Su Kaynağı Saldırısı

written by Mert SARICA | 2 January 2015

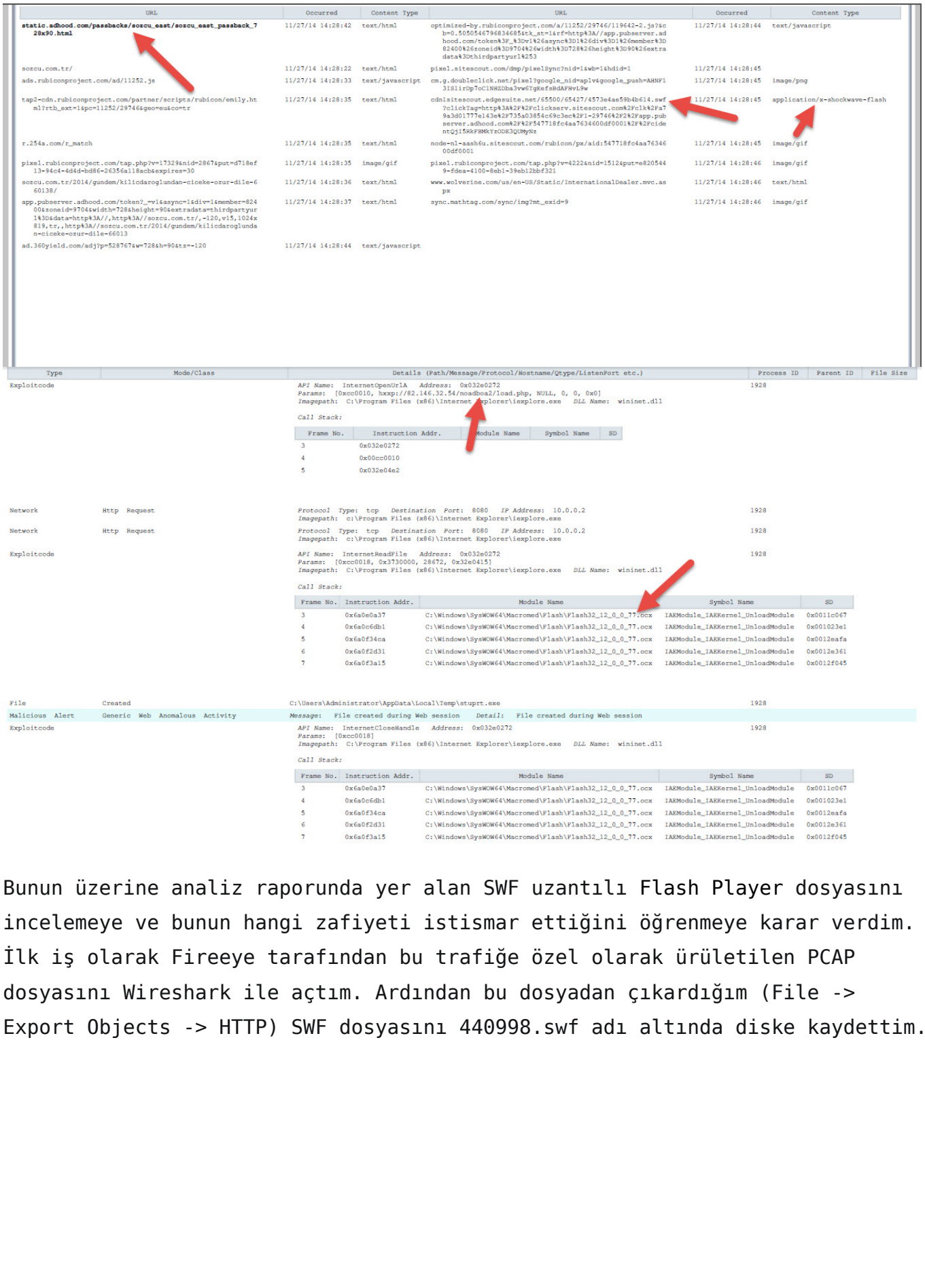
Watering Hole, Türkçe meali ile su kaynağı saldırısına kurak Afrika'da sıklıkla rastlanmaktadır. Susuzluğunu gidermek için su kaynağına giden hayvanların bir kısmı, bu su kaynağına ev sahipliği yapan timsahlar tarafından karşılanmaktadırlar. Pek misafirperver olan bu timsahların karınlarını doyurmak için tembel tembel suyun altında beklemek dışında başka bir şey yapmalarına gerek yoktur çünkü er ya da geç, susuzluğa yenik düşen hayvanlar, tıpış tıpış su kaynağına gidecek ve suyun altında gizlenen uyuşuk ama akıllı timsahların saldırıları sonucunda öğle yemeği olmaktan kurtulamayacaklardır.

İnternette gerçekleşen su kaynağı saldırılarının da Afrika'da gerçekleşenlerden pek bir farkı yoktur. Susayan hayvanların er ya da geç su kaynağına gitmesi gibi canı sıkılan, gündemi takip etmek isteyen çok sayıda kullanıcının da gün içinde haber, alışveriş, eğlence, magazin sitelerini ziyaret ettiğini bilen art niyetli kişiler, bu siteleri veya bu sitelerin içerik aldığı diğer siteleri/sistemleri (misal reklam siteleri, cdn vs.) hackleyerek, uyuşuk ama akıllı timsahlar gibi kurbanlarının, ayaklarına gelmelerini beklemektedirler. Hackledikleri sitelere zararlı kodlar yükleyen art niyetli kişiler, bu siteleri ziyaret eden kullanıcıların internet tarayıcılarında ve/veya eklentilerinde bulunan olası zafiyetleri (yaması geçilmemiş internet tarayıcısı, flash player, java vb.) istismar ederek bu kullanıcılarının sistemlerine zararlı yazılım yüklemektedirler.

Reklam olarak nitelendirilebilecek yazılar yazmamaya özen gösteren biri olarak, yazının devamında Fireeye NX cihazından bahsetmemin sebebinin, cihazın teknik olarak bu yazıya olan olumlu katkısı olduğunu belirtmek isterim.

Elinin altında Fireeye NX gibi kum havuzu analizinden faydalanarak ağ üzerinden zararlı yazılım tespiti yapabilen cihazı olanlar, 27 Kasım tarihinde Sözcü Gazetesi kaynaklı bir alarmla karşılaşmışlardır. Fireeye NX cihazı tarafından üretilen PCAP trafik dosyası ve analiz raporu incelendiğinde, Sözcü Gazetesi'nin web sitesinde yer alan reklam içeriğinin çekildiği bir sitenin (static.adhood.com/passbacks/sozcu_east/sozcu_east_passback_728x90.html) hacklendiği anlaşılabiliyordu. Analiz raporunda yer alan

Macromed\Flash\Flash32_12_0_0_77.ocx bilgisi sayesinde, istismar kodunun Flash Player yazılımı ile ilgili olduğu ve zafiyet barındıran Flash Player yazılımı istismar edildiğinde de, kullanıcıyı http://82.146.32.54/noadboa2/load.php adresine yönlendirildiği anlaşılıyordu.



URL	Occurred	Content Type	URL	Occurred	Content Type
static.adhood.com/passbacks/sozcu_east/sozcu_east_passback_728x90.html	11/27/14 14:28:42	text/html	optimized-by.rubiconproject.com/a/11252/29746/119642-2.js?cb=0.5050546796834685&tk_st=1&rf=http%3A//app.pubserver.adhood.com/token%3F_%3Dv1%26async%3D1%26div%3D1%26member%3D82400%26zoneid%3D9704%26width%3D728%26height%3D90%26extradata%3Dthirdpartyur1%253	11/27/14 14:28:44	text/javascript
sozcu.com.tr/	11/27/14 14:28:22	text/html	pixel.sitescout.com/dmp/pixel?sync?nid=1&wb=1&hdid=1	11/27/14 14:28:45	
ads.rubiconproject.com/ad/11252.js	11/27/14 14:28:33	text/javascript	cm.g.doubleclick.net/pixel?google_nid=aplv&google_push=AHNF131SlirDp7oC1NHZDba3vw6TgKefsBdAFHvL9w	11/27/14 14:28:45	image/png
tap2-cdn.rubiconproject.com/partner/scripts/rubicon/emily.html?rtb_ext=1&pc=11252/29746&geo=eu&co=tr	11/27/14 14:28:35	text/html	cdnlsitescout.edgesuite.net/65500/65427/4573e4ae59b4b614.swf?clickTag=http%3A%2F%2Fclickserv.sitescout.com%2Fclk%2Fa79a3d01777e143e%2F735a03854c69c3ec%2F1-29746%2F2%2Fapp.pubserver.adhood.com%2F%2F54771fc4aa7634600df0001%2F%2Fcidentqj15kkFBMkYzODE3QUMyNz	11/27/14 14:28:45	application/x-shockwave-flash
r.254a.com/r_match	11/27/14 14:28:35	text/html	node-nl-aash6u.sitescout.com/rubicon/px/aid:547718fc4aa7634600df0001	11/27/14 14:28:45	image/gif
pixel.rubiconproject.com/tap.php?v=17329&nid=2867&put=d718ef13-94c4-4d4d-bd86-26356a118acb&expires=30	11/27/14 14:28:35	image/gif	pixel.rubiconproject.com/tap.php?v=4222&nid=1512&put=e8205449-fdea-4100-8eb1-39eb12bbf321	11/27/14 14:28:46	image/gif
sozcu.com.tr/2014/gundem/kilicdaroglundan-ciceke-ozur-dile-660138/	11/27/14 14:28:36	text/html	www.wolverine.com/us/en-US/Static/InternationalDealer.mvc.aspx	11/27/14 14:28:46	text/html
app.pubserver.adhood.com/token?_=v1&async=1&div=1&member=82400&zoneid=9704&width=728&height=90&extradata=thirdpartyur1%3D&data=http%3A//,http%3A//sozcu.com.tr/,-120,v15,1024x819,tr,,http%3A//sozcu.com.tr/2014/gundem/kilicdaroglundan-ciceke-ozur-dile-66013	11/27/14 14:28:37	text/html	sync.mathtag.com/sync/img?mt_exid=9	11/27/14 14:28:46	image/gif
ad.360yield.com/adj?p=528767&w=728&h=90&tz=-120	11/27/14 14:28:44	text/javascript			

Type	Mode/Class	Details (Path/Message/Protocol/Hostname/Qtype/ListenPort etc.)	Process ID	Parent ID	File Size
Exploitcode		*API Name:* InternetOpenUrlA *Address:* 0x032e0272 *Params:* [0xcc0010, hxxp://82.146.32.54/noadboa2/load.php, NULL, 0, 0, 0x0] *Imagepath:* C:\Program Files (x86)\Internet Explorer\iexplore.exe *DLL Name:* wininet.dll *Call Stack:*	1928		

Frame No.	Instruction Addr.	Module Name	Symbol Name	SD
3	0x032e0272			
4	0x00cc0010			
5	0x032e04e2			

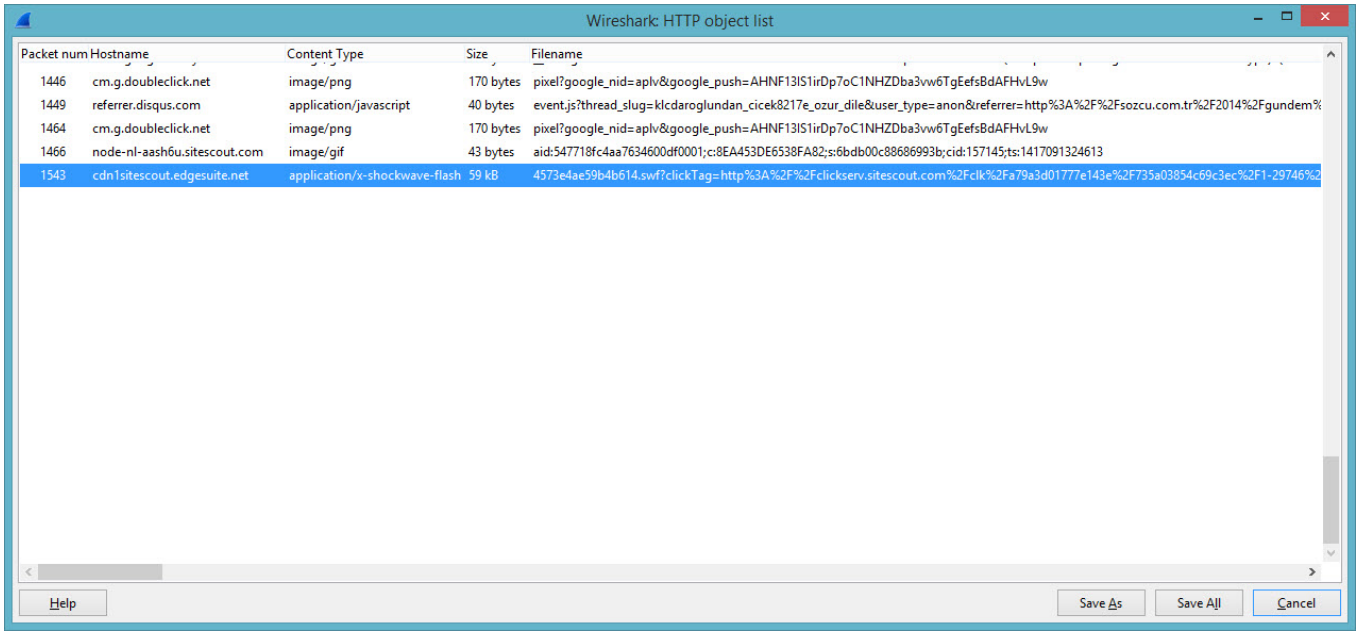
Network	Http Request	*Protocol Type:* tcp *Destination Port:* 8080 *IP Address:* 10.0.0.2 *Imagepath:* c:\Program Files (x86)\Internet Explorer\iexplore.exe	1928		
Network	Http Request	*Protocol Type:* tcp *Destination Port:* 8080 *IP Address:* 10.0.0.2 *Imagepath:* c:\Program Files (x86)\Internet Explorer\iexplore.exe	1928		
Exploitcode		*API Name:* InternetReadFile *Address:* 0x032e0272 *Params:* [0xcc0018, 0x3730000, 28672, 0x32e0415] *Imagepath:* C:\Program Files (x86)\Internet Explorer\iexplore.exe *DLL Name:* wininet.dll *Call Stack:*	1928		

Frame No.	Instruction Addr.	Module Name	Symbol Name	SD
3	0x6a0e0a37	C:\Windows\SysWOW64\Macromed\Flash\Flash32_12_0_0_77.ocx	IAEModule_IAEKernel_UnloadModule	0x0011c067
4	0x6a0c6db1	C:\Windows\SysWOW64\Macromed\Flash\Flash32_12_0_0_77.ocx	IAEModule_IAEKernel_UnloadModule	0x001023e1
5	0x6a0f34ca	C:\Windows\SysWOW64\Macromed\Flash\Flash32_12_0_0_77.ocx	IAEModule_IAEKernel_UnloadModule	0x0012eafa
6	0x6a0f2d31	C:\Windows\SysWOW64\Macromed\Flash\Flash32_12_0_0_77.ocx	IAEModule_IAEKernel_UnloadModule	0x0012e361
7	0x6a0f3a15	C:\Windows\SysWOW64\Macromed\Flash\Flash32_12_0_0_77.ocx	IAEModule_IAEKernel_UnloadModule	0x0012f045

File	Created	C:\Users\Administrator\AppData\Local\Temp\stuprt.exe	1928		
Malicious Alert	Generic Web Anomalous Activity	*Message:* File created during Web session *Detail:* File created during Web session			
Exploitcode		*API Name:* InternetCloseHandle *Address:* 0x032e0272 *Params:* [0xcc0018] *Imagepath:* C:\Program Files (x86)\Internet Explorer\iexplore.exe *DLL Name:* wininet.dll *Call Stack:*	1928		

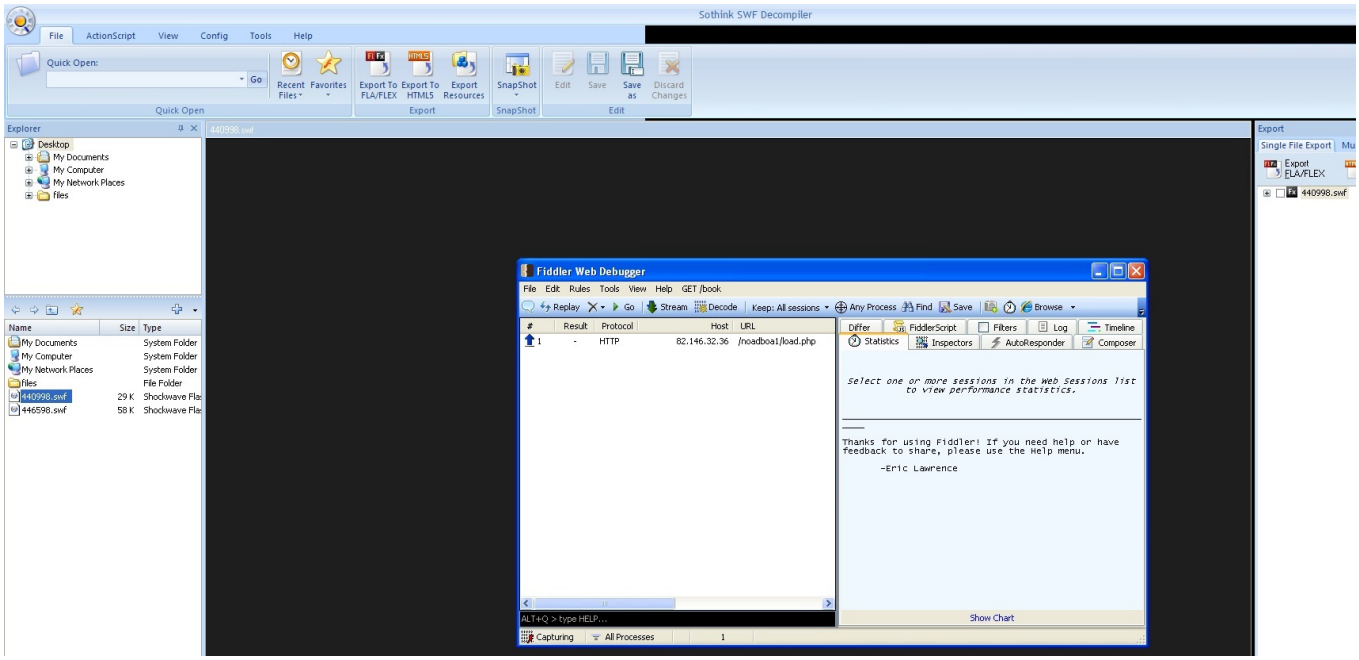
Frame No.	Instruction Addr.	Module Name	Symbol Name	SD
3	0x6a0e0a37	C:\Windows\SysWOW64\Macromed\Flash\Flash32_12_0_0_77.ocx	IAEModule_IAEKernel_UnloadModule	0x0011c067
4	0x6a0c6db1	C:\Windows\SysWOW64\Macromed\Flash\Flash32_12_0_0_77.ocx	IAEModule_IAEKernel_UnloadModule	0x001023e1
5	0x6a0f34ca	C:\Windows\SysWOW64\Macromed\Flash\Flash32_12_0_0_77.ocx	IAEModule_IAEKernel_UnloadModule	0x0012eafa
6	0x6a0f2d31	C:\Windows\SysWOW64\Macromed\Flash\Flash32_12_0_0_77.ocx	IAEModule_IAEKernel_UnloadModule	0x0012e361
7	0x6a0f3a15	C:\Windows\SysWOW64\Macromed\Flash\Flash32_12_0_0_77.ocx	IAEModule_IAEKernel_UnloadModule	0x0012f045

Bunun üzerine analiz raporunda yer alan SWF uzantılı Flash Player dosyasını incelemeye ve bunun hangi zafiyeti istismar ettiğini öğrenmeye karar verdim. İlk iş olarak Fireeye tarafından bu trafiğe özel olarak ürületilen PCAP dosyasını Wireshark ile açtım. Ardından bu dosyadan çıkardığım (File -> Export Objects -> HTTP) SWF dosyasını 440998.swf adı altında diske kaydettim.

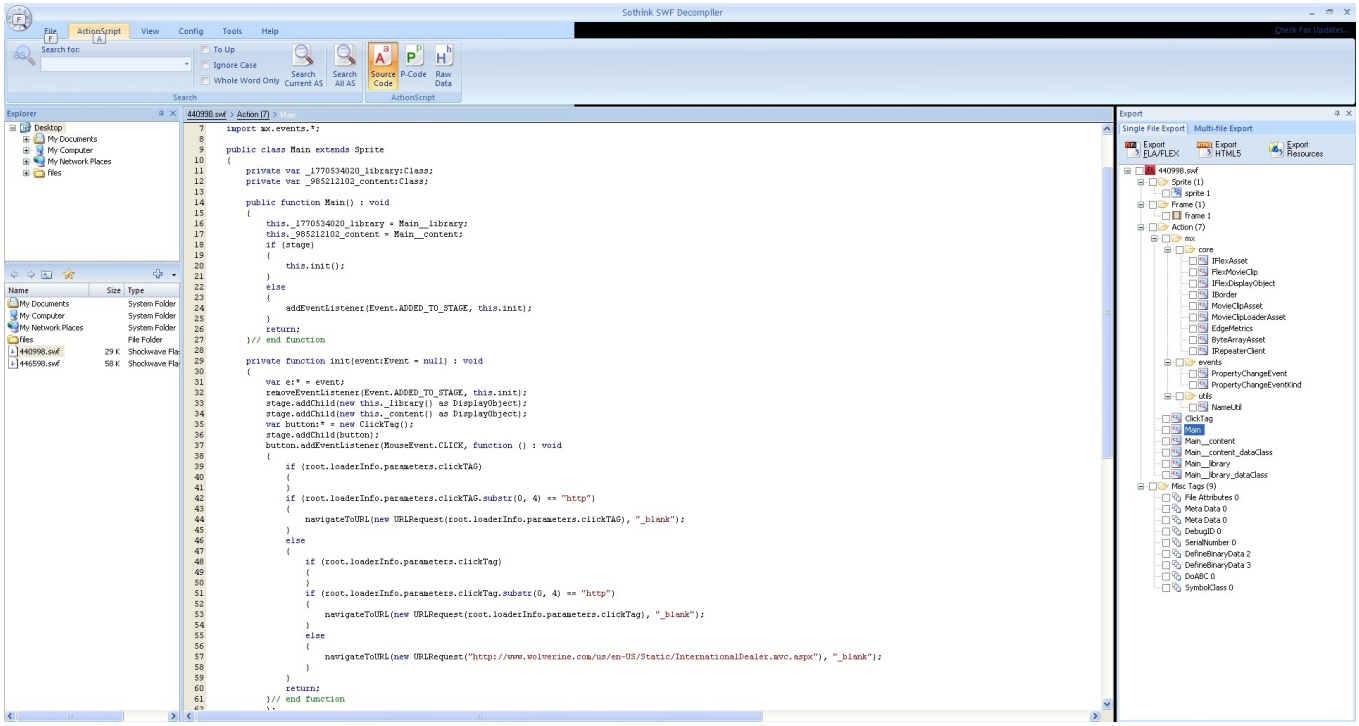


İşi gereği güvenlik testleri veya zararlı yazılım analizi ile ilgilenenler veya hobi olarak merak duyanlar, SWF dosyasının Flash Player sanal makinesi tarafından, çalışma esnasında derlenen bir baytkoddan (interpreted) oluştuğunu, bu nedenle SWF dosyasının Sothink SWF Decompiler, Flash Decompiler Trillix gibi ücretli ve JPEXS Flash Decompiler gibi ücretsiz araçlar ile kaynak koduna çevrilebildiğini biliyorlardır.

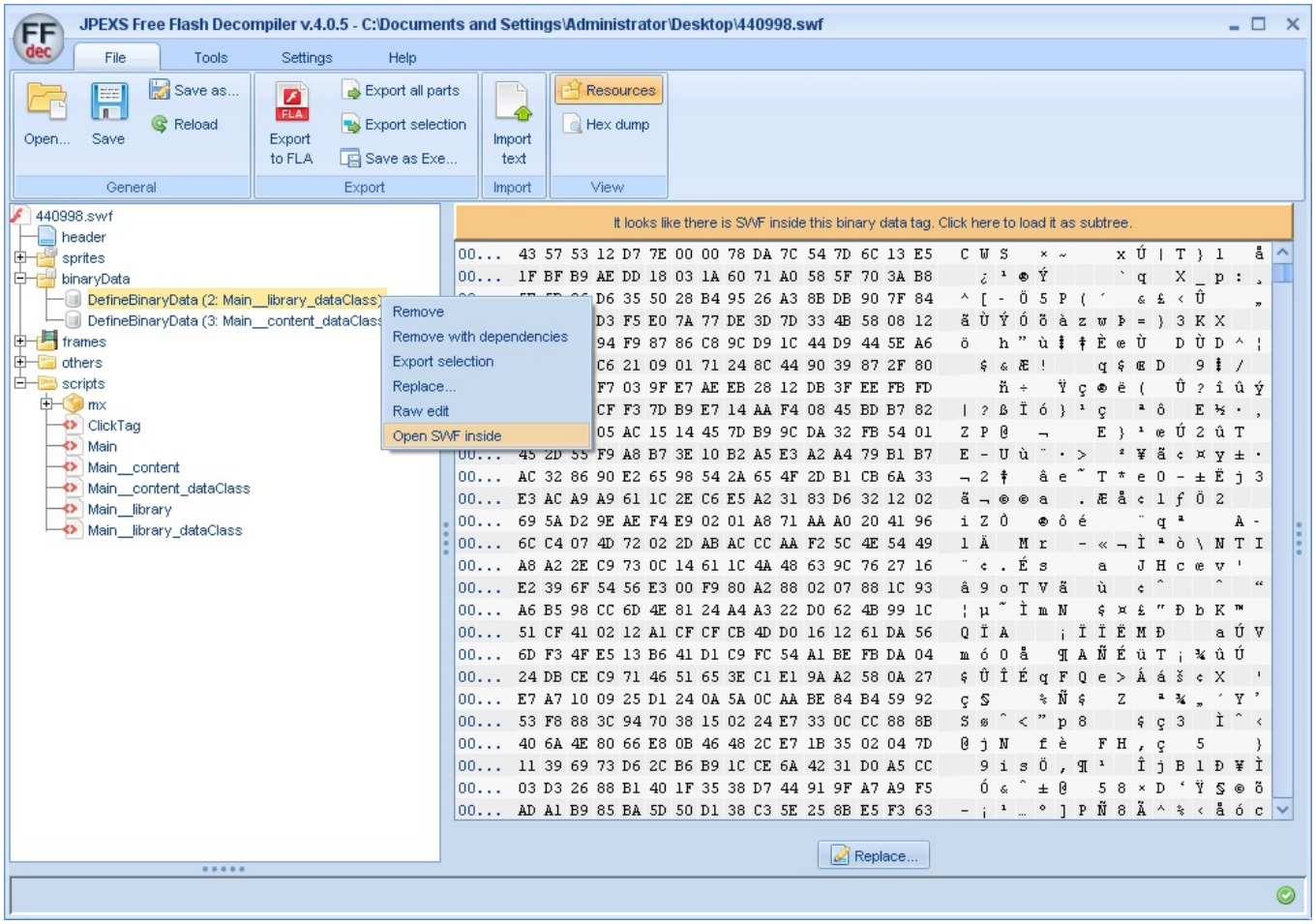
Her ne kadar kaynak koduna çevirme işlemi, statik kod analizi için yapılıyor olsa da, Sothink SWF Decompiler gibi araçlar, bayt kodunu kaynak koduna çevirdikten hemen sonra bu SWF dosyalarını da çalıştırdıkları için sanal makinede yapılmayan bu kaynak koduna çevirme işlemi, sisteminizde istismar kodunun çalışmasına sebep olabilir bu nedenle çok ama çok dikkatli olmanız gerekmektedir!



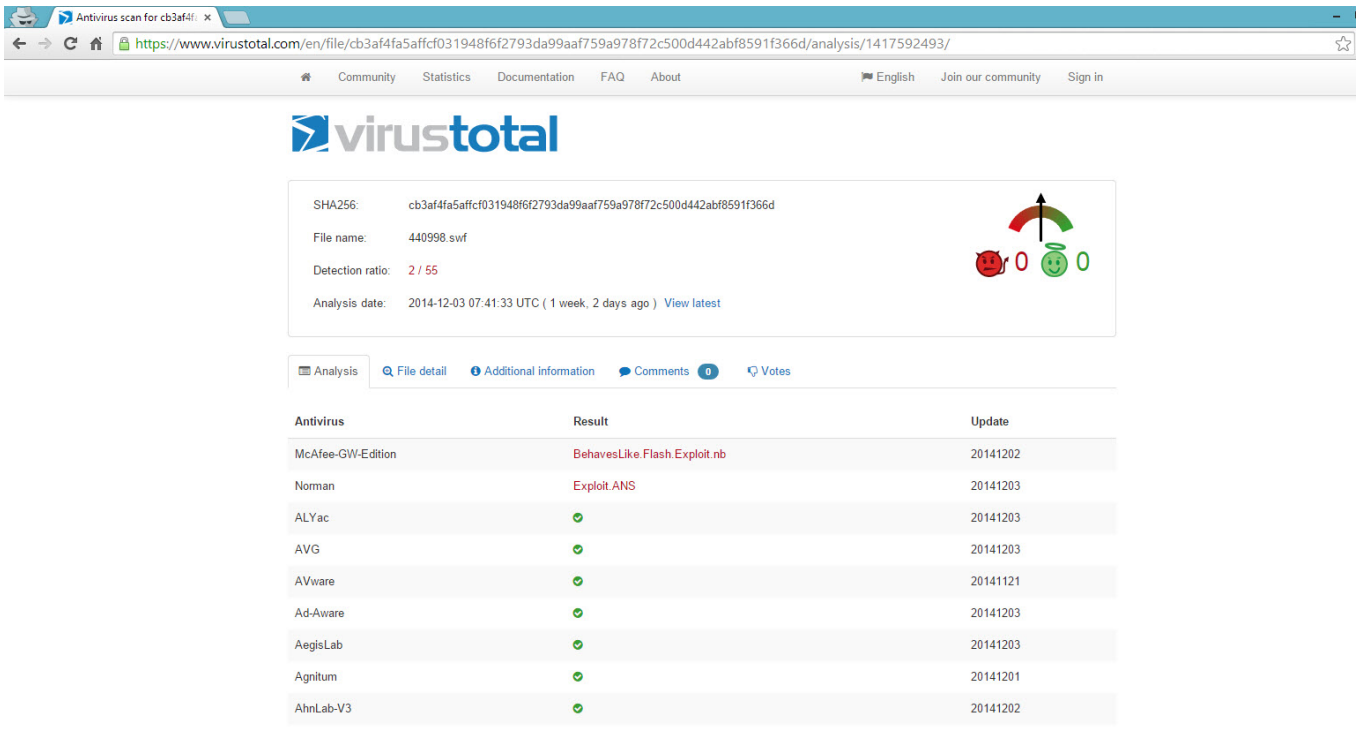
Flash Decompiler Trillix ile kaynak koduna çevirme işlemi başarısızlıkla sonuçlandıktan sonra Sothink SWF Decompiler aracı ile SWF dosyasını kaynak koduna çevirip, kodu incelediğimde herhangi bir zararlı koda rastlayamadım.

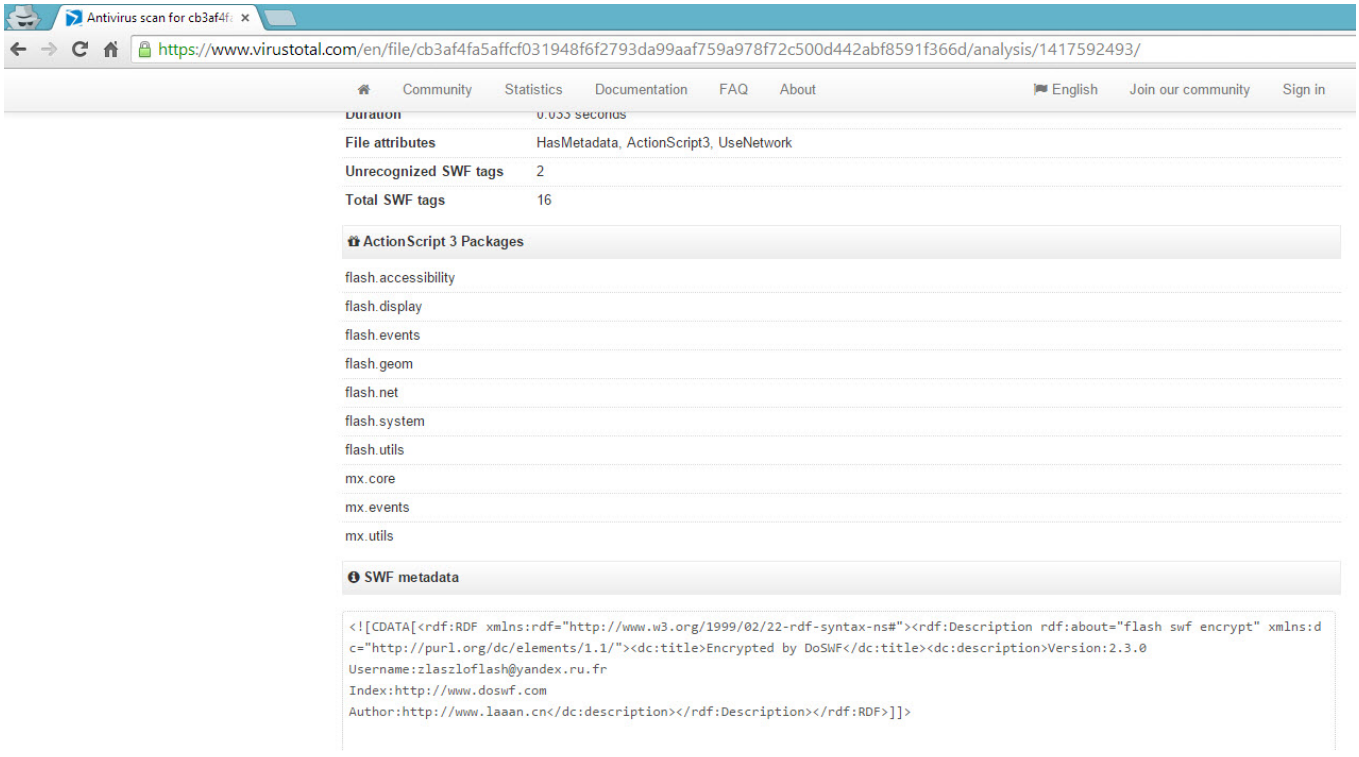


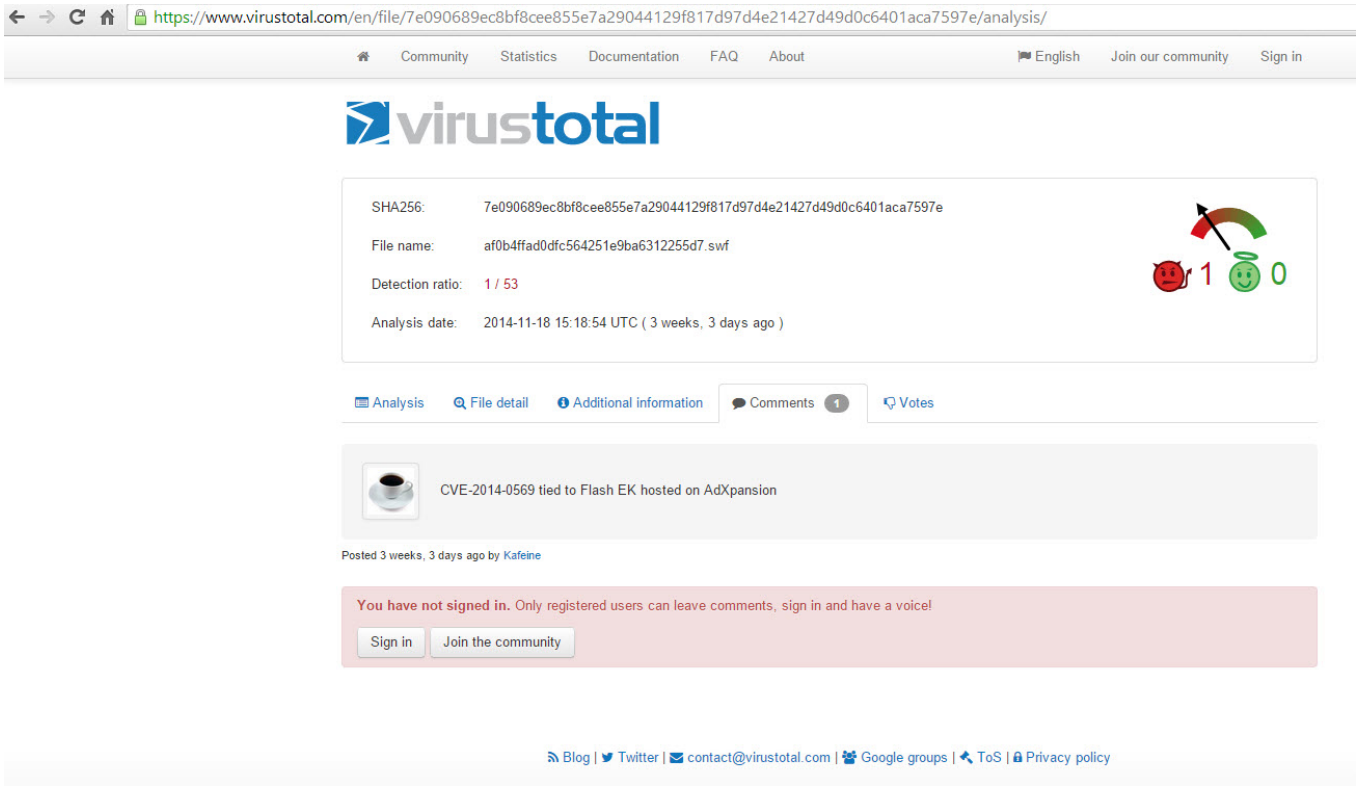
Ücretli kaynak koda çevirici yazılımların çuvalladığı noktada JPEXS Flash Decompiler aracına bir şans vermek istedim. SWF dosyasını bu araçla açtığımda, BinaryData kısmında başka bir SWF dosyası daha olduğunu gördüm. Bunu da açıp içine baktığımda ise bunun DOSWF isimli bir araç ile şifrelendiği ve gizlendiğini gördüm.



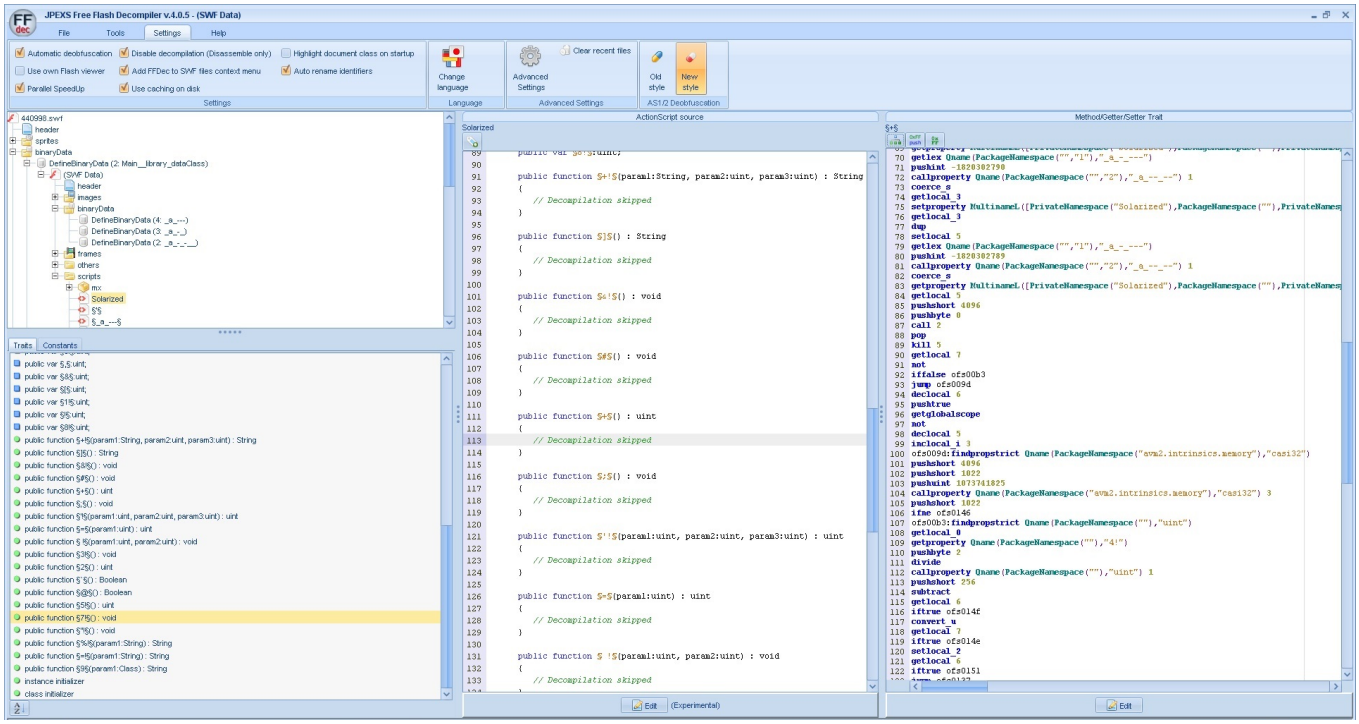
440998.swf isimli dosyayı VirusTotal sitesine yüklediğimde, 55 tane Antivirüs yazılımından sadece 2 tanesinin bunu zararlı yazılım olarak tespit edebiliyordu. VirusTotal analiz raporunun File detail bölümünde, bu SWF dosyasının DOSWF programı ile gizlendiği, şifrelendiği ve DOSWF programının Username:zlaszloflash@yandex.ru.fr adına lisanslı olduğunu gördüm. “zlaszloflash@yandex.ru.fr” e-posta adresini Google’da arattığımda bu defa başka bir VirusTotal analiz raporu ile daha karşılaştım ve bu analizin yorumlar (comments) kısmında burada kullanılan istismar kodunun CVE-2014-0569 zafiyetini istismar ettiği bilgisine yer verilmişti.


Antivirus scan for cb3af4fa5affcf031948f6f2793da99aaf759a978f72c500d442abf8591f366d
https://www.virustotal.com/en/file/cb3af4fa5affcf031948f6f2793da99aaf759a978f72c500d442abf8591f366d/analysis/1417592493/
Community
Statistics
Documentation
FAQ
About
English
Join our community
Sign in
virustotal
SHA256: cb3af4fa5affcf031948f6f2793da99aaf759a978f72c500d442abf8591f366d
File name: 440998.swf
Detection ratio: 2 / 55
Analysis date: 2014-12-03 07:41:33 UTC (1 week, 2 days ago) View latest
0 0
Analysis
File detail
Additional information
Comments 0
Votes
Antivirus
Result
Update
McAfee-GW-Edition
BehavesLike.Flash.Exploit.nb
20141202
Norman
Exploit.ANS
20141203
ALYac
20141203
AVG
20141203
AVware
20141121
Ad-Aware
20141203
AegisLab
20141203
Agnitum
20141201
AhnLab-V3
20141202

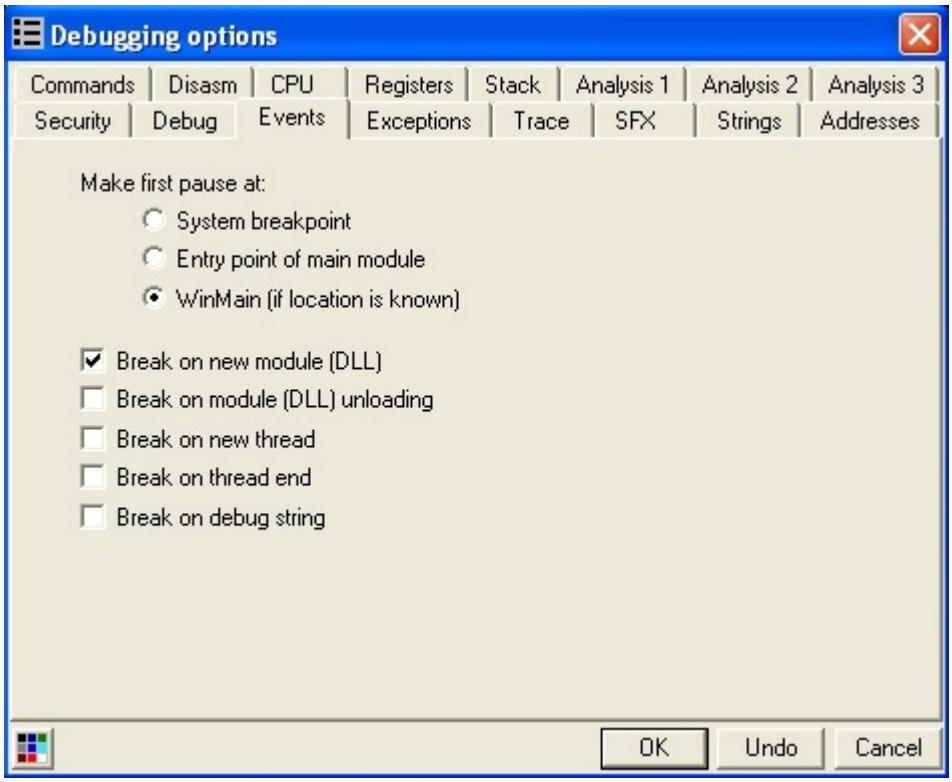

Antivirus scan for cb3af4fa5affcf031948f6f2793da99aaf759a978f72c500d442abf8591f366d
https://www.virustotal.com/en/file/cb3af4fa5affcf031948f6f2793da99aaf759a978f72c500d442abf8591f366d/analysis/1417592493/
Community
Statistics
Documentation
FAQ
About
English
Join our community
Sign in
Duration
0.033 seconds
File attributes
HasMetadata, ActionScript3, UseNetwork
Unrecognized SWF tags
2
Total SWF tags
16
ActionScript 3 Packages
flash.accessibility
flash.display
flash.events
flash.geom
flash.net
flash.system
flash.utils
mx.core
mx.events
mx.utils
SWF metadata
<![CDATA[<rdf:RDF xmlns:rdf="http://www.w3.org/1999/02/22-rdf-syntax-ns#"><rdf:Description rdf:about="flash swf encrypt" xmlns:dc="http://purl.org/dc/elements/1.1/"><dc:title>Encrypted by DoSWF</dc:title><dc:description>Version:2.3.0
Username:zlaszloflash@yandex.ru.fr
Index:http://www.doswf.com
Author:http://www.laaan.cn</dc:description></rdf:Description></rdf:RDF>]]>

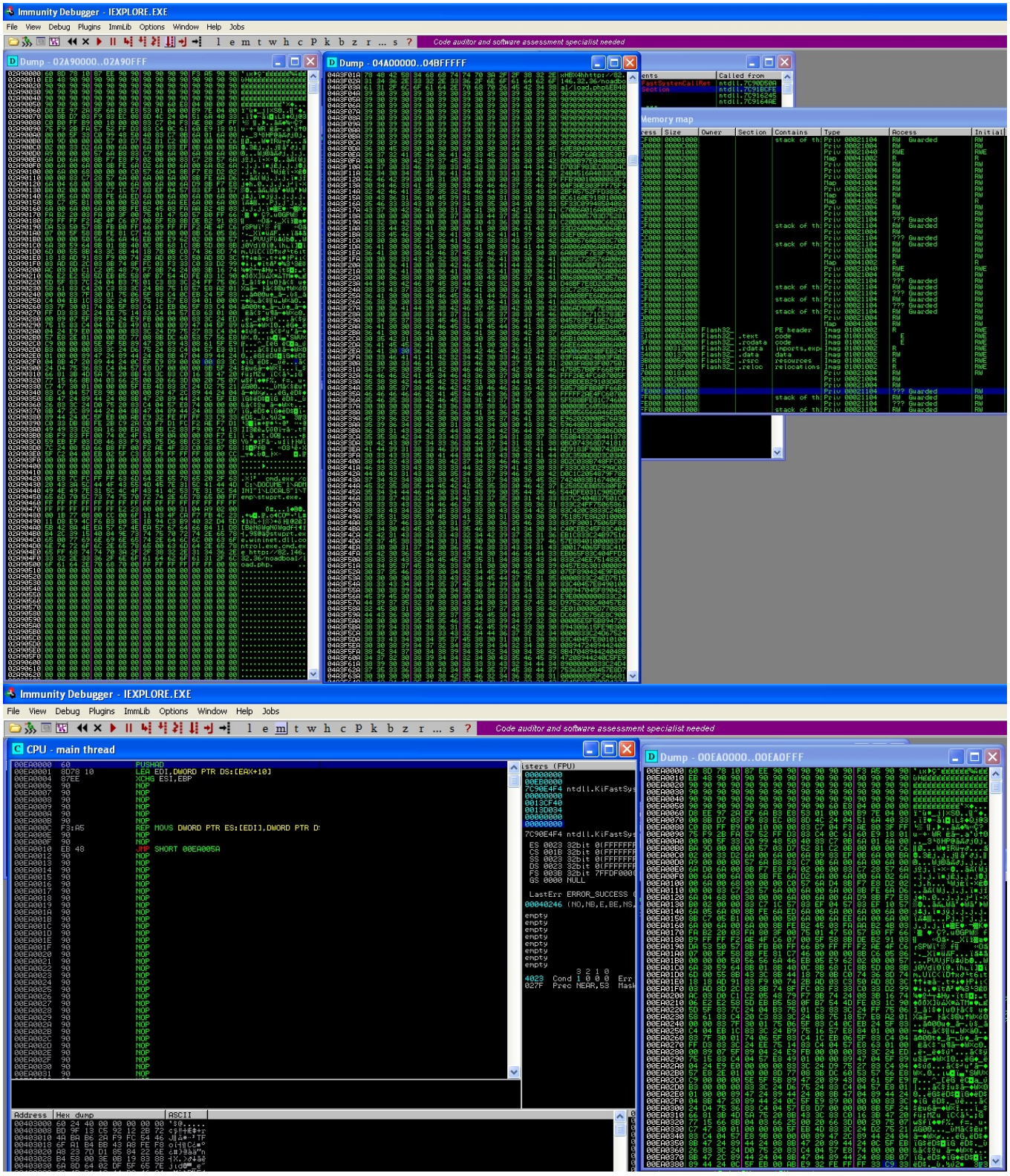


ZDI'ın web sitesinde, CVE-2014-0569 zafiyetinin casi32 fonksiyonu ile ilgili olduğu bilgisine yer verilmişti. JPEXS aracı ile SWF dosyasının baytkodunu incelediğimde, bu istismar kodunun casi32 fonksiyonunda bulunan tamsayı taşması (integer overflow) zafiyetini istismar ettiğini gördüm.

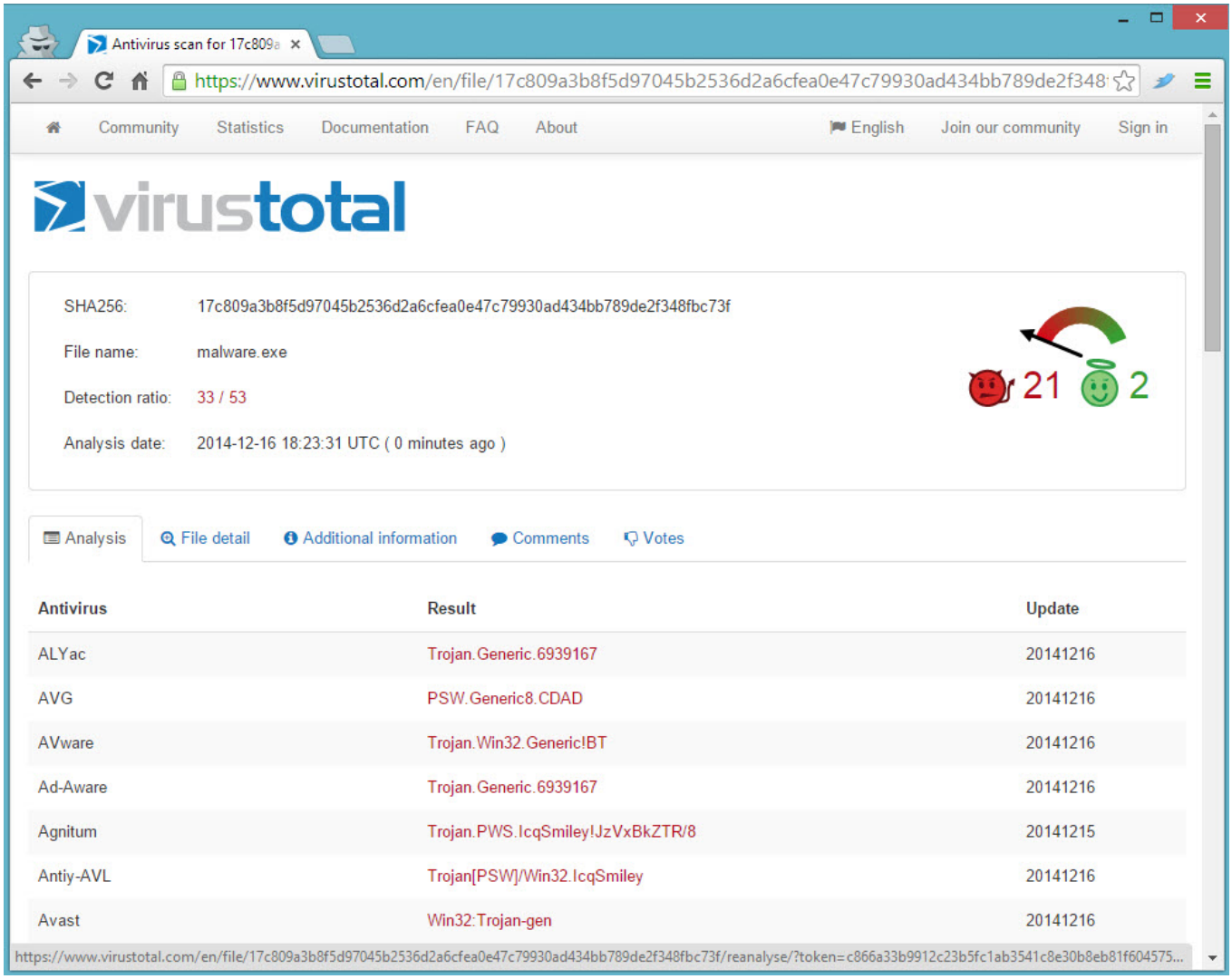


İstismar kodunun kalbine yani kabukkoduna ulaşmak için öncelikle sanal makineye Flash Player v12.0.0.77 (flashplayer12_0r0_77_winax.exe) sürümünü kurdum. Daha sonra Internet Explorer internet tarayıcısı ile 440998.swf dosyasını çalıştırıp, Immunity Debugger hata ayıklayıcısı ile incelemeye başladım. Immunity Debugger üzerinde yeni DLL yükleyince durakla özelliğini aktif hale getirdikten kısa bir süre sonra bellekte 9090909090 baytlarını aratarak kabukkoduna kolayca ulaşabildim.





Ortaya çıkan kabukkodunu incelediğimde, bunun dinamik analizden de anlaşıldığı üzere bir HTTP indirici (downloader) kabukkodu (shellcode) olduğu rahatlıkla anlaşılıyordu. Kabukkodu ile indirilen zararlı yazılımı, VirusTotal sitesinde analiz ettirdiğimde, bunun şifre çalan bir zararlı yazılım olduğu ve çok sayıda antivirüs yazılımı tarafından hali hazırda tespit edilebildiği ortaya çıktı.



Kıssadan hisse, bu vakada da olduğu gibi su kaynağı saldırıları, günümüzde art niyetli kişiler tarafından sıklıklıkla kullanılan yöntemlerden sadece bir tanesidir. Özellikle bu yönteme karşı çalışanlarını korumak isteyen, olası bir sızma girişiminden haberdar olmak isteyen kurumlar, sıkı güvenlik politikalarının yanı sıra kum havuzu analizinden faydalanan sistemleri de mevcut güvenlik sistemlerine ek olarak değerlendirebilirler.

Tabi bu tür sistemlerin kur ve unut türü sistemler olmadığını dolayısıyla bu sistemleri yönetecek veya SOME gibi faydalanacak ekiplerin, zararlı yazılım analizi bilgi ve becerisine sahip olmaları gerekeceğinin de altını çizmekte fayda var.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.