Hammertoss: What, Me Worry?

securityintelligence.com/hammertoss-what-me-worry/

September 28, 2015

Malware September 28, 2015

By David Strom 2 min read

Earlier this year, a Russia-based hacking group began distributing Hammertoss, a very nasty piece of malware that makes use of Twitter and Github to transfer its attack payloads and hide from view. Because it uses these common sites that are visited by millions, the notion is that its network traffic patterns are normally hard to detect since the traffic looks like ordinary end user queries of these services.

Opportunities for Malicious Acts

But hidden in these interactions are the directions for the malware to first download an image from Github, extract encrypted instructions and then finally upload a victimized PC's data to its servers. While each of these techniques isn't new, the combination shows that someone with a great deal of skill has taken the time to craft the code. For example, Hammertoss is able to:

- Retrieve legitimate commands from social media networks — again, looking like a normal user's interactions;
- Use compromised Web servers for command-and-control purposes;
- Update its code frequently to change its behavior and backdoor infection patterns;
- Automatically visit different Twitter handles daily on a scheduled basis; and
- Use a schedule to do all of these communications during the local workday so as not to appear suspicious.

How Hammertoss Works

Fusion explained how Hammertoss operates with Twitter, Github and other images.

"Each Hammertoss-created tweet is custom-tailored with a unique hashtag and a URL that links to a seemingly innocuous image," Charles Pulliam-Moore wrote on the site. "In reality, the image itself contains a small bit of encrypted data. The hashtag tells a computer where to look for the image and includes a matching bit of encrypted data that, when combined with the image, unleashes a new set of malware commands that can extract data from a compromised computer."

One security researcher has tracked the origins of Hammertoss to the APT29 group, which allegedly has nation-state ties. The group operates during the appropriate time zones and local Russian holidays, supporting this hypothesis.

What Should IT Teams Do?

What can IT departments do about Hammertoss, given this profile? First, they should employ a security product that can examine network traffic that it produces and look for unexpected behavior. While Hammertoss connects to random Twitter and Github accounts, it is using the information gleaned from these accounts in an automated and programmatic fashion.

Second, part of this analysis is also examining more carefully what kinds of data are leaving your network; if you don't have any way to do this, now is the time to start looking at protective tools that will allow for this kind of monitoring. Third, you should look at security products that examine file integrity and movement specifically. Finally, you should probably subscribe to several security news and intelligence feeds to keep up to date on the news about Hammertoss and other similar advanced threats.

Advanced Threats | Malware | Network Security | Security Intelligence

David Strom
Security Evangelist

David is an award-winning writer, speaker, editor, video blogger, and online communications professional who also advises numerous startup and well-establish...