Infoblox
CONTROL YOUR NETWORK

QUARTERLY REPORT 2015

INFOBLOX DNS THREAT INDEX

POWERED BY IID

EXPLOIT KITS UP 75 PERCENT

The Infoblox DNS Threat Index, powered by IID, stood at 122 in the third quarter of 2015, with exploit kits up 75 percent from the third quarter of 2014.

EXECUTIVE SUMMARY

- The Infoblox DNS Threat Index rose 18.5 percent compared to Q3 2014.
- Exploit kits, a component of the index, rose 75 percent from Q3 2014.
- Angler is the biggest threat among exploit kits.
- Matsnu, a type of domain generation algorithm (DGA) based malware, was a significant contributor to the command-and-control (C&C) category.
- Because exploit kits are best at taking advantage of zero-day vulnerabilities, they can be a leading vehicle for dropping malware that attempts data exfiltration.

INTRODUCTION

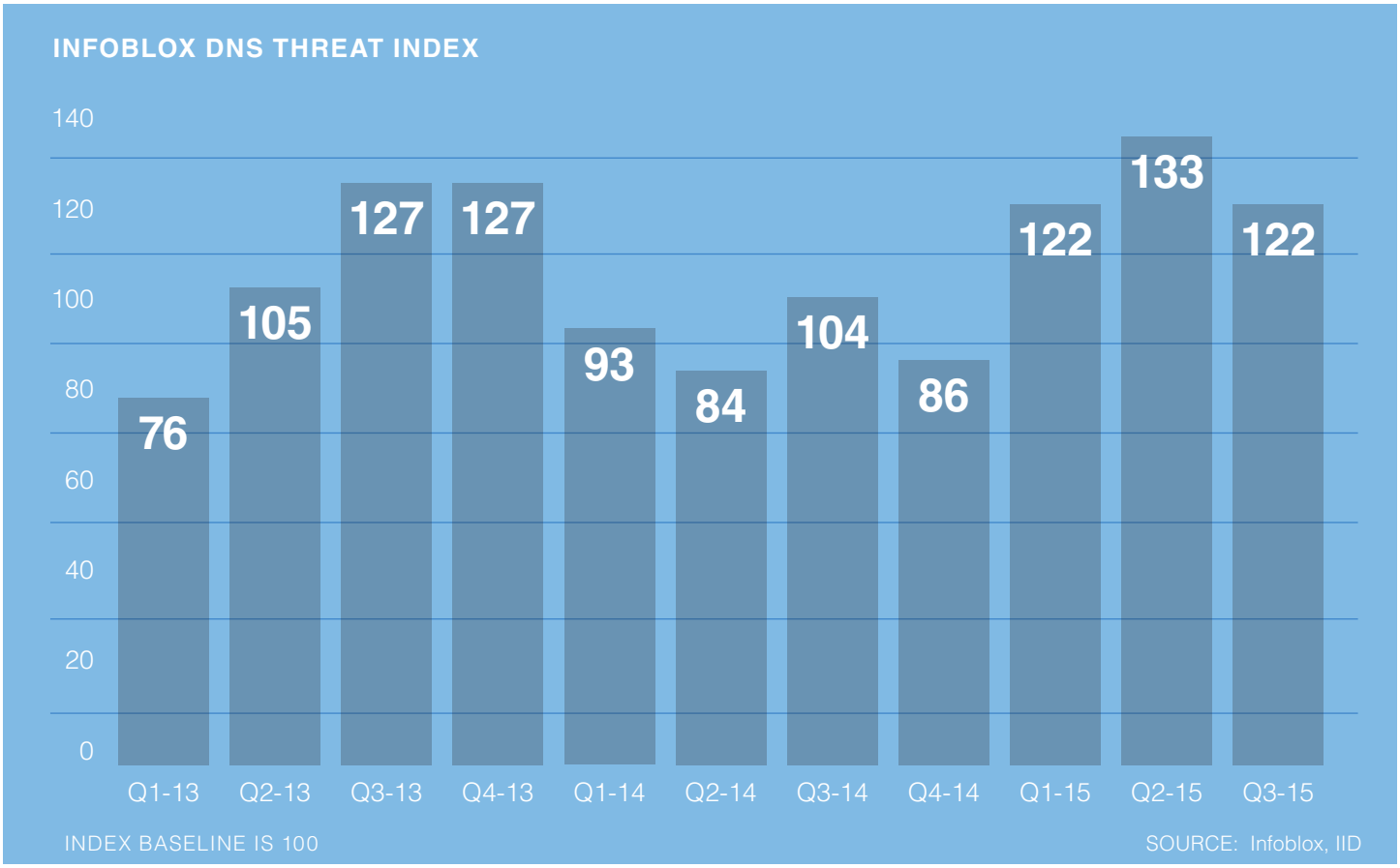
The Infoblox DNS Threat Index is an indicator of malicious activity worldwide that exploits the Domain Name System (DNS). Cybercriminals create new domains as a foundation for unleashing a variety of threats ranging from simple malware to exploit kits, phishing, distributed denial of service (DDoS) attacks, and data exfiltration. The index tracks creation of malicious domains tied to 67 separate threat categories globally, using data from a range of sources including government agencies, Internet service providers, enterprise network operators, and open sources. For details on how the index is calculated, see the Methodology section at the end of this report.

Q3 2015 FINDINGS

Exploit kits continue as a significant component of the Index this year, and the third quarter saw an increase of 75 percent in creation of DNS infrastructure for exploit kits as compared to the same quarter of 2014. In Q3, new incidents of the Angler, Magnitude, Neutrino, and Nuclear malware families were the biggest drivers of new exploit kit activity. In addition, the DGA-based malware Matsnu was a significant contributor to the C&C malware category of the Index.

Although the Index for the third quarter was slightly down from the record-high second quarter of 133, it continues to be well above average levels in the last two years. Cybercriminals usually go through a cycle of “planting” and “harvesting” when it comes to malicious infrastructure. During the planting phase, there is a significant rise in the number of malicious domains created for malware and

ANGLER, MAGNITUDE, NEUTRINO, AND NUCLEAR ARE THE BIGGEST DRIVERS OF NEW EXPLOIT KIT ACTIVITY



exploit kits, leading to a larger Infoblox DNS Threat Index number. Once this phase ends, the attackers begin to harvest the extensive infrastructure they have built to launch attacks, steal data, and generally cause harm to their victims. In this phase, the threat index number may be lower.

In Q3, we seem to be in the early stages of the harvesting cycle where cybercriminals are utilizing the infrastructure they built up previously to launch attacks. A case in point is the recent Angler exploit kit attack on a high-profile national daily newspaper in Britain that potentially exposed millions of its readers to malvertising.

EXPLOIT KITS AND DNS SECURITY

Exploit kits are toolkits for hire that deliver malware via drive-by download. The payload will vary depending on what the current user of the exploit kit specifies; past payloads have included all kinds of malware, such as banking malware, advertising click-fraud malware, and ransomware.

Exploit kits typically take advantage of security holes or vulnerabilities in operating systems, browsers, and popular software such as Adobe Flash and Java.

The main purpose of an exploit kit is to deliver some sort of malware onto a computer or mobile device. Users can be exposed to exploit kits either via spam or malicious ads. When a user is lured to a malicious or compromised website, the exploit kit is delivered and a malicious payload is subsequently downloaded and executed on the victim's computer. While the functionality of the various exploit kits is largely identical, the main distinctions among the exploit kits are the vulnerabilities used to infect visitors and the tricks used to defeat antivirus defenses.

Currently, exploit kits are mostly targeting computers, but mobile devices can also be compromised. Mobile malware is becoming hugely popular with cybercriminals because of the vast number of people using mobile devices for tasks

such as email, web surfing, banking, and social media. Also, users typically take fewer security precautions with mobile devices, making them easier to invade. Attackers are expected to gradually shift to delivery of mobile malware through mobile browser web pages, essentially the same approach that drives most infections on conventional computers.

When an exploit kit succeeds in delivering its payload onto a victim's computer or mobile device, that payload is now behind the company's or service provider's firewalls. The malware can now spread to other devices and communicate back to its C&C server through the Internet to download further malicious software or exfiltrate data. More often than not, communication between the infected device and C&C server requires DNS.

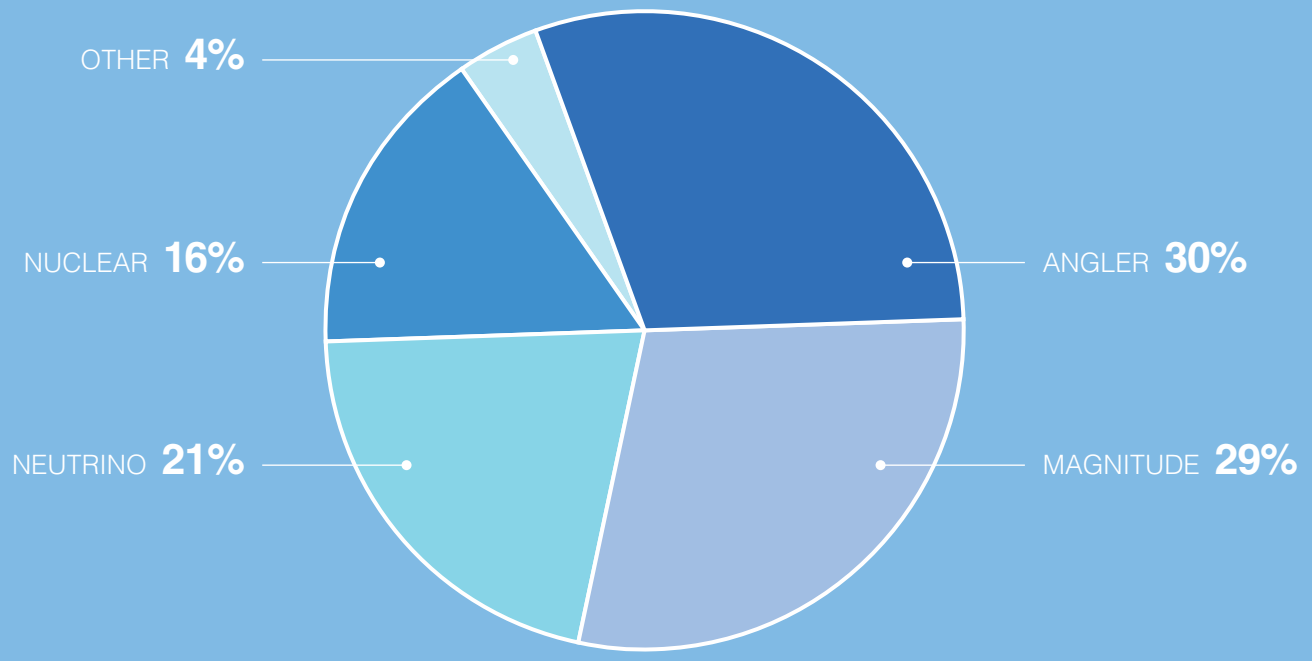
ANGLER

The Angler exploit kit is one of the most sophisticated currently used by cybercriminals and leads exploit kit DNS activity for Q3. Angler is notorious for pioneering the "domain shadowing" technique used to defeat reputation-based blocking strategies, and for infiltrating malicious URLs into legitimate ad networks, infecting visitors to websites that are generally considered safe.

Angler exploit kits are often quickly updated with the latest zero-day vulnerabilities in popular software and use sophisticated obfuscation techniques, making it difficult for traditional antivirus technologies to detect. The constant evolution of Angler exploit kits means organizations need to invest in protection technologies that not only address one stage of the exploit, but can detect and disrupt activity across the entire kill chain.

Recently, a major British newspaper, which has hundreds of millions of monthly visits to its website, was hit with the Angler exploit kit. The attack resulted in malicious ads being displayed to its readers over the period of four to five days. This could have exposed many of the daily visitors to infection from clicking on the malicious ads.

NEWLY OBSERVED EXPLOIT KIT ACTIVITY Q3 2015



SOURCE: Infoblox, IID

Cisco's Talos security group recently reported that it disrupted a major part of the Angler network infrastructure, including the servers of a targeted service provider, as reported in this blog. The operation was estimated to be generating US$30 million annually from ransomware and could very well exceed US$60 million if the full scope of the activity is taken into account. Considering the amount of money involved, it seems likely the hackers will rebuild and resume operations.

Recent cyberthreat research has found that Cryptowall 3.0 ransomware operators have been using the Angler platform to launch attacks and have been successful in raking in about US$325 million in ransom, mostly through Bitcoin payments.

MAGNITUDE

Closely following on the heels of Angler in the Q3 rankings is the Magnitude exploit kit. Recent variations of Magnitude targeted vulnerabilities in Adobe's Flash Player and were used to deliver Cryptowall 3.0 ransomware. Countries most affected by the Magnitude threat include the United States, Canada, and the United Kingdom.

Unlike other exploit kits, Magnitude uses a unique traffic-sharing model. Instead of paying rent to administrators of the exploit kit, cybercriminals trade anywhere from 5 to 20 percent of the traffic related to their campaigns. The administrators then embark on their own malicious activities using their share of traffic, such as dropping in ransomware. Magnitude gives its customers the option to upload their own executable payloads, which could be attractive to many cybercriminals.

NEUTRINO

The Neutrino exploit kit takes advantage of vulnerabilities in older versions of Java and is used to download ransomware. Neutrino exploit kits are advertised as easy to use, with extensive functionality for monitoring and management of stolen information. Typically, Neutrino kits are offered by cybercriminals for as little as US$40 a day.

NUCLEAR

The Nuclear exploit kit first appeared in 2009 and has constantly evolved since then. It exploits a wide range of vulnerabilities, including those in Adobe Flash, Adobe PDF, and Microsoft Internet Explorer. Nuclear is also used to drop in advanced payloads such as ransomware, and is typically used in high-volume compromises. The Nuclear kit's creators are constantly improving its capabilities to avoid detection and increase infection rates.

MATSNU IS THE MOST SIGNIFICANT THREAT IN C&C CATEGORY

MATSNU DGA-BASED MALWARE SPIKES UP

Q3 2015 saw Matsnu become a significant contributor to the C&C malware category in the Index.

Matsnu (also known as Androm) is malware that acts as a backdoor in infected systems and can be used to download and install additional malicious software for purposes including ransomware and data theft. The malware then uses DGA to communicate with C&C servers. With DGA, a domain is dynamically generated from a list of words following a certain format (noun-verb-noun-verb), and will be contacted by the infected device for a short period of time (such as 72 hours), after which a new C&C domain will be generated. This method makes blocking difficult because the domains are used only for a short amount of time. The distribution vector for Matsnu is usually an email attachment.

PHISHING CONTINUES TO BE A DRIVER

Phishing continues as a significant component of the Index for the second quarter in a row, with more than double the average phishing activity over the previous nine quarters. Although Phishing has been around for a long time, criminals still use the technique because it works, and because it's often easier to trick humans into giving up sensitive information than to overcome increasingly sophisticated cybersecurity systems. This makes end-user education and risk management processes more important than ever to ensure protection of data and applications. Also, as mentioned above, enterprise and service provider organizations should deploy DNS-based technology that can leverage current threat intelligence to disrupt communications to and from phishing sites.

THE ENDLESS CYCLE OF PLANTING AND HARVESTING

Attackers are waging a constant cat-and-mouse game with threat researchers. Cybercriminals rapidly create DNS infrastructure and set up domains as a base for launching attacks. During this planting phase, there is a significant rise in the number of malicious domains associated with malware and exploit kits, leading to a larger Infoblox DNS Threat Index number.

Once this phase ends, the attackers begin to harvest the extensive infrastructure they have built to launch attacks, steal data, and generally cause harm to their victims. In this phase, the threat index number may be lower. However, this doesn't mean malicious activity has subsided.

The Infoblox DNS Threat Index shows this endless cycle of planting and harvesting when looking across the twelve quarters to date. If the index is lower in a given quarter, this may correspond with a period in which the malicious agents are harvesting the infrastructure they have already created and are not setting up new bad domains at the same pace. If the index is higher in a quarter, this could indicate that the attackers are in a planting phase, establishing domains and other infrastructure to execute their plans.

SUMMARY

The Infoblox DNS Threat Index in 2015 continues to remain well above the average for the previous two years, indicating that cybercriminals are continuing to expand their infrastructures. Exploit kits and phishing remain significant components of the index because these techniques have been successful for malicious actors.

Infoblox and IID will continue to monitor new malicious domain-creation activity to help their customers better prepare to handle threats to their infrastructure and data.

INDEX METHODOLOGY

The Infoblox DNS Threat Index, powered by IID, measures the level of malicious domain creation within the quarter. The baseline for the index is 100, which is the average for creation of DNS-based threat infrastructure during the eight quarters of 2013 and 2014.

To create the index, IID examines domains worldwide associated with malicious activities from the proprietary methods and capabilities the company utilizes on a daily basis. Malicious domain indicators come from a broad network of partner organizations, Internet infrastructure players and law enforcement agencies. The result is not a comprehensive list of bad domains, but rather a representative sampling.

Newly observed malicious domains are categorized by threat type and the 67 most active threat types are factored into calculations for the index. As new threat classifications emerge and become more active, and as some become less active or disappear, the categories are adjusted to reflect the mix of actual threats in use.

Because the index can be artificially inflated or distorted by the activities of DGAs and sub-domain resellers, these are removed from the calculations. There is also a check for any variation due to harvesting anomalies. If certain sources report a sudden spike or dip in the number of threat indicators, the cause is investigated. If the change is due to the way the data is gathered, rather than to a change in real number of malicious domains being created, statistical smoothing is applied to better reflect reality.

Infoblox
CONTROL YOUR NETWORK

Infoblox delivers critical network services that protect Domain Name System (DNS) infrastructure, automate cloud deployments, and increase the reliability of enterprise and service provider networks around the world. As the industry leader in DNS, DHCP, and IP address management, the category known as DDI, Infoblox reduces the risk and complexity of networking. More information on the Infoblox DNS Threat Index, powered by IID, is available at www.infoblox.com/dns-threat-index.

IID

IID is a cybersecurity company. Its flagship product, ActiveTrust, adds clarity to cyberthreat intelligence by distilling threat data from thousands of trusted sources, and fusing it into actionable intelligence delivered to security professionals and automated infrastructure. Fortune 500 companies and U.S. government agencies leverage IID to detect and mitigate threats, making ActiveTrust one of the world's largest commercial cyberthreat data exchanges. For more, go to www.internetidentity.com.