APT REPORTS

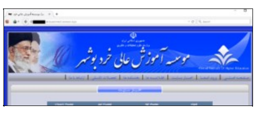
Freezer Paper around Free Meat

Repackaging Open Source BeEF for Tracking and More

By GReAT on April 27, 2016. 11:20 am

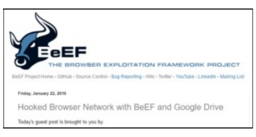
BeEF Wrapped Up and Delivered in 2016

In late February 2016, a University website in Iran stood out for thoroughly vetting its current and potential students and staff. The University's web site served repackaged content from the Browser Exploitation Framework (BeEF) with embedded JavaScript content maintaining the potential to hook visitors' web browsers, identify visited websites and domains, explore for vulnerabilities (we did not observe any auto-pwning), and provide tracking through evercookies. Even a partial listing of visited sites can be sensitive and valuable information, and this sort of "sites visited" data gathering via other techniques, like screengrabbing and keylogging, were observed in past APT incidents like the Madi campaigns. Currently, it's advisable to avoid the site.



The embedded BeEF content appears not to be fully configured, and only partially implemented. Perhaps a limited data set was of interest for this attacker, or this was an early attempt at deploying BeEF.

This incident is interesting because at the same time and a bit earlier, another group was heavily relying on repackaging open source offensive security product in their toolset by deploying both BeEF and Metasploit-produced components across a select set of strategic web compromises. This particular APT has years of low-tech elaborate social engineering schemes and re-purposed open source efforts under its belt.


BeEF
THE BROWSER EXPLOITATION FRAMEWORK PROJECT
BeEF Project Home - GitHub - Source Control - Bug Reporting - Wiki - Twitter - YouTube - LinkedIn - Mailing List

Friday, January 22, 2016

Hooked Browser Network with BeEF and Google Drive

Today's guest post is brought to you by:

While we call them the NewsBeef APT, they have been reported in the past as Charming Kitten or Newscaster in 2014, social engineering their way into sensitive circles of trust with spoofed LinkedIn profiles and phony news media organizations.

They continue to be highly active, but this time, they are using a slightly more technical toolset. On one hand, they have developed skills or discovered tools to compromise select web applications and sites, supporting their watering hole campaigns. On the other hand, they have repackaged leaked bot source code and repackaged open source Metasploit and PowerSploit components to produce and administer backdoors and downloaders.

Newsbeef/Newscaster will find a way to compromise a web site, usually the vulnerability appears to be CMS related, in an outdated WordPress plugin, Joomla version, or Drupal version. Attackers usually perform one of two things, Newsbeef has been performing the first of the two:

- inject a src or iframe link into web pages or css sheets
- inject the content of an entire BeEF web page into one of the internally linked javascript helpers

The injected link will redirect visitors' browsers to a BeEF server. Usually, the attackers deliver some of the tracking and system/browser identification and evercookie capabilities. Sometimes, it appears that they deliver the metasploit integration to exploit and deliver backdoors (we haven't identified that exploitation activity in our ksn data related to this group just yet). Sometimes, it is used to pop up spoofed login input fields to steal social networking site credentials. We also haven't detected that in ksn, but some partners have privately reported it about various incidents. But we have identified that attackers will redirect specific targets to laced Adobe Flash and other installers from websites that they operate.

So, the watering hole activity isn't always and usually isn't delivering backdoors. Most of the time, the watering hole injections are used to identify and track visitors or steal their browser history. Then, they deliver the backdoors to the right targets.

In addition to the University site and the NewsBeef APT, in the past couple of months, we identified a variety of compromised sites around the world serving the BeEF. Most are cleaned up. Deployments to interesting and strategic web sites and their true reach on a global scale appears to be on the increase:

- Middle eastern embassy in the Russian Federation
- Indian military technology school
- High conflict regional presidency
- Ukrainian ICS Scanner mirror
- European Union education diversification support agency
- Russian foreign trade management organization
- Progressive Kazakh news and politics media
- Turkish news organization
- Specialized German music school
- Japanese textile manufacturing inspection corporate division
- Middle Eastern social responsibility and philanthropy
- surprisingly popular British "lifestyle" blog
- Algerian University's online course platform
- Chinese construction group
- Russian overseas business development and holding company
- Russian gaming developer forum
- Romanian Steam gaming developer
- Chinese online gaming virtual gold seller
- Brazilian music instrument retailer

BeEF Capabilities

Key to these incidents are the development, distribution, and ease of use of toolkits like BeEF.

BeEF itself is an open source collection of tools and tricks, some years old, that combined together can effectively hook a visiting web browser for evaluation and full exploitation. Because of its capabilities, we have seen increased adoption of the framework for the past year or so.

- Browser enumeration and reporting
- Plugin enumeration and reporting
- Retrieve visited domains (based on an old browser cache fetch timing trick)
- Social engineering via live sessions and phishing within the browser
- Network exploration, discovery, and exfiltration tunneling
- Metasploit exploit integration and autopwning
- Evercookie deployment for persistent tracking – multiple platforms
- XSS evaluation and exploitation

At the same time, many of the techniques implemented are very old and public. The kit is extensible, customizable, and integrates with metasploit for autopwnage. Some of the techniques were discussed during Jeremiah Grossman's 2006 Black Hat conference presentation. The delay in deployment for techniques of this type indicates that some teams are dependent on open source tool packaging and ease of use. We have seen this sort of reliance on both open source offensive toolkits and legitimate software in the past from APT like Crouching Yeti, TeamSpy, and now the Newsbeef.

Fighting against the use of browser hooking frameworks for identification, tracking, live session social engineering, and precision and auto-exploitation effectively requires a mix of technologies. When these JavaScript-based frameworks are used in a malicious manner, the combination of network and host based detection is required to fully handle more serious incidents.

Unfortunately, these incidents are on the increase. You can disable JavaScript in your own browser with NoScript, but that's much like just moving to Lynx or a text-based browser – people don't want that because it kills functionality in the browser they do want. A Chrome plugin that detects the BeEF cookie is easily evaded by serious players. And preventing the tracking methods altogether is another whole ball of wax, because much of the functionality is tied into legitimate web pages by third party marketers and retailers.

Preventing the social engineering sessions for credential theft and Metasploit exploit integration makes immediate sense and can be incorporated at the network and more effectively at the host level. AntiAPT can help wipe out most of an operation on the network at scale, but these measures can be evaded as well. In other words, dealing with a determined attacker using tools like this one is difficult.

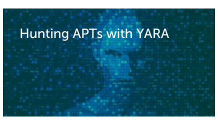
References

NEWSCASTER – An Iranian Threat Inside Social Media
The Browser Exploitation Framework Project
Metasploit: Penetration Testing Software

APT | CYBER ESPIONAGE | CYBERCRIME | TARGETED ATTACKS | VULNERABILITIES AND EXPLOITS | WEBSITE HACKS

Share post on:

Related Posts


Hunting APTs with YARA

Mokes and Buerak distributed under the guise of security certificates

Operation AppleJeus Sequel

IN THE SAME CATEGORY

APT trends report Q3 2019

COMpfun successor Reductor infects files on the fly to compromise TLS traffic

Recent Cloud Atlas activity

APT trends report Q2 2019

Turla renews its arsenal with Topinambour

LEAVE A REPLY

Your email address will not be published. Required fields are marked *

Enter your comment here

Name *

Email *

□
Save my name, email, and website in this browser for the next time I comment.

□ Notify me when new comments are added.

SUBMIT

□ I'm not a robot reCAPTCHA Privacy - Terms

Email

□ I agree to provide my email address to "AO Kaspersky Lab" to receive information about new posts on the site. I understand that I can withdraw this consent at any time via e-mail by clicking the "unsubscribe" link that I find at the bottom of any e-mail sent to me for the purposes mentioned above.

SUBSCRIBE