyDbg aracında olduğu gibi F7 tuşuna basarak ilgili fonksiyonun içine girebiliyor, F8 tuşuna basarak ise (step over) fonksiyonun içine girmeden akışın (flow) devam etmesini sağlayabiliyoruz. Özetle Dbug aracı sayesinde adım adım fonksiyonların ne işe yaradığını öğrenerek, fonksiyonların yanına yorum (comment) da yazarak kısa bir süre içinde zararlı yazılımın/betiğin ne iş yaptığını kolaylıkla öğrenebiliyoruz.

C:\Docun	nents and Settings\Administrator\Application Data\Apple_Updater\safe.au3 - SciTE		L 🔼
File Edit Se	arch View Tools Options Language Buffers Help		
3690	[ ∰ ] \$ № № X   ∞ ⊂ Q Q <sup>2</sup> Local Same = D10:11 ("Kernel?? d11" "bool" "Hell-twile" "Local # CL411. "due 1"	d(Cioffeet) "depend" minut bit	Sicffeet) Marcad Marcad
3681	Local varet - Dilcal("Kernel32.dll", "Dool", "Unlockrile", "handle", While, "dword", _whapi_lodword If Gerror Then Return SetError(Gerror, Gextended, 0)	a(sioriset), "dword", _winapi_nidword()	sioriset), "dword", _winspix
3682	Return Saret[0]	ADBUG ver. 2016.03.25 - Rt	unning safe. au3 📃 🗖 🔀
3684	blue uno	🛶 🖓 🕅 🖉 🚧	o 📑 🖏 🖈 🖬
3685	Func_winapi_unmapviewoffile(Spaddress)		***
3685	<pre>Local saret = Difcal("kernels.all", "bool", "OmmaplewOrrile", "ptr", spadaress) If Geror Then Return SetError(Geror(, Gextended, False)</pre>	1	
3688	Return Saret[0]	Break in Global (3711)	
3689 -	EndFunc	Watch Commands Info	Settings Help
3691	Func _winapi_wow64enablewow64fsredirection(\$benable)	~~~DBUG help~~~	
3692	<pre>Local Saret = DlCall("kernel2.dll", "boolean", "WoolfeEnableWow64FsRedirection", "boolean", Shenable Televise Then Beetware SetForce (devised d)</pre>	) 1. Hotkeys list:	
3694	Return Saret[0]	Ctrl+F2 - set/reset brea	kpoint line
3695 -	EndFunc	F5 - run/resume execution	n
3697 - #	EndRegion Public Functions	F6 - activate main DBUG	window
3698 = #	Region Internal Functions	F8 - step over	
3700	Pune winapi makeqword(Silodword, Sihidword)	F9 - run to cursor Ctrl+Enter - execute com	mand
3701	Local \$tint64 = DllStructCreate("uint64")	Ctrl+F10 - quit from DBU	G
3702	Local \$tdwords = DilstructGrate("dword; Moord", DilStructGetPtr(\$tinto4)) DilstructSetData(\$tdwords, 1, \$ilodword)	2. Tips:	
3704	DllStructSetData (Stdwords, 2, Sihidword)		
3705	Return D11StretGetData(\$tint64, 1) EndFung		
370			
3708 4	EndRegion Internal Functions		
3710 \$	Lordos2co3373 = dy68609b50361("0xA2470BDDDC254F2777F336934D6885BDBA04422207FC87A78033F85B6123D47", "12038392	604502155876") ; http://149.202.206.57	
3711 0	vf684 <u>17a23886 = dv68609b50361("0x0012BEPBAC170826FB37DP3CFBB1756", "12038392604502155876")</u> ; Winter giftess	: 6pRxSLyV4	
3712 \$	xqys6/S3014251=100/J145202.00.307/pU950361("UX3C4DBF/EF3953A3743D7E8266F0AB7ED", "1203837204302135876") & c 20452141773 = 0AppDataDir & dy6809950361("UX3C4DBF7EF395A3743D7E8266F0AB7ED", "1203832604502135876") & c	y68609b50361("0x559DF08EC6DF2A5A726B338 y68609b50361("0xD7F022EEBCAE748B1DCAF7E	B1F29BCF10", "1203839260450 B280801EF3", "1203839260450
3714 \$	jh25321c89783 = @AppDataDir & dy68609b50361("0x5C4DB77E7595A3743D7FB2E68F0AB7ED", "12038392604502155876") ;	C:\Documents and Settings\Administrato	r\Desktop\743672679\App_Upc
3715	dv24654k21486 = dy68609b50361("0x787CEBB0303A6b51C340A5DB14D9713", "12038392604502155876") ; #comments-stal 1x7864558153 = dv68609b50361("0x786585653297PB178921PF185DB80E84", "12038392604502155876") ; #lcomments-stal		
3717 \$	jz77591w36570 = <b>dy68609b50361("0x4105F2FE54787450BFFE9BE16D9A2BCD"</b> , <b>"12038392604502155876"</b> ) ; unbin.bin		
3718 9	t=25061z22023 = dy68609b50361("0x2BF926F090B8C2F8EB737042E098CD9A", "12038392604502155876") ; unbin2.bin b=70852943458 = Scala see 255 25128		
3720 \$	mg/032433100 - Volig_e05_200 / 2012 0)71712231123 = Random(10000, 9999999999, 1) < dy68609b50361("0x1CD97CDD945058012E6F84D112D8847E", "1203835	2604502155876")	
3721	f (FileGetSize(\$zp4521411773) > 1024 * 1024 * 2) AND th18284o71855() == 4 Then ; buraya girdi. Script orjina p(27402-201564)	l yerinden çalışmaz ise buraya girmiyo:	r
3723	lise		
3724	cc53833175674 ()		
2705			
3725 3726 - E	gi87402u79156() mdIf		
3725 3726 3727	gi87402u79156() mdIf		×
3725 3726 3727	gi87402u79156() mdIf		× >
3725 3726 3727 Press P6 f	gi87402u79156() mdIf 		× *
3725 3726 3727 Press P6 f MustDeclar http://149	gi87402u79156() mdIf 		, •
3725 3726 - E 3727 Press F6 f MustDeclar http://149	gi87402u79156() ndlf 		, • •
3725 3726 3727 Press F6 f MustDeclar http://149	gi87402u79156() indif or activate DBUG window. "# STOP DBUG" and "# START DBUG" - stop and resume debug below this line. eVars .202.206.57/		2 2 2 2
3725 3726 B 3727 C Press P6 f Mustbeclar http://149 C =3710 co=8 J	gi87402u79156() indif 		2 2 2 2
3725 3726 Bress P6 f Mustbeclar http://149 <	gi87402u79156() indIf or activate DBUG window. "# BTOP DBUG" and "# START DBUG" - stop and resume debug below this line. eVars .202.206.57/ NS (CR+LF) pion Internal Functions E largeosciption, bytestigatese, benefotovit202, fbj77172c9412), frye52141177, fev2465421866		2 2 2 2 2
3725 3726 B 3727 C Press P6 f MustDeclar http://149 C S S S S S S S S S S S S S	<pre>gie7402u79156() ndIf indIf or activate DBUG window. "# STOP DBUG" and "# START DBUG" - stop and resume debug below this line. eVars .202.206.57/ SS(CR4LF) Sgion Internal Functions Ilinokassing in the state in the st</pre>		• • •
3725 3726 B 3727 Yress P6 f Mustbeclar http://149 K 1000-81	<pre>gi87402u79156() ndIf ndIf cor activate DBUG window. "# STOP DBUG" and "# START DBUG" - stop and resume debug below this line. eVars .202.206.57/  VS (CR+LF)  pion Internal Functions E LipPoSC20075, ivt648172086, 5ex00050vi402, Sbj77172z4123, Szy4531411773, Stoc465421466 E LipPoSC20075, ivt648172086, 5ex00050vi402, Sbj77172z4123, Szy4531411773, Stoc465421466 E LipPoSC20075, ivt648172086, 5ex00050vi402, Sbj77172z4123, Szy4531411773, Stoc465421466 E LipPoSC20075, ivt648725000000000000000000000000000000000000</pre>	2960710*, *120203986044001155074*) _dri (becumenta and 001297-1, *12020398604501155074*) _dri (becumenta and	anetang kalangina sa sa tu banka op 1/2007 seetang kalangina sa sa tu banka op 1/2007 seetang kalangina sa sa tu banka op 1/2007
3725 3726 B 3727 S 3727 S Press P6 f Mustbeclar http://149	<pre>gi87402u79156() ndIf conditional for the formation of the formation o</pre>	1980710", "11038392604501155876") ///) Ubcuments and 9611870", "11038392604501155876") ///) Ubcuments and actor/147077771/ug_/0ydectubally_0ydets	Settings\Administrator\Deaktop\74367 Settings\Administrator\Deaktop\74367
37225 37226 37227 Fress P6 f Mustbeclar http://149	<pre>gid7402u79156() indIf ind</pre>	2960710", "1203932004501155876"), /C) (Documents and 8018873, "1203832004501155876"), /C) (Documents and actop() 7457/2774/Jug. Dydstar (Jug. Dydstar #) DBUG ver. 2014 03 26 - Numning safe au)	Settings \dministrator\beaktop\74367 Settings \dministrator\beaktop\74367
3725 3726 E 3727 ₹ Press F6 f MustDeclar http://149 € 3709 End/ 3709 End/ 370	<pre>gis7402u79156() ndIf or activate DBUG window. "# BTOP DBUG" and "# START DBUG" - stop and resume debug below this line. eVars eVars .202.206.57/  Signa Internal Functions Signa Internal</pre>	2960710*, *1202998604400155874*) /r? Lbouwents and 0021879, 12021998604400155874*) /r? Lbouwents and exclp1744/07279/App_Updates 4)0040 ver.2001.22 + Summing safe au3 40 (ver. 2001) / ver.	anetings \administrator \beaktop \7007 settings \administrator \beaktop \7007 settings \administrator \beaktop \7007
3725         B           3726         B           3727         C           3727         C           C         C           B         3710 coell           K         C           B         3710 coell           1000         G           111         Srde           112         Srde           113         Srde           114         Srde           115         Srde           116         Srde           11712         Srde           118         Srde           119         Srde           1100         Srde           111         Srde           1114         Srde	<pre>gis7402u79156() nndIf indIf cor activate DBUG window. "# STOP DBUG" and "# START DBUG" - stop and resume debug below this line. eVars .202.206.57/  WS (CR+LF)  mpion Internal Functions E 10705253373, style#1721986, beh0005014102, Sbj7717224123, Spy851141773, 5604655421486 E 10705253373, style#1721986, beh0005014102, Sbj7717224123, Spy851141777, 5604655421486 E 10705253373, style#1721986, beh0005014102, Sbj7717224123, Spy851141777, 5604655421486 E 10705253373, style#1721986, beh000501400000000000000000000000000000000</pre>	2965710*, *120339260450013587(*), /02 Liboruments and 801873*, *120389260450013587(*), /02 Liboruments and extrop/7472677 Upp Updater (Lippic_Ordeter ● DBUG vr. 2014 0.0 12 6 Hunning safe au) ● 文化 区、中 二 一 一 二 二 二 二 二 二 二 二 二	Sectings \dds.inistsetor \Deaktop\7367 Sectings \dds.inistsetor \Deaktop\7367 Sectings \dds.inistsetor \Deaktop\7367
3725 g 3726 g 3727 c 3727 c 3727 c 3727 c 3728 c 3728 c 4 c 4 c 4 c 4 c 4 c 4 c 4 c 4	<pre>gi87402u79156() nndIf nndIf or activate DBUG window. "# STOP DBUG" and "# START DBUG" - stop and resume debug below this line. eVars .202.206.57/  ws(CR+LF)  status kstatus kstatu</pre>	1980年1997、**1603399500659015587(**), //0) (Documents and 2005年7、**200399500501015587(**), //0) (Documents and 2005(**2017) //0) (Documents and 2005(**2017) //0) (Documents) 2005(***********************************	Secting Administrator Deaktop 174567 Secting Administrator Deaktop 174567
3725 g 3726 g 3727 c 3727 c 3727 c 3728 g 3728 g 3728 g 3728 g 3728 g 1729 g 1729 g 1729 g 1720	<pre>gi87402u79156() nndIf notIf control = 0000 window. "# STOP DBUG" and "# START DBUG" - stop and resume debug below this line. eVers cVers cV</pre>	2900710", "12038392004501155876") (C) (Documents and 001870", "1201893201450125976") (C) (Documents and actop(12527671400) (C) (Documents and actop(12527671400) (D) (D) (D) (D) (D) (D) (D) (D) (D) (D	Settings \Administrator\Deaktop\74367 Settings \Administrator\Deaktop\74367 Settings \Administrator\Deaktop\74367
3725         3726           3726         3727           3727         3727           C         3727           MustDelar         4	<pre>gis7402u79156() ndIf  or activate DBUG window. "# BTOP DBUG" and "# START DBUG" - stop and resume debug below this line. eVars eVars .202.206.57/  sign Internal Functions sign Internal Fu</pre>	2960710", "1203932004501155876") /0/ LDocuments and 801873", "1203932004501155876") /0/ LDocuments and extops/1426/2767/490, pychatest laggl_copdates 80000 ver. 2014.01 /2 - Hunning taife au) 9 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 0 0 0 0	Sectings \dministrator\beaktop\7d367 Sectings \dministrator\beaktop\7d367 Secting \dministrator\beaktop\7d367 Secting \dministrator\beaktop\7d367 Secting \dministrator\beaktop\7d367 Secting \dministrator\beaktop\7d367 Secting \dministrator\beaktop\7d367 Secting \dministrator\beaktop\7d367 Secting \dministrator\fracto
3725         B           3726         B           3727         B           3727         B           3727         B           3728         B           3727         B           3727         B           S         B           B         S           S         B           S </td <td><pre>gis7402u79156() indIf  cor activate DBUG window. "# STOP DBUG" and "# START DBUG" - stop and resume debug below this line. eVars .202.206.57/  wind If  cor activate DBUG window. "# STOP DBUG" and "# START DBUG" - stop and resume debug below this line. eVars .202.206.57/  wind If  cor activate DBUG window. "# STOP DBUG" and "# START DBUG" - stop and resume debug below this line. eVars .202.206.57/  wind If  cor activate DBUG window. "# STOP DBUG" and "# START DBUG" - stop and resume debug below this line202.206.57/ window in the interval inte</pre></td> <td>296C710*, *1203392604500135874*) /0/10otuments and 801897*, *1203892604500135874*) /0/10otuments and extop/7472677 Upp (printer/Lpp1Opidets #0000 0vr.2016 0/10 * Unning sife au) ************************************</td> <td>Sectings \dds/nistsetor \Deaktop\7487 Sectings \dds/nistsetor \Deaktop</td>	<pre>gis7402u79156() indIf  cor activate DBUG window. "# STOP DBUG" and "# START DBUG" - stop and resume debug below this line. eVars .202.206.57/  wind If  cor activate DBUG window. "# STOP DBUG" and "# START DBUG" - stop and resume debug below this line. eVars .202.206.57/  wind If  cor activate DBUG window. "# STOP DBUG" and "# START DBUG" - stop and resume debug below this line. eVars .202.206.57/  wind If  cor activate DBUG window. "# STOP DBUG" and "# START DBUG" - stop and resume debug below this line202.206.57/ window in the interval inte</pre>	296C710*, *1203392604500135874*) /0/10otuments and 801897*, *1203892604500135874*) /0/10otuments and extop/7472677 Upp (printer/Lpp1Opidets #0000 0vr.2016 0/10 * Unning sife au) ************************************	Sectings \dds/nistsetor \Deaktop\7487 Sectings \dds/nistsetor \Deaktop
3725 g 3726 g 3727 c 3727 c 3727 c 3727 c 3728 c 4 c 4 c 4 c 4 c 4 c 4 c 4 c 4	<pre>gis7402u79156() ndIf core activate DBUG window. "# STOP DBUG" and "# START DBUG" - stop and resume debug below this line. eVars eVars core activate DBUG window. "# STOP DBUG" and "# START DBUG" - stop and resume debug below this line. eVars core activate DBUG window. "# STOP DBUG" and "# START DBUG" - stop and resume debug below this line. eVars core activate DBUG window. "# STOP DBUG" and "# START DBUG" - stop and resume debug below this line. eVars core activate DBUG window. "# STOP DBUG" and "# START DBUG" - stop and resume debug below this line. eVars core activate DBUG window. "# STOP DBUG" and "# START DBUG" - stop and resume debug below this line. eVars core activate DBUG window. "# STOP DBUG" and "# START DBUG" - stop and resume debug below this line. eVars core activate DBUG window. "# STOP DBUG" and "# START DBUG" - stop and resume debug below this line. eVars core activate DBUG window. "# STOP DBUG" and "# START DBUG" - stop and resume debug below this line. eVars core activate DBUG window. "# Stop DBUG" and "# START DBUG" - stop and resume debug below this line. eVars core activate DBUG window. "# Stop DBUG" and "# Stop DBUG" - stop and resume debug below this line. eVars core activate DBUG window. "# Stop DBUG" - stop activate DBUG" - stop - stop</pre>	SBCCTLD*, *1202039600450215507(*), JC: Lbouments and           SB2207, '1202039600450215507(*), JC: Lbouments and           SB2207, '1202039600450215507(*), JC: Lbouments and           SB206, V2: 2014-01.25 * Lunning tafe au)	Sectings Links (strator linektor 1787) Sectings Links (strator linektor 1787) Sectings Links (strator linektor 1787) Sectings (strator
3725 g 3726 g 3727 c 3727 c 3727 c 3727 c 4	<pre>git7402u79156() nndII notIf not</pre>	1980710*         *12038392604501155876*)         yC) Lbocuments and 001870*         yC) Lbocuments and accord v50272404101155876*)         yC) Lbocuments and accord v50272404101155876*)         yC) Lbocuments and accord v502724042           00100 var. 2014 0.0 20 × Numning safe au3         yC         yC         yC           00100 var. 2014 0.0 20 × Numning safe au3         yC         yC         yC           00100 var. 2014 0.0 20 × Numning safe au3         yC         yC         yC           00100 var. 2014 0.0 20 × Numning safe au3         yC         yC         yC           00100 var. 2014 0.0 20 × Numning safe au3         yC         yC         yC           00100 var. 2014 0.0 20 × Numning safe au3         yC         yC         yC           00100 var. 2014 0.0 20 × Numning safe au3         yC         yC         yC           00100 var. 2014 0.0 20 × Numning safe au3         yC         yC         yC           00100 var. 2014 0.0 20 × Numning safe au3         yC         yC         yC           00100 var. 2014 0.0 20 × Numning safe au3         yC         yC         yC           00100 var. 2014 0.0 20 × Numning safe au3         yC         yC         yC           0010 var. 2014 0.0 20 × Numning safe au3         yC         yC         yC           0010 var. 2014 0.0 20 × Numing safe au3 <td< td=""><td>Sectings\Administrator\Deaktop\74367 Sectings\Administrator\Pacific\74367 Sectings\Administrator\Pacific\74367 Sectings\Administrator\Pacific\74367 Sectings\Administrator\Pacific\74367 Sectings\Administrator\Pacific\74367 Sectings\Administrator\Pacific\74367 Sectings\A</td></td<>	Sectings\Administrator\Deaktop\74367 Sectings\Administrator\Pacific\74367 Sectings\Administrator\Pacific\74367 Sectings\Administrator\Pacific\74367 Sectings\Administrator\Pacific\74367 Sectings\Administrator\Pacific\74367 Sectings\Administrator\Pacific\74367 Sectings\A
3725         ₽           3726         ₽           3727         ₹           3727         ₹           1728         ₽           1729         ₽           1720         ₽           1721         ₽           1721         ₽           1721         ₽           1720         ₽           1720         ₽           1720         ₽           1720         ₽           1720         ₽           1720         ₽           1720         ₽           1721         ₽           1725         ₽           1726         ₽           1727         ₽           1720         ₽           1721         ₽           1720         ₽           1720         ₽           1722         ₽           1722         ₽           1722         ₽           1722         ₽           1722         ₽           1722         ₽           1723         ₽           1724         ₽           1725           <	<pre>gis7402u79156() indIf if if</pre>	290c710", "1203032604502155876") /C) \Documents and 3001870", "1203032604502155976") /C) \Documents and actorp(1450/2761/40g, Dydstets(14)g,	Sectings Lådministrator Desktop \74367 Sectings Lådministrator Desktop \74367 Sectings Lådministrator Desktop \74367 Sectings Desktop \74367 Sectings Desktop \74367 Secting 0 Period Desktop
3725 g 3726 g 3727 g 3727 g 3727 g 3727 g 4 4 4 4 5 5 5 5 5 5 5 5 5 5 5 5 5	<pre>gis7402u79156() indIf if if</pre>	2900710", "1203392004500135874") /0'LDocuments and 801897", "1203892004500135874") /0'LDocuments and extop/741072677 Mpg Cyndrter Upple_Opdres #00000 vr.2016 01 26 * Unning safe au] ************************************	Acceloge Laborhistore Deaktop/7487 Sectinge Laborhistore Deaktop/7487 Sectinge Laborhistore Deaktop/7487 Sectinge Deaktop/7487 Secti
3725 g 3726 g 3727 g 3727 g 3727 g 3728 g 4 g 4 g 4 g 4 g 4 g 4 g 4 g 4	<pre>gie7402u79156() ndII or activate DBUG window. "# STOP DBUG" and "# START DBUG" - stop and resume debug below this line. eVars eVars t.202.206.57/  WS (CR+LF)  mpion Internal Functions i licrosoftavitate (%) Statistic (%) Statisti</pre>	2960710 <sup>-11</sup> , "1100299960440015507(*) ,dr. Uboutments and 200297-1, '120299960450015597(*) ,dr. Uboutments and extroj1/4/672679 /kgp (tydeter lappig, (tydeter 200600 vr. 2016 0.0 20 - kunning safe au) 20060 vr. 2016 0.0 20 - kunning safe au) 20070 vr. 2016 0.0 20 - kunning safe au 20070 vr. 2016 0.0 20 - kunn	Bettings \ Labs/nistratus \ Deaktop \ 7,887           Settings \ Labs/nistratus \ Deaktop \ 7,887           Bettings \ Labs/nistratus \ Deaktop \ 7,887           Settings \ Deaktop \ 7,887
3725 g 3726 g 3727 c 3727 c 3727 c 3727 c 4 4 4 4 4 4 4 4 4 4 4 4 4	<pre>gi87402u79156() nndII  or activate DBUG window. "# STOP DBUG" and "# START DBUG" - stop and resume debug below this line. eVars i.202.206.57/  ws(CR+LF)  pion Internal Functions iline(Statistic) - statistic)  pion Internal Function  p</pre>	1980710*         *1203839200450135876*)         yd) Ubocumenta end           001887*         *100389200450135876*)         yd) Ubocumenta end           00180*         *1004920000000000000000000000000000000000	Sectings\Administrator\Deaktop\74367 Sectings\Administrator\Period\74367 Sectings\Administrator\Period\74367 Sectings\Administrator\Period\74367 Sectings\Administrator\Period\74367 Sectings\Administrator\Period\74367 Sectings\Administrator\Period\74367 Sectings\Administrator\74367 Sectings\Administrator\P
372.5	<pre>git1402u79156() ndII indII or activate DBUG window. "# BTOP DBUG" and "# START DBUG" - stop and resume debug below this line. eVars eVars .202.206.57/  StoCCA-LF)  StoCCA-LF) StoCC</pre>	2500710", "1008032004501155976") /C) /Documents and 001870", "1008032004501155976") /C) /Documents and action(142076774/000000000000000000000000000000000	Sectings Ldministrator Deaktop 174367 Sectings Ldministrator Deaktop 174367 Sectings Ldministrator Deaktop 174367 Secting 0 4 Ministrator Deaktop 174367 Secting 0 4 Ministrat
3725 g 3726 g 3727 g 3727 g 3727 g 3727 g 4 4 4 4 5 5 5 5 5 5 5 5 5 5 5 5 5	<pre>git1402u79156() ndII or activate DBUG window. "# STOP DBUG" and "# START DBUG" - stop and resume debug below this line. eVars202.206.57/  WS (CR+LF)  mpion Internal Functions i i ichologicality, intercent interce</pre>	T1033326045011537741) /01 Uboruments and     the second seco	Actings Ldministere basktop/7467 Settings Ldministere basktop/7467 Settings Ldministere basktop/7467 Settings Ldministere basktop/7467 Settings Ldministere basktop/7467 Settings basktop/2467 Settings basktop/2467 Settings District Settings District Settings basktop/2467 Settings District Settings Distri
3725 g 3726 g 3727 g 3727 g 3727 g 3727 g 3728 g 3728 g 3728 g 3728 g 3729 g 3729 g 3720 g 3720 g 3720 g 3720 g 3721	<pre>gi87402u79156() ndII control to the set of the set</pre>	290710", "1202099604400155074") J7: Ubouments and 200710", "1202099604500155074") J7: Ubouments and extop174/072679 Upp Updeter Uppla_Opdeter 200800 vr: 2014.01.25 = Nummers 146 au1 400800 vr: 2014	Acciency Labornistrature lawaktor 17887 Sectings Labornistrature lawaktor 17887 Sectings Labornistrature lawaktor 17887 Sectings Labornistrature lawaktor 17887 Sectings 1 Administrature lawaktor 17887 Secting 1
3725 g 3726 g 3727 g 3727 g 3727 g 3727 g 4 g 4 g 4 g 4 g 4 g 4 g 4 g 4	<pre>gi87402u79156() ndII or activate DBUG window. "# STOP DBUG" and "# START DBUG" - stop and resume debug below this line. eVars cvars c</pre>	1900710", "120337200450135976") (C) (Documents and 00187"), "12029720010135976") (C) (Documents and accord) 74507274010135976") (C) (Documents and accord) 74507274010125976") (C) (Documents and accord) 7450727401215976") 20000 vor.2014.01 20 5 Numoing Safe au) 20000 vor.2014.01 2	Acetings Ladministrator Deaktop (74)67 Settings Ladministrator Deaktop (74)67 Settings Ladministrator Deaktop (74)67 Settings Construction (14) Settings Construction (14) Settings Construction (14) Settings Construction (14) Setting Construction (14) S
372.5	<pre>gis7402u79156() ndII indII or activate DBUG window. "# BTOP DBUG" and "# START DBUG" - stop and resume debug below this line. eVars eVars .202.206.57/  StoCCA-LF)  StoCCA-LF) S</pre>	SSCTIO", "100807200450115597(") (C) LDocuments and 001870", "100807200450115597(") (C) LDocuments and accord V5072707400, g) Opticat Langle Dydelse 200800 vm: 2016 CD 10 = Nurning safe au) 200800 vm: 2016 CD 10 = Nurning safe au) 2008000 vm: 2016 CD 10 = Nurning safe au) 2008000 vm: 2016 CD 10 = Nurning safe au) 20080000000000000000000000000000000000	Settings \Administrator\Deaktop\74567 Settings \Administrator\Deaktop\74567 Settings \Administrator\Deaktop\74567 Settings \Administrator\Deaktop\74567 Settings \Deaktop\74567 Settings \Deaktop\7457
3725 8 3726 8 3727 8 3727 8 3727 8 3727 8 3727 8 4 4 4 4 4 4 4 4 4 4 4 4 4	<pre>gis7402u79156() ndII indII core activate DEUG window. "# STOP DEUG" and "# START DEUG" - stop and resume debug below this line. eVars .202.206.57/  NS(CR+LF)  mpion Internal Functions i stopportune internal Functions i s</pre>	PROFILO", "110030392004500135074"), /O'L Mocuments and Ref Control (Control (Contr	Acctings Lidministrator Deaktop/7407 Sectings Lidministrator Deaktop/7407 Sectings Lidministrator Deaktop/7407 Sectings Lidministrator Deaktop/7407 Sectings Deaktop/7407 Sectin
3725 8 3726 8 3727 8 3727 8 3727 8 4 4 4 4 4 4 4 4 4 4 4 4 4	<pre>glaP102u791256() ndII constructed DBUG window. "# STOP DBUG" and "# START DBUG" - stop and resume debug below this line. eVars .202.206.57/  KC(R+LF)  pion Internal Functions is introductions is introduction is intro</pre>	296270', "1202039566440015507(*) jd: boouments and 296270', "1202039566440015507(*) jd: boouments and extop/14/672677/bpg bydeter/laple_Opdeter 206800 vr.2016.01.25 * Kunning 146 au) 90 0 0 0 0 vr.2016.01.25 * Kunning 146 au) 140 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Beetings \ Labs/mistratus \ Deaktop\ 7,007           Beetings \ Labs/mistratus \ Deaktop\ 7,007           Bettings \ Deaktop\ 7,007           Bettings \ Disk           Comments-meters 'sam allyor. (command           Bettings Disk           Bettings Disk <t< td=""></t<>

Bu yazının son yıllarda AutoIt ile geliştirilen zararlı betikleri analiz etmede faydalı olması dileğiyle bir sonraki yazıda görüşmek üzere herkese güvenli günler dilerim.