CARRIER INSIGHTS REPORT

Executive Summary
Executive Summary / Akamai, the world’s largest and most trusted cloud delivery platform, uses its globally distributed Akamai Intelligent Platform™ to process trillions of Internet transactions each day. This allows us to gather massive amounts of data on metrics related to broadband connectivity, cloud security, and media delivery. The State of the Internet report was created to enable businesses and governments to make better strategic decisions by leveraging this data and the insights it offers. Akamai publishes State of the Internet reports based on this data, with a focus on broadband connectivity and cloud security.

The State of the Internet / Security: Carrier Insights, Spring 2018 report focuses on DNS data from Akamai’s global infrastructure and represents the research of a diverse set of teams from around the globe.

Business Implications / More than ever, data sharing and collaboration are vitally important to the health of individual organizations and the Internet as a whole. It’s not simply that businesses need to share data with other corporations — they need to cooperate to make the data meaningful. Sharing data internally and correlating the data internally is a challenge for many organizations; sharing it between enterprises complicates the problem immeasurably.

This report focuses on how information sharing between organizations and internally within an organization lead to greater intelligence and a more robust Internet. This report’s guest author — Megan Stifel, CEO, Silicon Harbor Consultants, former Director for International Cyber Policy on the National Security Council — highlights how important data sharing and trust are to securing our systems.

Learning to combine data from various sources and glean intelligence from its correlation is one of the most vital responsibilities of security teams. This report represents an evolution of Akamai’s reporting and a concentrated effort to bring data and intelligence from throughout the organization to create a deeper picture of the threats we face. We would challenge organizations to explore their own environment to better understand the data streams and intelligence that may not be used to their fullest today.

Editor’s Overview / Akamai’s Security Research team analyzed over 14 trillion DNS queries from the past six months in order to bring our readers research about the malware, botnets, and other threats we see attacking businesses and individuals daily. The Loapi botnet family highlights an evolution of malware to be more flexible in nature. At the same time, we see market forces driven by cryptocurrencies are affecting both businesses and malware authors in similar ways. Combining our DNS data with wider research within Akamai, as well as with other organizations, allows us to look deeper into the Mirai botnet and how it operates — a continuing effort for many organizations.

Sometimes these threats feel like they’re static, never changing, never growing. Then there are the times that our adversaries seem to make huge leaps in their capabilities, such as when the Mirai botnet was created. But these are both mostly just illusions created by the final effects of slow, gradual changes constantly happening in the landscape. It’s only by understanding the seemingly small changes, like Loapi’s change to a modular structure, that we have a chance to predict the bigger changes, such as the rapid adoption of the memcached vulnerability for DDoS. Evolution only looks sudden if you can’t see what’s happening behind the curtain when you aren’t looking.
No organization, not even one with a planetary scale network like Akamai, can see everything and make sense of it. Only when we combine our intelligence can we see the small changes that lead to evolutionary leaps.

**Threat Tracker /** Threats don’t have to be new to be costly. During the recent reporting period, two spikes in the malicious activity were detected. The first of these was from October 3 to November 1, driven by the Dorkbot botnet’s command and control domain traffic. The botnet is being updated to take advantage of new Domain Generation Algorithm work from malware authors.

The second spike in activity wasn’t driven by a specific botnet. Instead, the increase in domain lookups was caused by the exploitation of the Web Proxy Auto-Discovery (WPAD) protocol. When exposed to the Internet, WPAD allows an attacker to push a proxy configuration file to exposed systems and open them to Man-in-the-Middle attacks.

It’s important to remember that not all threats are global in nature. We tracked five threats that were very localized. Several of these bots targeted specific countries, maintaining an infrastructure specific to the region, while others relied upon cloud services to thrive.

**Emerging Trends /** Using malware to steal financial data is so 15 minutes ago ... at least that’s what some malware authors seem to think. The Terdot malware, a descendant of the Zeus family, has branched out to include a collection of social media credentials as part of its campaign. The malware acts as a proxy, which enables it to direct the user to any site the author wants, which opens up a number of interesting options.

The Loapi botnet takes a different approach. Designed to run on mobile devices, this malware was originally used to fuel DDoS attacks. But its creators have decided that being a one-trick pony wasn’t good enough, and pushed a modular version. This means that the botnet can be easily modified when a new vulnerability is found or a new capability is needed.

To the surprise of no one, cryptocurrencies are the new hotness in malware. With Bitcoin nearly hitting $20,000 last year, malware authors and legitimate sites alike are starting to explore ways to mine the coins on your servers. While we know it’s wrong for someone to use your computer for mining by installing malware, the morality of a site including JavaScript that taps your CPU cycles to run is still a gray area.

**Collaboration in Action /** It’s not often a botnet like Mirai comes along. But this botnet is important because it highlighted some of the best of what security can be. Multiple organizations communicated behind the scenes to collect, understand, and disseminate as much information as possible about the botnet. Many of these organizations continue to cross-pollinate and share data.

Building upon research in the Q4 2017 State of the Internet report leads us to a deeper look at credential abuse and the types of tools that are being used in this space. Looking at the DNS requests and domain resolutions for botnets gives us a different view into the activities of this type of threat.

To download the full report visit [akamai.com/stateoftheinternet-security](akamai.com/stateoftheinternet-security).