HookAds Malvertising Installing Malware via the Fallout Exploit Kit

bleepingcomputer.com/news/security/hookads-malvertising-installing-malware-via-the-fallout-exploit-kit/

Lawrence Abrams

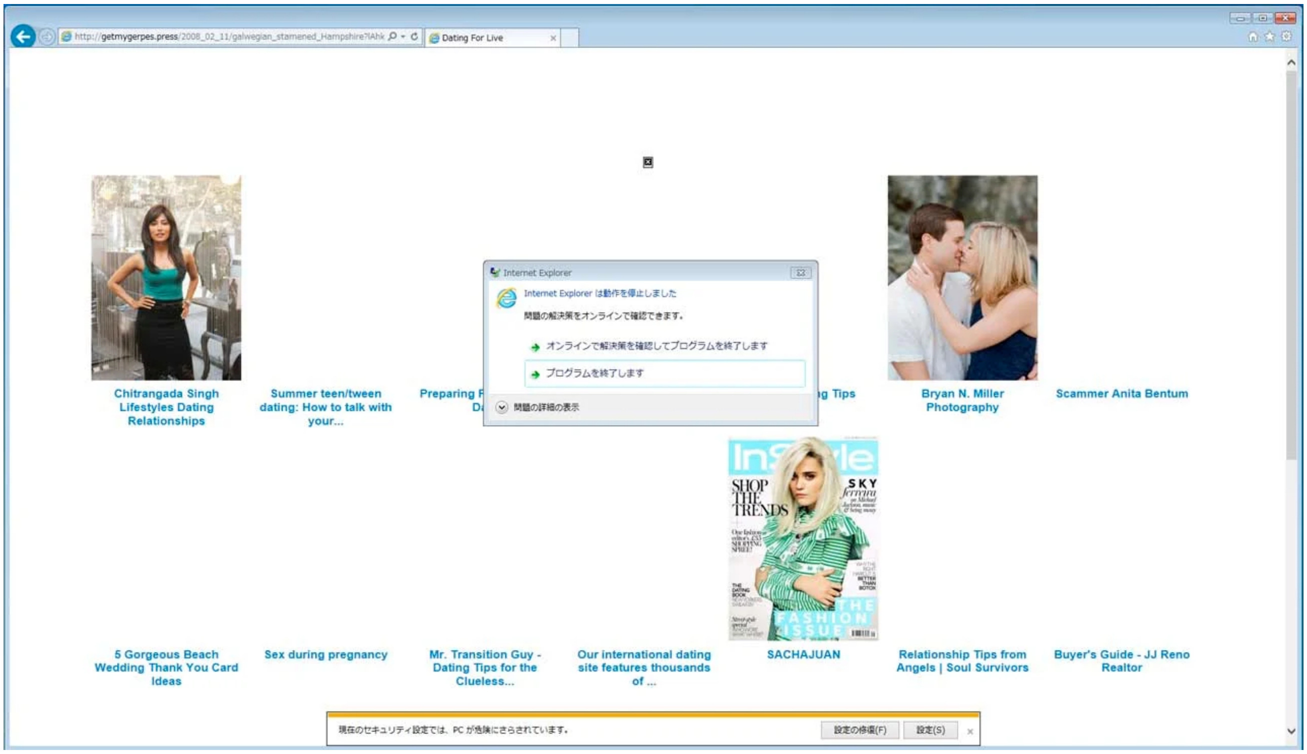
By
Lawrence Abrams

- November 13, 2018
- 03:30 AM
- 0

The HookAds malvertising campaign has been active lately and redirecting visitors to the Fallout Exploit Kit. Once the kit is activated, it will attempt to exploit known vulnerabilities in Windows to install different malware such as the DanaBot banking Trojan, the Nocturnal information stealer, and GlobeImposter ransomware.

HookAds is a malvertising campaign that purchases cheap ad space on low quality ad networks commonly used by adult web sites, online games, or blackhat seo sites. These ads will include JavaScript that redirects a visitor through a serious of decoy sites that look like pages filled with native advertisements, online games, or other low quality pages. Under the right circumstances, a visitor will silently load the Fallout exploit kit, which will try and install its malware payload.

You can see an example of one of the decoy sites discovered last week by exploit kit expert nao_sec below.


http://getmygerpes.press/2008_02_11/galwegian_stamened_Hampshire?IAhk
Dating For Live
Chitrangada Singh Lifestyles Dating Relationships
Summer teen/tween dating: How to talk with your...
Preparing F... Da...
...g Tips
Bryan N. Miller Photography
Scammer Anita Bentum
5 Gorgeous Beach Wedding Thank You Card Ideas
Sex during pregnancy
Mr. Transition Guy - Dating Tips for the Clueless...
Our international dating site features thousands of ...
SACHAJUAN
Relationship Tips from Angels | Soul Survivors
Buyer's Guide - JJ Reno Realtor

Internet Explorer

Internet Explorer は動作を停止しました

問題の解決策をオンラインで確認できます。

→ オンラインで解決策を確認してプログラムを終了します

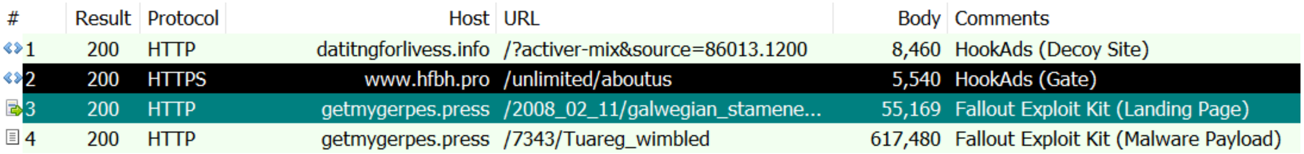
→ プログラムを終了します

問題の詳細の表示

現在のセキュリティ設定では、PC が危険にさらされています。 設定の修復(F) 設定(S)

Example HookAds Decoy Site

According to nao_sec, these two campaigns were discovered last week with one campaign being on November 8th that was distributing the DanaBot password stealing Trojan and another campaign on November 10th that was installing the Nocturnal stealer and the GlobeImposter ransomware.



#	Result	Protocol	Host	URL	Body	Comments
1	200	HTTP	datitngforlivess.info	/?activer-mix&source=86013.1200	8,460	HookAds (Decoy Site)
2	200	HTTPS	www.hfbh.pro	/unlimited/aboutus	5,540	HookAds (Gate)
3	200	HTTP	getmygerpes.press	/2008_02_11/galwegian_stamene...	55,169	Fallout Exploit Kit (Landing Page)
4	200	HTTP	getmygerpes.press	/7343/Tuareg_wimbled	617,480	Fallout Exploit Kit (Malware Payload)

Fiddler Traffic showing Redirects from HookAds campaign

If the redirected user is running Internet Explorer, the Fallout Exploit Kit will attempt to exploit the Windows CVE-2018-8174 VBScript vulnerability to install the payload.

Therefore, it is very important that users make sure to have all available Windows security updates installed in order to protect themselves from known vulnerabilities.

Related Articles:

New ChromeLoader malware surge threatens browsers worldwide

RIG Exploit Kit drops RedLine malware via Internet Explorer bug

- DanaBot
- Exploit Kit
- Fallout Exploit Kit
- GlobeImposter
- HookAds

- Malvertising

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

Post a Comment Community Rules

You need to login in order to post a comment

Not a member yet? Register Now

You may also like: