SECURITY

This article is more than **1 year old**

Wicked WikiLeaks leaks considered harmful: Alert over malware lurking in dumped docs

Tip-toe through the old-days, hope you don't hit a zero-day

Chris Williams, Editor in Chief

Fri 17 Jul 2015 // 05:01 UTC

Documents laced with malware have been found in WikiLeaks.org's cache of files obtained from hacked CIA wannabe Stratfor.

Intelligence biz Stratfor was ransacked by Jeremy Hammond in late 2011, and its email archives passed to whistleblowing website WikiLeaks in early 2012. The Julian Assange™-led organization soon began distributing the archives using the BitTorrent file-sharing network, and publishing extracts on its website. In March 2015, WikiLeaks made the emails available in a handy searchable database, just like it's done with the leaked Sony Pictures and Hacking Team files.

Unfortunately, no one appears to have had the time to scrub the five million Stratfor emails, which date back to 2001, clean of malware.

Josh Wieder, a sysadmin who found a load of bad code in the Stratfor leaks, fears journalists, activists, researchers and anyone else curious enough to peruse the disclosed data may end up infecting themselves with a software nasty.

El Reg has verified that the documents identified by Wieder are dangerous. A lot of the malware is smuggled in as VBScript macros, or OLE and PE files. It's possible there are more infected files lurking in WikiLeaks' databases of unfiltered data.

For example, take this internal memo dated February 2011 about Cyrenaica and Tripolitania, two regions of conflict-torn Libya. The attached Microsoft Word document triggers malware alarms on VirusTotal because it includes a code-execution exploit for Microsoft Office on Windows and Mac (CVE-2010-3333).

Wieder, who has blogged about his findings here and in more detail here, has helpfully drawn up a list of Stratfor emails to avoid.

"I recently took a look at the Wikileaks 'Global Intelligence Files,' a giant trove of emails from defense contractor Stratfor, provided to WikiLeaks by former LulzSec member Jeremy Hammond," Wieder told *The Register* on Thursday.

"Inside the trove I found 18 pieces of live malware, most of which were embedded within PDF, Excel and Word files. At least one of the malware scripts was designed to scrape user registration information like name and address from applications and send it back to a remote server."

'A photo in an article is usually believed to not contain spyware'

Wieder says he's been trying to contact the whistleblowing website to get the data cleaned up. He argues that you wouldn't expect a reputable news source to host malicious files, so WikiLeaks – which seeks to hold power to account – shouldn't either.

"An expectation that a video posted on Fox News will not contain an embedded script is not a wild expectation," Wieder noted.

"Similarly a *New York Times* article that includes a photo in an article is usually believed to not contain spyware. This is a basic expectation of service on every website, not just news outlets. Primary sources are important. User transparency is also important."

It is worth noting that a lot, if not all, of these blobs of malware exploit vulnerabilities that have been patched by software makers. If you keep your machine up to date with security upgrades, you'll most likely dodge the bullets.

"I haven't had an opportunity to either complete a review of all the attachments in the [Stratfor files] dump (or other file dumps for that matter), nor test the malware on a few different software and OS version combinations to get a good feel for the behavior of each," Wieder added.

"I am reaching out to the public for two reasons: the first is to make sure that users are warned but also, and perhaps just as importantly, is to get assistance from some security researchers."

If you're combing through the Stratfor memos – or any of the other hundreds of thousands of leaked emails and documents WikiLeaks is hosting – do take care, and consider opening any files in a locked-down throwaway virtual machine just in case there's anything really nasty lurking inside.

A spokesperson for WikiLeaks was not available for comment. ®