

## Top 5: The Largest Malware Delivery Networks

The Blue Coat 2011 Mid-Year Security Report described the powerful tools that make malware delivery networks successful: dynamic web links that enable cybercrime to change out payload servers and avoid detection. Last year, the malware web delivery infrastructure was hacking into popular and trusted domains where cybercriminals can display lures beyond the reach of reputation filters and web category blocking.

With an eye on acceptable-use policies, the lures often inhabit categories such as Online Storage and Software Downloads. Still, the categories that draw the highest percentage of malware-network entries are search engines (39.2 percent), email (6.9 percent), pornography (6.7 percent), and social networking (5.2 percent). The single most perilous activity for web users was searching for images or pirated media.

Analysis of these findings forced the conclusion reached in the report: single-layer defenses such as firewalls and anti-virus software are incompetent to deal with dynamic, constantly changing threats. The clear solution is an intelligent, real-time cloud-based web defense that is equally dynamic and effective.

On any given day, an average of 50 malware delivery networks will be in operation. Here are the largest:

### Top 5 Malware Delivery Networks by Number of Unique Host Names

#### 1. Shnakule

**Unique attack hosts: Average, 2001; Maximum, 4357**

By far the biggest and most successful of the malware delivery networks. During the first half of 2011, Shnakule was the most effective at luring users, drawing an average of 21,000 requests per day with a peak of 51,000. Shnakule is broad-based. Its malicious activities include drive-by downloads, fake anti-virus and codecs, fake Flash and Firefox updates, fake-warez, and botnet/command and controls. The primary malicious activity is fake anti-virus attacks, typically conducted through search engine poisoning. Shnakule has a finger in many pies: pornography, gambling, pharmaceuticals, link farming, and work-at-home scams.

Bear in mind that Shnakule contains many component networks. Ishabor, which is number 2 on this list, is a component of Shnakule, as are other malware delivery networks identified in the Mid-Year Security Report.

#### 2. Ishabor

**Unique attack hosts: Average, 766; Maximum, 1140**

Ishabor, exclusively devoted to distributing fake anti-virus scareware, launched in late April 2011 and quickly ramped up traffic. It operated independently for a week; then Blue Coat WebPulse™ collaborative defense, using input from a community of 75 million users, determined it was sharing malware delivery infrastructure with Shnakule. Given the speed at which Ishabor was able to drive traffic to its malware servers, it may be that it was part of Shnakule from the start – and that what

WebPulse observed was the deployment of a new piece of infrastructure that was set up and tested as a stand-alone piece before being integrated into the larger parent network.

#### 3. Cinbric

**Unique attack hosts: Average, 505; Maximum, 1602**

Malware delivery networks may find diversity essential for long-term survivability, but Cinbric demonstrates the impact of doing one thing and doing it well. This network relies primarily on spam to drive traffic to porn-themed ransomware. Essentially, they lure users to their malware servers with promises of exclusive webcam access if they download and install their software. While this network has not seen much growth this year, it continues to put up noteworthy numbers, both in unique host names and in attack traffic.

#### 4. Naargo

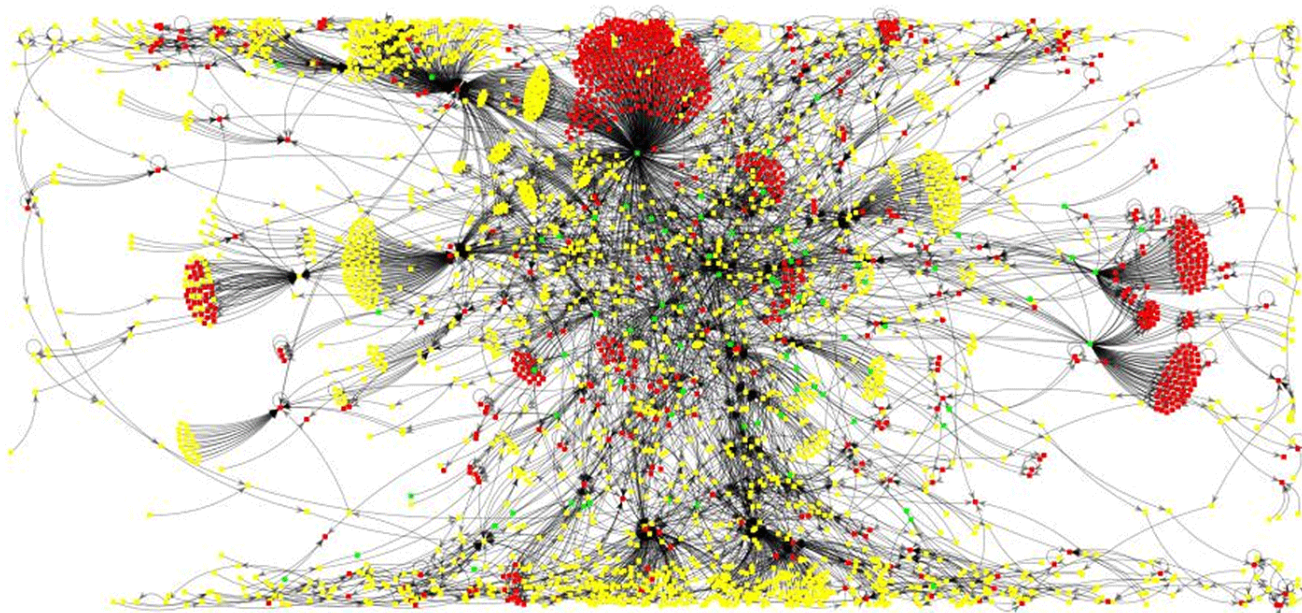
**Unique attack hosts: Average, 199; Maximum, 299**

While this network is not categorically devoted to malware delivery, it exhibits many shady characteristics and therefore merits continued tracking and investigation. Like Cinbric, it focuses primarily on using spam and search-engine poisoning to drive traffic to porn sites.

#### 5. Vidzeban

**Unique attack hosts: Average, 156; Maximum, 347**

A fake-warez network with a significant Russian-language presence. As with other fake-warez networks, very little of its traffic is driven by spam. Users that visit this site are looking for software to download and install, so search-engine poisoning is its major source of traffic. Typically, these users know they are looking in the shady, less-reputable areas of the Internet.



A graphical representation of – Shnakule – Malware Delivery Network (Blue Coat Security Labs, 2011)

## How Blue Coat web security solutions powered by WebPulse can defend your network against malware delivery.

When Snakule mounted a malware delivery offensive on June 29, 2011, Blue Coat's WebPulse collaborative defense had already been identifying and blocking its payload servers for five days. The global WebPulse user community, 75 million strong, was contributing unrecognized sites and pages into the cloud as input to the WebPulse analysis and ratings service. The system, processing over 500 million web requests per day, used 16 automated analysis layers to identify and block Shnakule payload servers.

To the community of Blue Coat web security users, The WebPulse architecture delivers:

- > The industry's most accurate defense against malware delivery
- > Over 1.2 billion dynamic ratings in an average week
- > Real-time ratings on demand

WebPulse deals with a primary malware delivery weapon – dynamic links – with dynamic link analysis. WebPulse not only looks at the entry point but also tracks the request through the shifting links and relays of the malware delivery network.

Blue Coat has developed over 300 real-time rating libraries, which work with the many threat detection modules within WebPulse to deliver the most accurate real-time threat protection in the industry.

### It also gives you:

**Granular categories per URL:** WebPulse uses more than 80 categories with up to four ratings per web request, such as IM Chat within Social Networking. This granularity drives Blue Coat's defense systems and enables accurate web control at customer sites.

**Multiple languages:** WebPulse provides ratings in 55 languages, 19 of them in real time.

**Worldwide professional backup:** Blue Coat's automated systems are backed up and trained by professionals in Blue Coat Security labs around the world. These security experts provide in-depth analysis of suspicious web behavior and deep insight into malware payloads and the networks that deliver them.

For all these reasons, Blue Coat's web security solutions, powered by the WebPulse collaborative defense, are positioned to protect your organization's networks against the most sophisticated attacks that malware networks can deliver.