The Wonder of Sirefef Plunder

msft-mmpc
0

20 May 2013 10:37 PM

Sirefef, also known as ZeroAccess, is a malware platform for receiving and running malware modules.

Two prominent modules generate revenue for the cyber criminals, by mining for bitcoins and perpetrating click-fraud.

Click-fraud is the deliberate misappropriation of ad revenue by generating online clicks that don't originate from a potential customer or the rightful publisher. Click-fraud is lucrative and a relatively easy way for cyber criminals to monetize their malware and/or launder ill-gotten revenues.

On February 12, 2013, Microsoft added its Sirefef signature set to the Microsoft Malicious Software Removal Tool (MSRT). Over a period of one month this signature set was installed 640 million times and roughly 500,000 machines were cleaned of Sirefef.

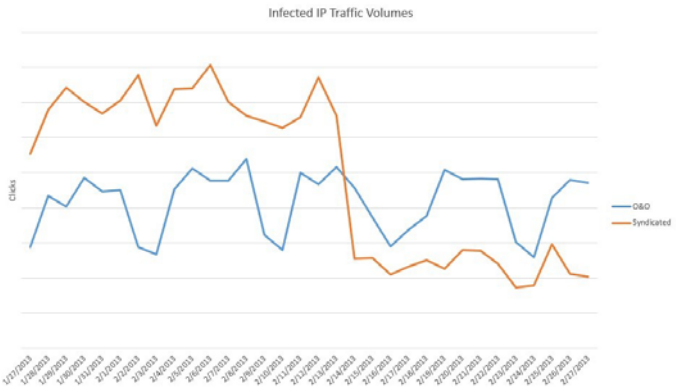

Figure 1: Sirefef infected IP traffic volumes.

Figure 1 illustrates a very small, yet instructive, slice of the Sirefef click-fraud picture. The blue line represents what is called the Owned and Operated (O&O) publishers in the Microsoft ad network; this includes sites like Bing.com and Yahoo.com.

The orange line represents traffic on the Microsoft extended publishing network. It is common for these publishers to have agreements with other publishers who may have agreements with other sources of traffic and so on. These types of obfuscated partnerships can lead to the introduction of low quality traffic to advertisers, and provide an opportunity for malware authors to monetize their software. This is an industry problem driven by the need for additional supply (visitors) in order to fulfill demand (advertisers' budgets).

The steep decline of the orange line on February 13, 2013 was caused by the MSRT cleaning of Sirefef. Prior to the 13th, these computers, running Sirefef click-fraud modules, had a level of traffic roughly three times greater than after they were cleaned.

The graph represents the traffic from 1874 unique computers generating ad-clicks on the Microsoft ad network where MSRT removed the Sirefef click-fraud module. We focused on these 1874 machines out of the 500,000 machines cleaned of Sirefef, to definitively show a causal relationship between Sirefef and clicks.

This was done by looking at a few Sirefef click-modules, as well as machines with advanced telemetry and machines that generated clicks on the Microsoft ad network. A less restrictive view of the data, looking at other ad networks for example, would describe a much larger problem.

Again the blue line represents those IPs clicking on Bing and Yahoo, while the orange represents clicks on the extended publisher network where there exists opportunities for click-fraud. Of course, there are many more infected

Each of these 1874 machines generated, on average, between $0.50 and $1.60, in what we call billable traffic, per day when they were active. It is unknown what percentage of this actually gets into the hands of cyber criminals and what percentage is taken by layers of syndicated publishers to effectively launder the click.

With half a million infected computers, active even a few days, there exists significant theft of ad revenue.

Microsoft is dedicated to protecting our advertising marketplace and we are dedicated to protecting our customers. We continually look for innovative ways to improve our ability to bring the highest quality traffic to the online commerce ecosystem and prevent abuse like Sirefef.

Sirefef victims are not only the users whose machine and computer experience is impacted by the running of this malware. The advertisers who are paying for clicks which are never generated by potential customers are also affected.

And this lost revenue is passed on to you, the customer. When you buy a product whose ad budget is being stolen, you fractionally bear this cost.

And that is a wonder of Sirefef plunder.

Tommy Blizard and Nikola Livic

MMPC

26