HookAds Malvertising Installing Malware via the Fallout Exploit Kit

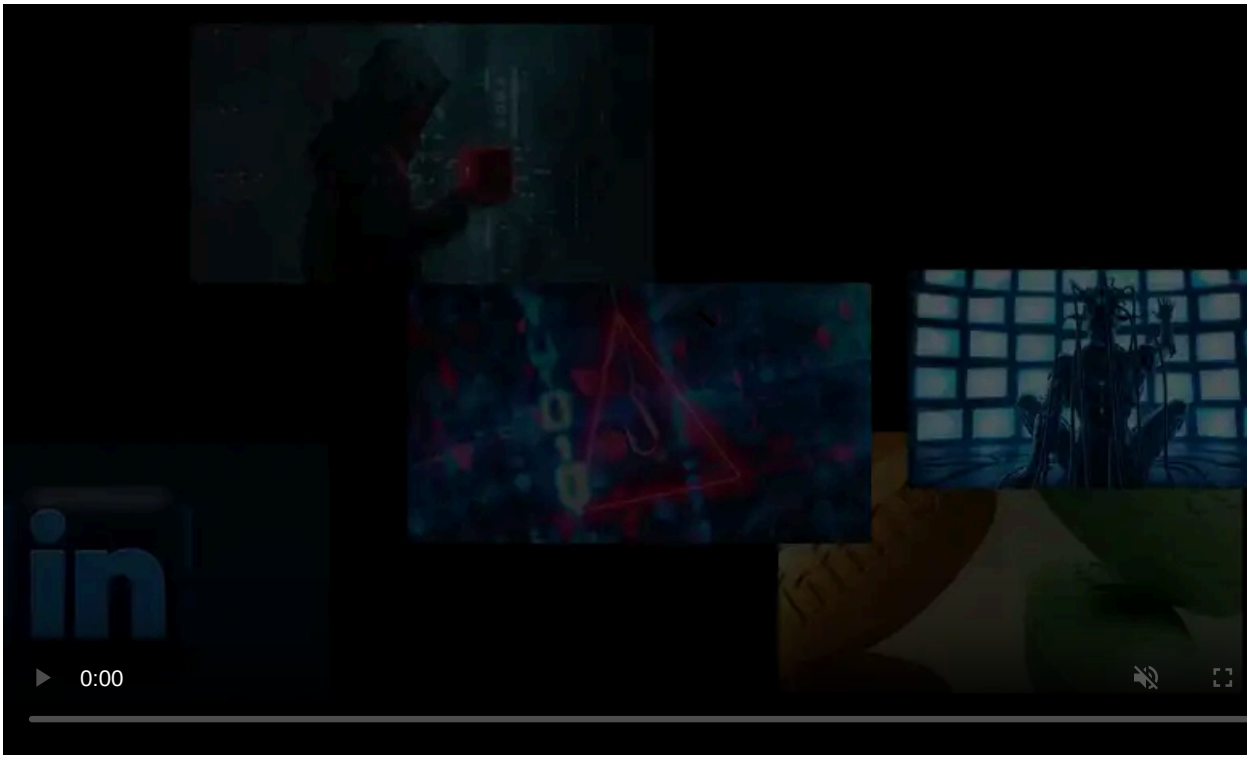
By Lawrence Abrams

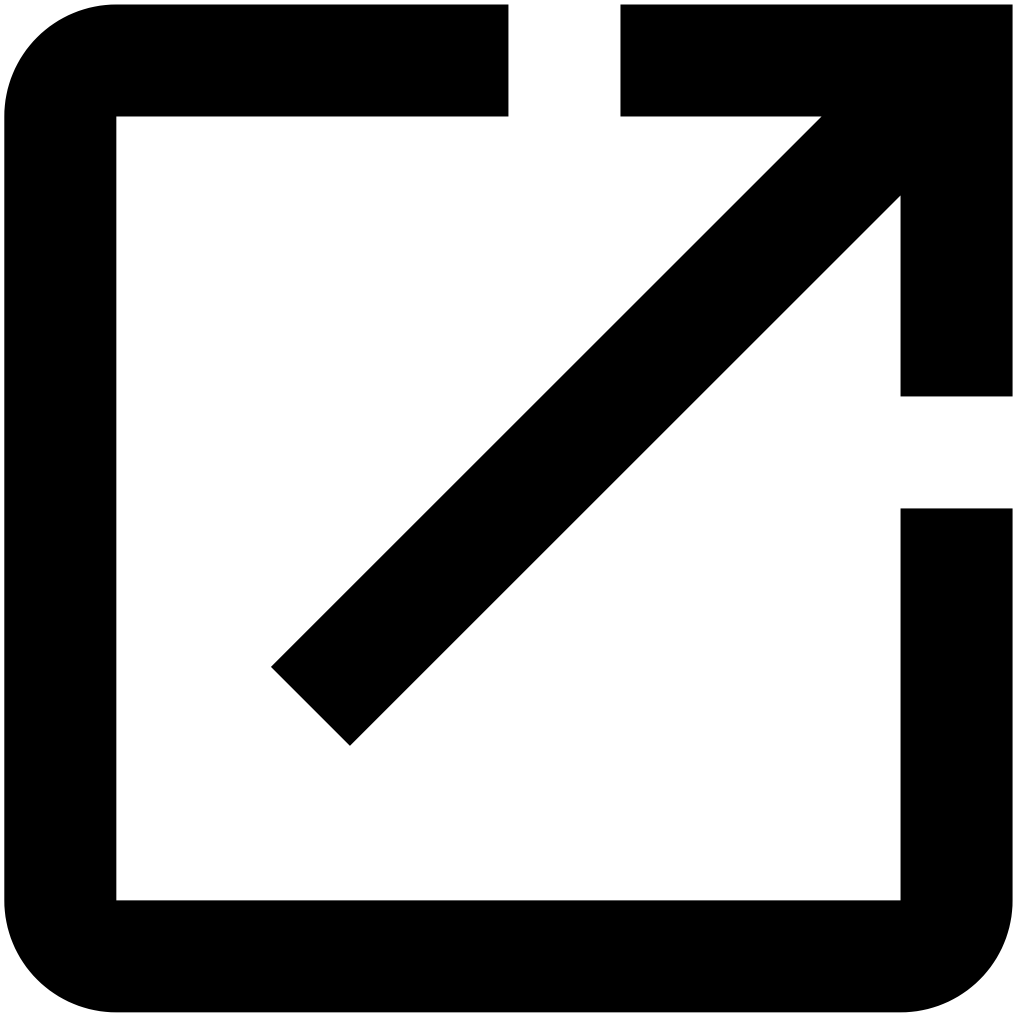
Published: 2018-11-13 · Archived: 2026-04-05 18:58:32 UTC

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.

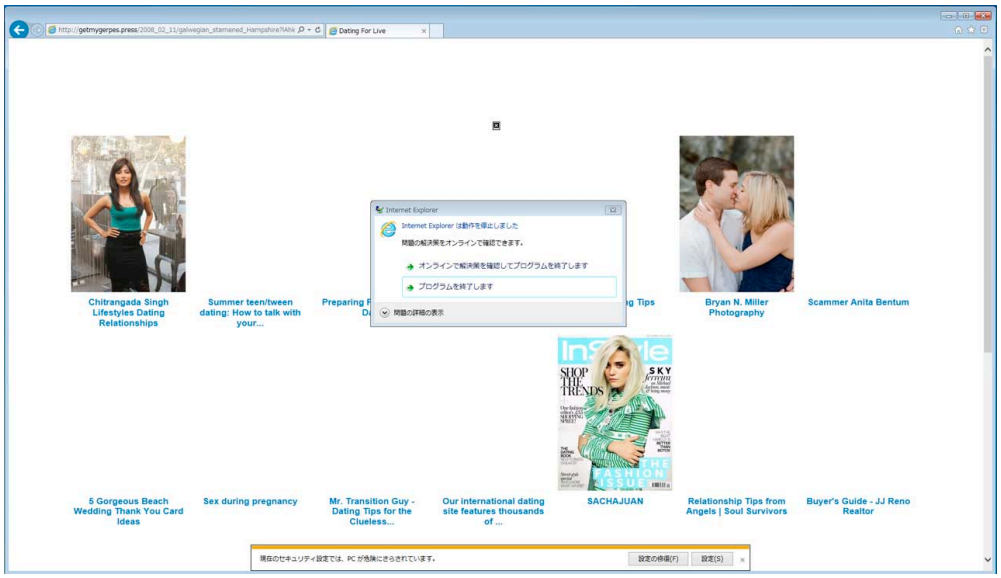
HookAds is a malvertising campaign that purchases cheap ad space on low quality ad networks commonly used by adult web sites, online games, or blackhat seo sites. These ads will include JavaScript that redirects a visitor through a serious of decoy sites that look like pages filled with native advertisements, 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.


0:00



Visit Advertiser website[GO TO PAGE]



Example HookAds Decoy Site

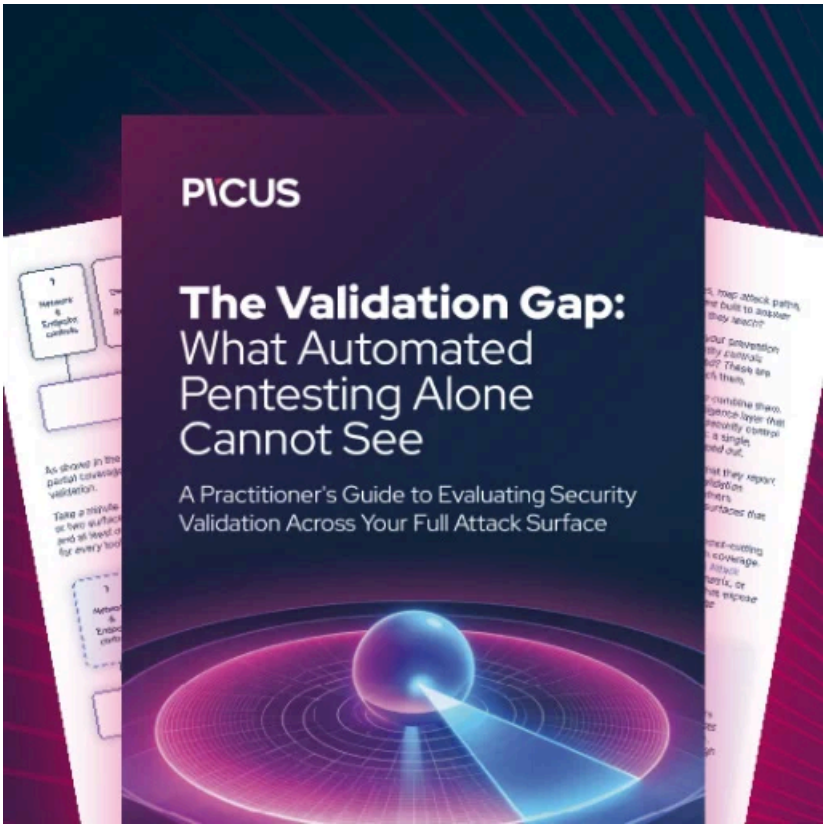
According to nao_sec, these two campaigns were discovered last week with one campaign being on November 8th that was distributing the DanaBot password stealing Trojan and another campaign on November 10th that was installing the Nocturnal stealer and the GlobeImposter ransomware.

#	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.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

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