Blue Coat

2012 Web Security Report - *Executive Summary*

Exposing Malnet Strategies and Best Practices for Threat Protection

State of the Threat Landscape

In 2011, malnets (malware networks) emerged as the next evolution in the threat landscape. These infrastructures last beyond any one attack, allowing cybercriminals to quickly adapt to new vulnerabilities and repeatedly launch malware attacks. By exploiting popular places on the Internet, such as search engines, social networking and email, malnets have become very adept at infecting many users with little added investment.

Driven in part by malnet activity, malicious sites increased 240 percent in 2011. The increase can be attributed to a combination of factors. Chiefly, cybercriminals are more quickly rotating through domain names. As malicious software kits have become easier to buy, customize and deploy, there are also more people distributing malware.

The vast majority of attacks target users on their desktops and laptops. However, the explosion of mobile devices gives cybercriminals a new platform. While attacks on mobile devices are limited today, the growing usage will make them a high-value target moving forward. And cybercriminals are ready. Today's existing malnet infrastructures will be the same ones used to deliver tomorrow's attacks on mobile devices.

Malnet infrastructures enable cybercriminals to launch dynamic attacks that are often not detected by traditional anti-virus vendors for days or months. In one case in early February 2011, a malware payload changed locations more than 1,500 times in a single day. These types of attacks are far too dynamic even for defenses that inspect content in real time to keep pace. The rise of malnets demands a new type of security to protect against corporate data loss, financial or identity theft, and other costly consequences. Businesses need a proactive defense that can stop attacks before they launch by identifying and blocking the source. The key to this type of defense is to understand malnets, their structure, their targets and their strategy.

Malware Networks

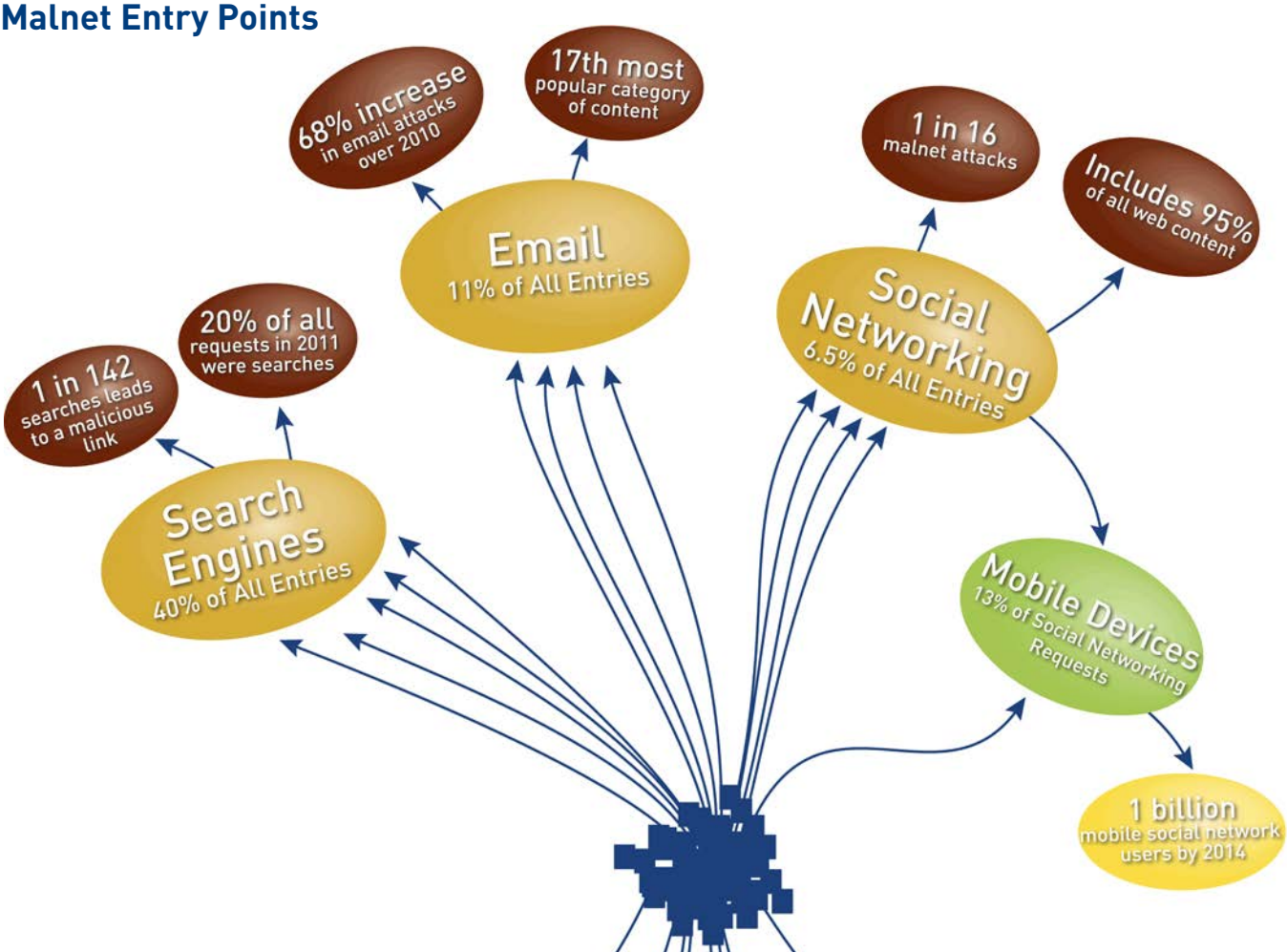
What You Need to Know to Protect Your Organization

A malware network (malnet) gathers users, typically when they are visiting trusted sites, and routes them to malware, via relay, exploit and payload servers that continually shift to new domains and locations.

5000 Threats
Confront the average business every month

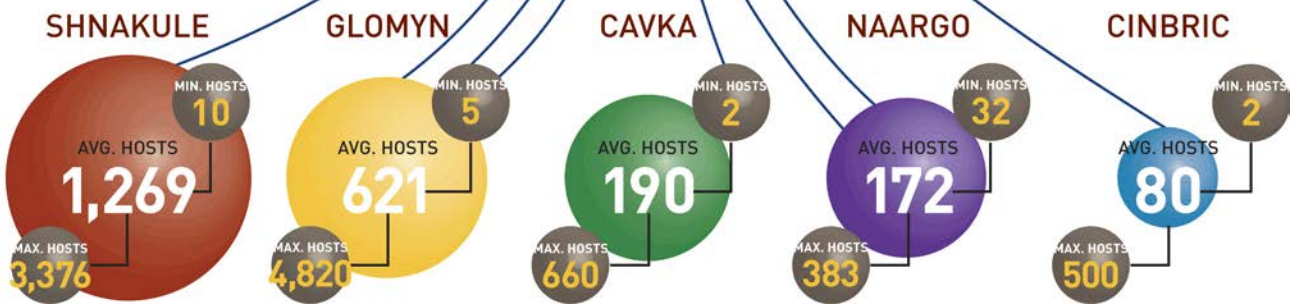
240%
Increase in malicious sites over 2010

Malnet Entry Points

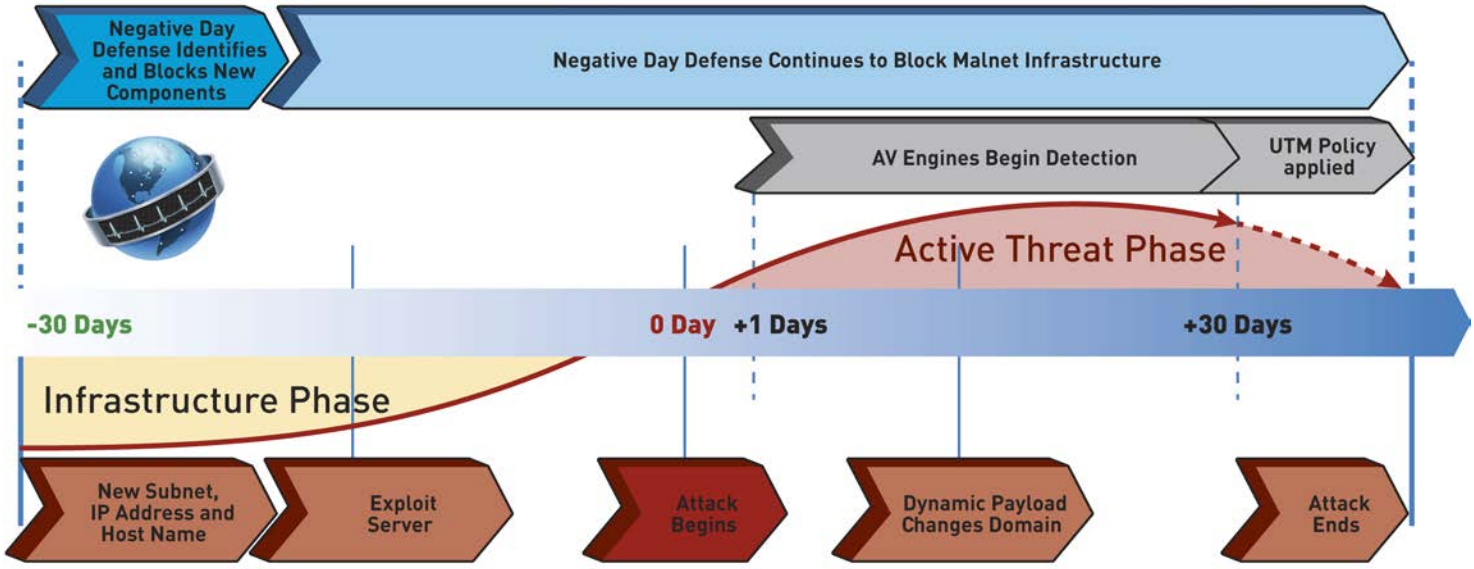


Top 5 Malware Networks

Blue Coat Labs is tracking over 500 malnets like these



A New Malnet Defense



Key Takeaways for Your Organization

- **Real-time analysis** of search results is required to identify malicious links
- **Granular application and operation controls** are essential to effectively manage and mitigate risks of social networking
- **Layered defenses** are critical to protect against malicious executables within webmail, which remains a valuable threat vector despite a decline in popularity of email
- **Negative day defenses** are required to stop future attacks by blocking them at their source

About Blue Coat Web Security

The insights reviewed in this report are derived from Blue Coat Security Labs' analysis of data from the WebPulse collaborative defense. Blue Coat WebPulse™ is a cloud-based, real-time analysis and ratings service that unites users in a common defense. Delivered via Blue Coat ProxySG appliances and the Blue Coat Cloud Service, WebPulse receives one billion web requests from 75 million globally diverse users. With comprehensive visibility into the web ecosystem, WebPulse can automatically identify abnormal traffic and correlate it to known malware networks (malnets) to block attacks before they are launched. Utilizing these techniques and other advanced analysis tools, WebPulse blocks 3.3 million threats per day.

Refer to the Complete **Web Security Report** for Further Details

Blue Coat