

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 karşılanmaktadır. 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.

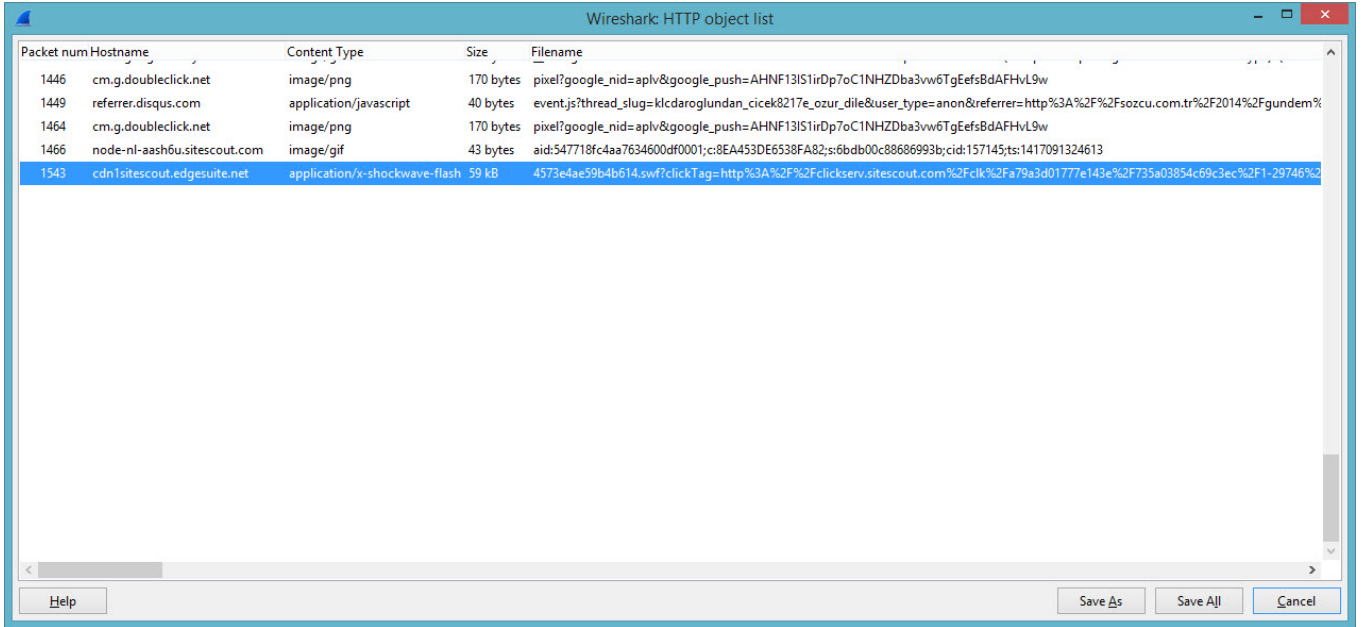
Elinin altında Fireeye NX gibi kum havuzu analizinden faydalanarak ağ üzerinden zararlı yazılım tespiti yapabilen cihazı olanlar, 27 Kasım tarihinde Sözcü Gazetesi kaynaklı bir alarmla karşılaşmışlardır. Fireeye NX cihazı tarafından üretilen PCAP trafik dosyası ve analiz raporu incelendiğinde, Sözcü Gazetesi'nin web sitesinde yer alan reklam içeriğinin çekildiği bir sitenin (static.adhood.com/passbacks/sozcu_east/sozcu_east_passback_728x90.html) hacklendiği anlaşılabilirdi. 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.ahood.com/passbacks/sozcu_east/sozcu_east_passback_72890.html	11/27/14 14:28:42	text/html	optimized-by.rubiconproject.com/s/11252/23746/119642-2_3e74c2e0d_50554078683448581c_s1-larfbtq43a//app.pubserver.ahood.com/token43f_43bvr1426async3d1426div43d1426member43d82400426zonsid43d9704426width43d728426height43d90426extra_data43dchirdpartyrur14263	11/27/14 14:28:44	text/javascript
sozcu.com.tr/	11/27/14 14:28:22	text/html	pixel1.sitescout.com/dmp/pixel1sync?nid=1&wb=1&hddid=1	11/27/14 14:28:45	image/png
ads.rubiconproject.com/ad/11252.js	11/27/14 14:28:33	text/javascript	cm.g.doubleclick.net/pixel1google_nid=apl6google_push=AHNF131ilrip7c0iWm2ba3w6v9gafad8p9d9w	11/27/14 14:28:45	application/x-shockwave-flash
tap2-odn.rubiconproject.com/partner/scripts/rubicon/emily.html?rtb_ext=1&pc=11252/29746&noscore=1	11/27/14 14:28:35	text/html	cdn1.sitescout.edgesuite.net/65500/65427/4573e4ae59b4b614.swf?elicktag=http43a424242e1c1ckserv.sitescout.com2f2c1k42Fa79a3d01777e143e42f735a03854c69c3ec42f1-2974642f242app.pubserver.ahood.com42f42f547718fc4aa7634600d4f00142f42f4cde5xg3158k9mstr0283g0m5z	11/27/14 14:28:45	image/gif
r.254a.com/r_match	11/27/14 14:28:35	text/html	node-nl-tash6s.sitescout.com/rubicon/pix/aid:547718fc4aa7634600d4f001	11/27/14 14:28:46	text/html
pixel1.rubiconproject.com/tap.php?v=17329&nid=28674&put=d718ef13-94c4-4d4d-bd8e-2635e6118acb&expires=30	11/27/14 14:28:35	image/gif	pixel1.rubiconproject.com/tap.php?v=4222&nid=1512&put=8205449-fdea-4100-8eb1-39eb12bbf321	11/27/14 14:28:46	text/html
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	image/gif
app.pubserver.ahood.com/token?_w16async=1&div=1&member=82460&zonsid=97044&width=728&height=90&extadata=thirdpartyrur143d6data=http43a//http43a/sozcu.com.tr/,-120,v15,1024x819,tr,,http43a//sozcu.com.tr/2014/gundem/kilicdaroglundan-ciceke-ozur-dile-66013	11/27/14 14:28:37	text/html	sync.mathtag.com/sync/img?m_extid=9	11/27/14 14:28:46	
ad.360yield.com/adj?w=528767&w=728&h=90&tr=-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: [0x00010, http://82.146.32.54/noadboa2/load.php, NULL, 0, 0, 0x] ImagePath: C:\Program Files (x86)\Internet Explorer\iexplore.exe DLL Name: wininet.dll	1928		
		Call Stack:			
		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: [0x00018, 0x3730000, 28672, 0x32e0415] ImagePath: C:\Program Files (x86)\Internet Explorer\iexplore.exe DLL Name: wininet.dll	1928		
		Call Stack:			
		Frame No. Instruction Addr. Module Name Symbol Name SD			
		3 0x6a0e0a37 C:\Windows\SysWOW64\Macromed\Flash\Flash32_12_0_0_77.ocx	IARModule_IARKernel_UnloadModel	0x0011c067	
		4 0x6a0c6db1 C:\Windows\SysWOW64\Macromed\Flash\Flash32_12_0_0_77.ocx	IARModule_IARKernel_UnloadModel	0x001023e1	
		5 0x6a0f34ca C:\Windows\SysWOW64\Macromed\Flash\Flash32_12_0_0_77.ocx	IARModule_IARKernel_UnloadModel	0x0012eafa	
		6 0x6a0f2d31 C:\Windows\SysWOW64\Macromed\Flash\Flash32_12_0_0_77.ocx	IARModule_IARKernel_UnloadModel	0x0012e361	
		7 0x6a0f3a15 C:\Windows\SysWOW64\Macromed\Flash\Flash32_12_0_0_77.ocx	IARModule_IARKernel_UnloadModel	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: [0x00018] ImagePath: C:\Program Files (x86)\Internet Explorer\iexplore.exe DLL Name: wininet.dll	1928		
		Call Stack:			
		Frame No. Instruction Addr. Module Name Symbol Name SD			
		3 0x6a0e0a37 C:\Windows\SysWOW64\Macromed\Flash\Flash32_12_0_0_77.ocx	IARModule_IARKernel_UnloadModel	0x0011c067	
		4 0x6a0c6db1 C:\Windows\SysWOW64\Macromed\Flash\Flash32_12_0_0_77.ocx	IARModule_IARKernel_UnloadModel	0x001023e1	
		5 0x6a0f34ca C:\Windows\SysWOW64\Macromed\Flash\Flash32_12_0_0_77.ocx	IARModule_IARKernel_UnloadModel	0x0012eafa	
		6 0x6a0f2d31 C:\Windows\SysWOW64\Macromed\Flash\Flash32_12_0_0_77.ocx	IARModule_IARKernel_UnloadModel	0x0012e361	
		7 0x6a0f3a15 C:\Windows\SysWOW64\Macromed\Flash\Flash32_12_0_0_77.ocx	IARModule_IARKernel_UnloadModel	0x0012f045	

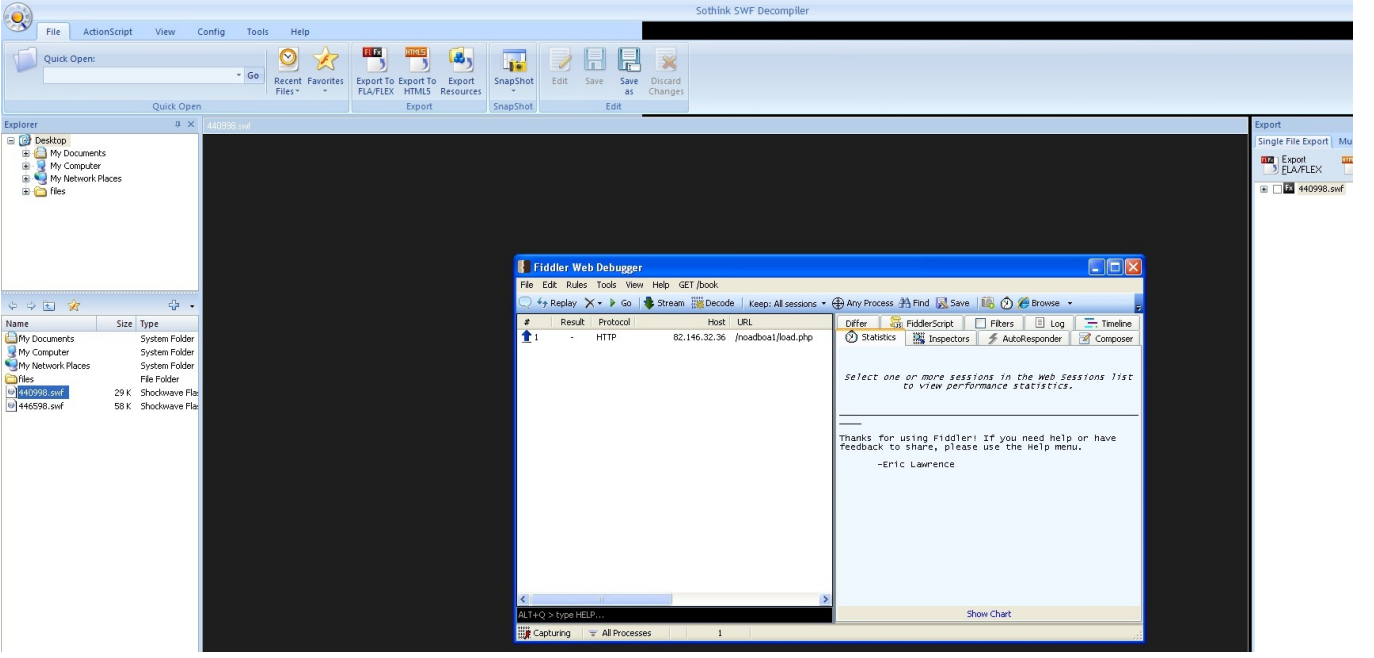
Bunun üzerine analiz raporunda yer alan SWF uzantılı Flash Player dosyasını incelemeye ve bunun hangi zafiyeti istismar ettiğini öğrenmeye karar verdim. İlk iş olarak Fireeye tarafından bu trafiğe özel olarak üretilen PCAP dosyasını Wireshark ile açtım. Ardından bu dosyadan çıkardığım (File -> Export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



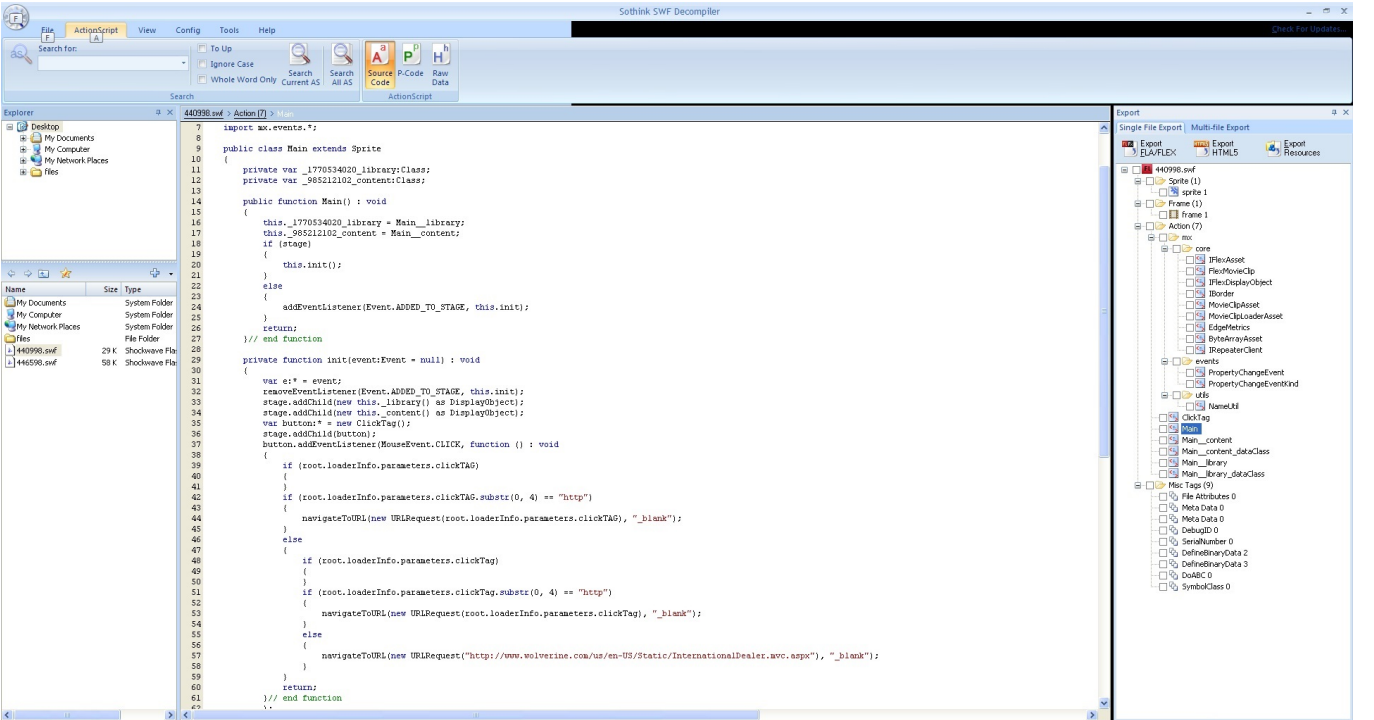
Packet num	Hostname	Content Type	Size	Filename
1446	cm.g.doubleclick.net	image/png	170 bytes	pixel?google_nid=aplv&google_push=AHNF13IS1irDp7oC1NHZDba3vw6TgEefsBdAFHvL9w
1449	referrer.disqus.com	application/javascript	40 bytes	event.js?thread_slug=klcdaroglundan_cicek8217e_ozur_dile&user_type=anon&referrer=http%3A%2F%2Fsozcu.com.tr%2F2014%2Fgundem%
1464	cm.g.doubleclick.net	image/png	170 bytes	pixel?google_nid=aplv&google_push=AHNF13IS1irDp7oC1NHZDba3vw6TgEefsBdAFHvL9w
1466	node-nl-aash6u.sitescout.com	image/gif	43 bytes	aid:547718fc4aa7634600df0001;c:8EA453DE6538FA82;s:6bdb00c88686993b;cid:157145;ts:1417091324613
1543	cdn1sitescout.edgesuite.net	application/x-shockwave-flash	59 kB	4573e4ae59b4b614.swf?clickTag=http%3A%2F%2Fclickserv.sitescout.com%2Fclk%2Fa79a3d01777e143e%2F735a03854c69c3ec%2F1-29746%2

İş 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.

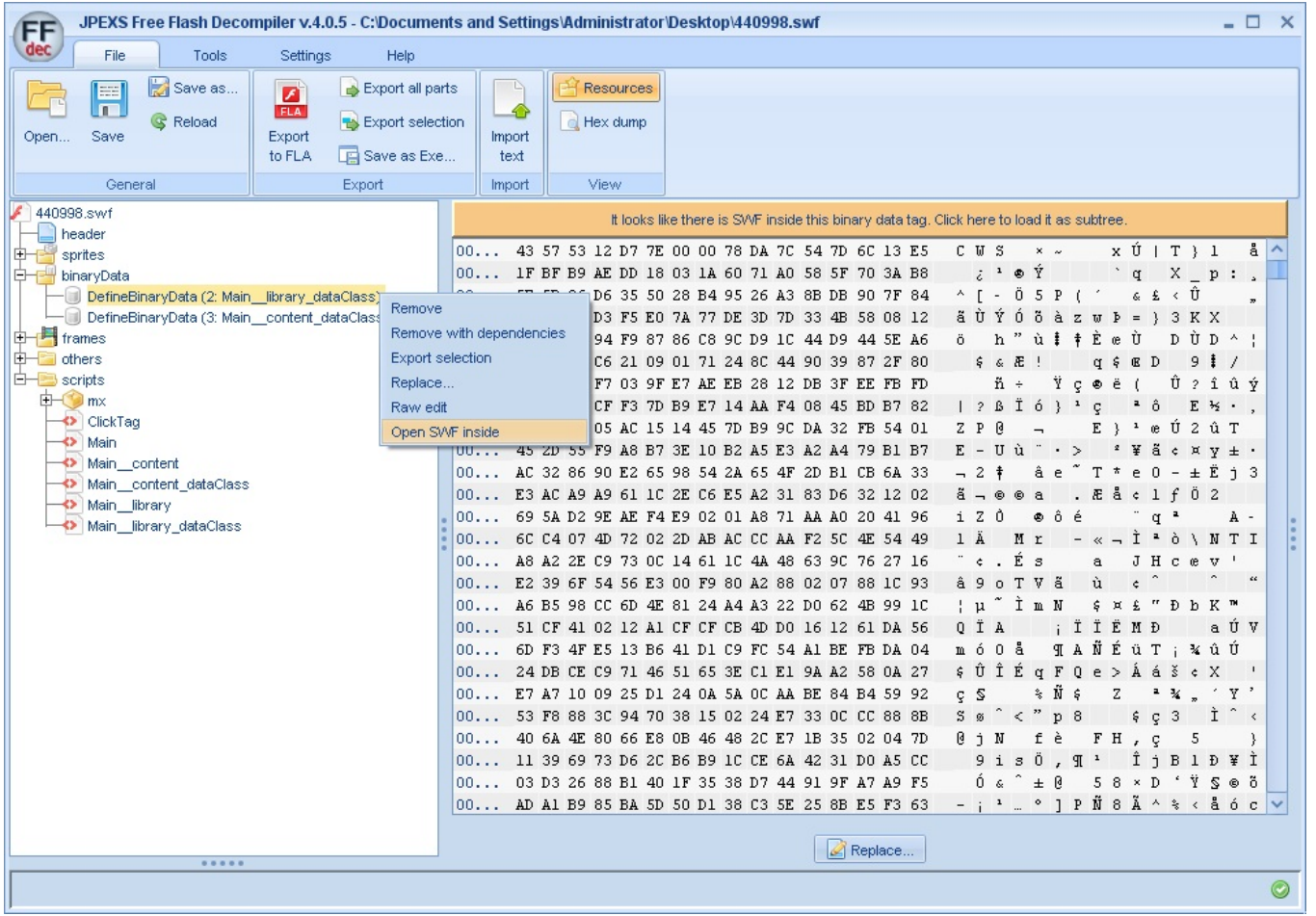
Her ne kadar kaynak koduna çevirme işlemi, statik kod analizi için yapıyor olsa da, Sothink SWF Decompiler gibi araçlar, bayt kodunu kaynak koduna çevirdikten hemen sonra bu SWF dosyalarını da çalıştırdıkları için sanal makinede yapılmayan bu kaynak koduna çevirme işlemi, sisteminizde istismar kodunun 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 çuvaldığı 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.



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](#)



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
Aegis.Lab	✓	20141203
Agnitum	✓	20141201
AhnLab-V3	✓	20141202

Duration 0:00:30 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>]]>
```



SHA256: 7e090689ec8bf8cee855e7a29044129f817d97d4e21427d49d0c6401aca7597e
File name: af0b4ffad0dfc564251e9ba6312255d7.swf
Detection ratio: 1 / 53
Analysis date: 2014-11-18 15:18:54 UTC (3 weeks, 3 days ago)



Analysis File detail Additional information Comments 1 Votes

 CVE-2014-0569 tied to Flash EK hosted on AdXpansion

Posted 3 weeks, 3 days ago by Kafeine


You have not signed in. Only registered users can leave comments, sign in and have a voice!

Sign in Join the community

ZDI'nin web sitesinde, CVE-2014-0569 zafiyetinin cas32 fonksiyonu ile ilgili olduğu bilgisine yer verilmişti. JPEXS aracı ile SWF dosyasının baytkodunu incelediğimde, bu istismar kodunun cas32 fonksiyonunda bulunan tamsayı taşması (integer overflow) zafiyetini istismar ettiğini gördüm.

www.zerodayinitiative.com/advisories/ZDI-14-365/

TippingPoint Zero Day Initiative



Adobe Flash Player cas32 Integer Overflow Remote Code Execution Vulnerability
ZDI-14-365: October 14th, 2014

CVE ID
CVE-2014-0569

CVSS Score
6.8, (AV:N/AC:M/Au:N/C:P/I:P/A:P)

Affected Vendors
Adobe

Affected Products
Flash Player

Vulnerability Details

This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Adobe Flash Player. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file.

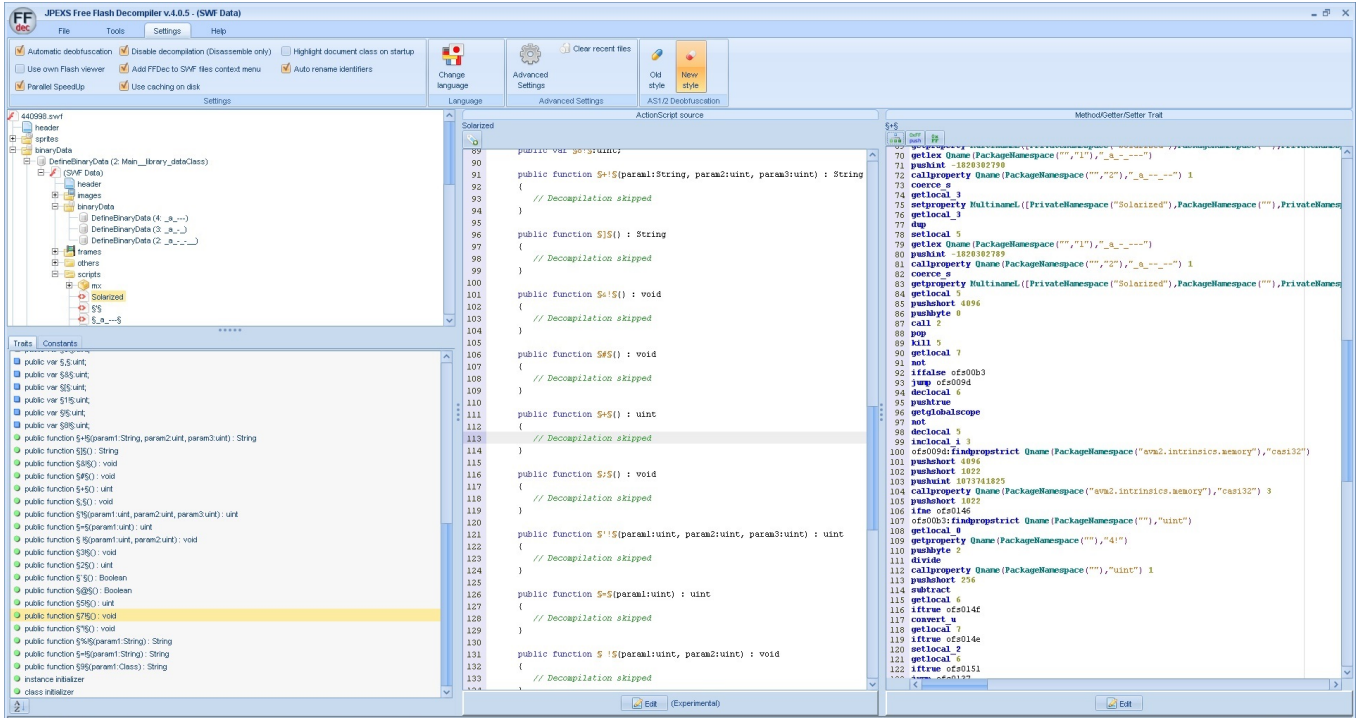
The specific flaw exists within the implementation of cas32. The issue lies in the failure to properly sanitize a user-supplied length value with a specific array implementation. An attacker can leverage this vulnerability to execute code within the context of the current process.

Vendor Response

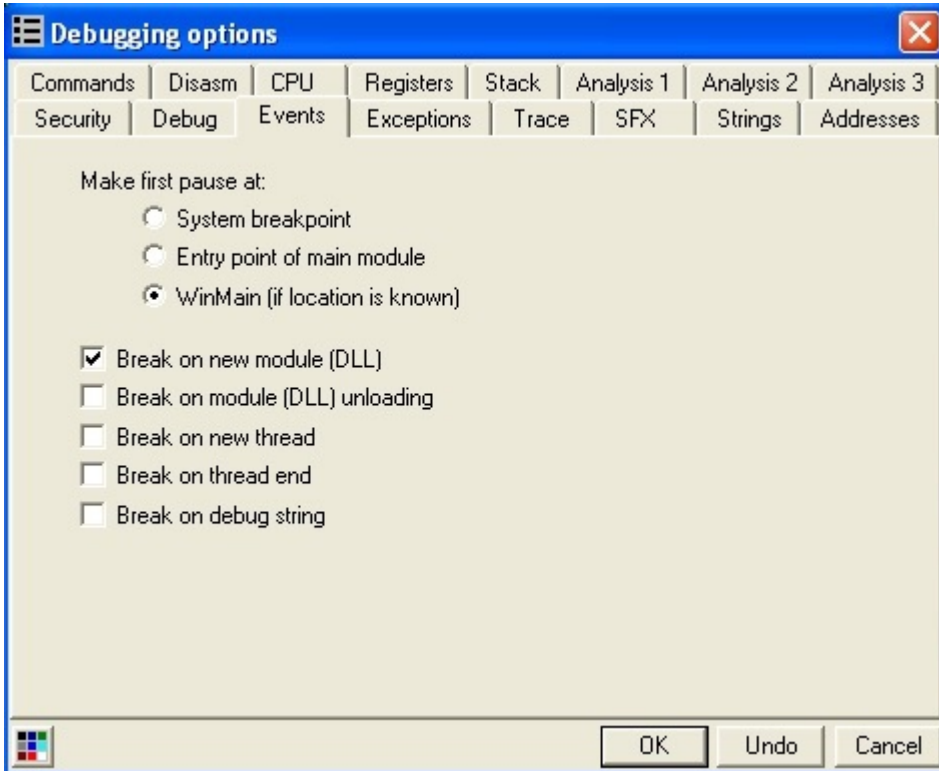
Adobe has issued an update to correct this vulnerability. More details can be found at:
<https://helpx.adobe.com/security/products/flash-player/apsb14-22.html>

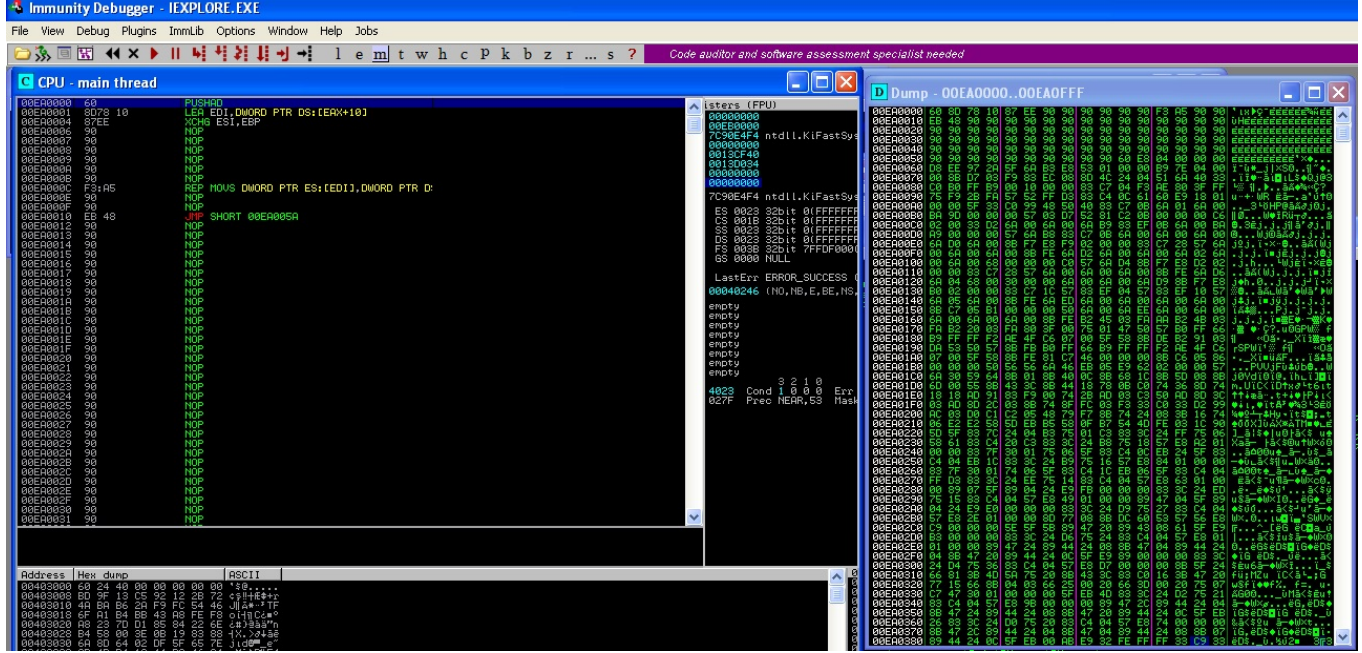
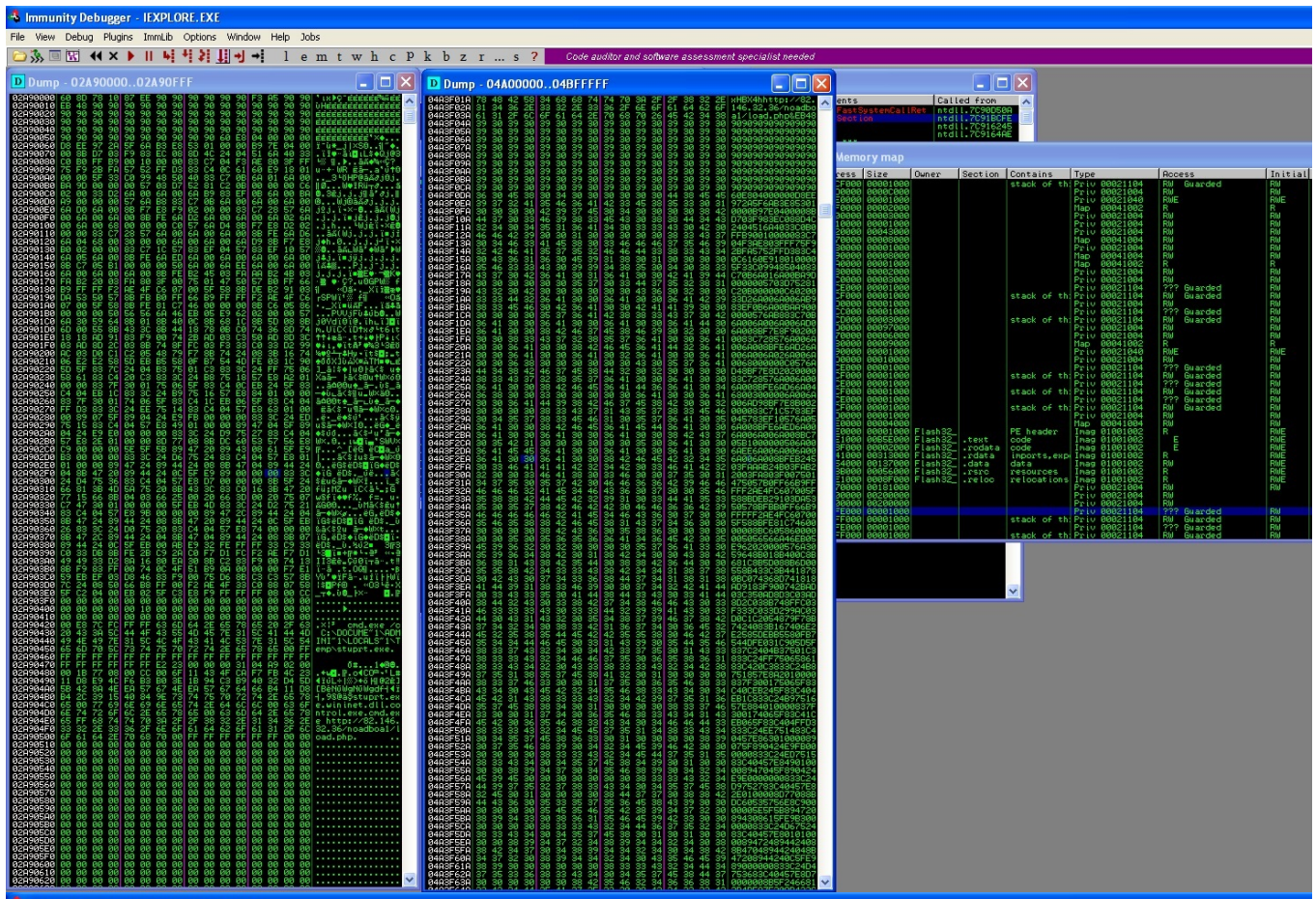
Disclosure Timeline

2014-09-10 - Vulnerability reported to vendor
2014-10-14 - Coordinated public release of advisory



İstismar kodunun kalbine yani kabuk koduna 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 kabuk koduna kolayca ulaşabildim.





Ortaya çıkan kabuk kodunu incelediğimde, bunun dinamik analizden de anlaşıldığı üzere bir HTTP indirici (downloader) kabuk kodu (shellcode) olduğu rahatlıkla anlaşılıyordu. Kabuk kodu 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.

Antivirus scan for 17c809a x

https://www.virustotal.com/en/file/17c809a3b8f5d97045b2536d2a6cfea0e47c79930ad434bb789de2f348fbc73f

Community Statistics Documentation FAQ About English Join our community Sign in


virustotal

SHA256: 17c809a3b8f5d97045b2536d2a6cfea0e47c79930ad434bb789de2f348fbc73f

File name: malware.exe

Detection ratio: 33 / 53

Analysis date: 2014-12-16 18:23:31 UTC (0 minutes ago)



Analysis File detail Additional information Comments Votes

Antivirus	Result	Update
ALYac	Trojan.Generic.6939167	20141216
AVG	PSW.Generic8.CDAD	20141216
AVware	Trojan.Win32.Generic!BT	20141216
Ad-Aware	Trojan.Generic.6939167	20141216
Agnitum	Trojan.PWS.IcqSmiley!JzVxBkZTR/8	20141215
Antiy-AVL	Trojan[PSW]/Win32.IcqSmiley	20141216
Avast	Win32:Trojan-gen	20141216

https://www.virustotal.com/en/file/17c809a3b8f5d97045b2536d2a6cfea0e47c79930ad434bb789de2f348fbc73f/reanalyse/?token=c866a33b9912c23b5fc1ab3541c8e30b8eb81f604575...

Kıssadan hisse, bu vakada da olduğu gibi su kaynağı saldırıları, günümüzde art niyetli kişiler tarafından sıklıkla 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.