Infoblox
CONTROL YOUR NETWORK

QUARTERLY REPORT 2015

INFOBLOX DNS THREAT INDEX

POWERED BY IID

DNS THREATS UP 58 PERCENT

The Infoblox DNS Threat Index, powered by IID, reached a record high of 133 in the second quarter of 2015, up 58 percent from 84 in the second quarter of 2014.

OVERVIEW

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 related 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.

Q2 2015 FINDINGS

While the first quarter of 2015 saw a surge of malicious domain creation driven by the Angler, Neutrino, and Nuclear malware families, the second quarter's record number was driven by a significant increase in phishing activity. Exploit kit activity was down from the previous quarter, but was still a significant threat and was higher than four of the previous five quarters.

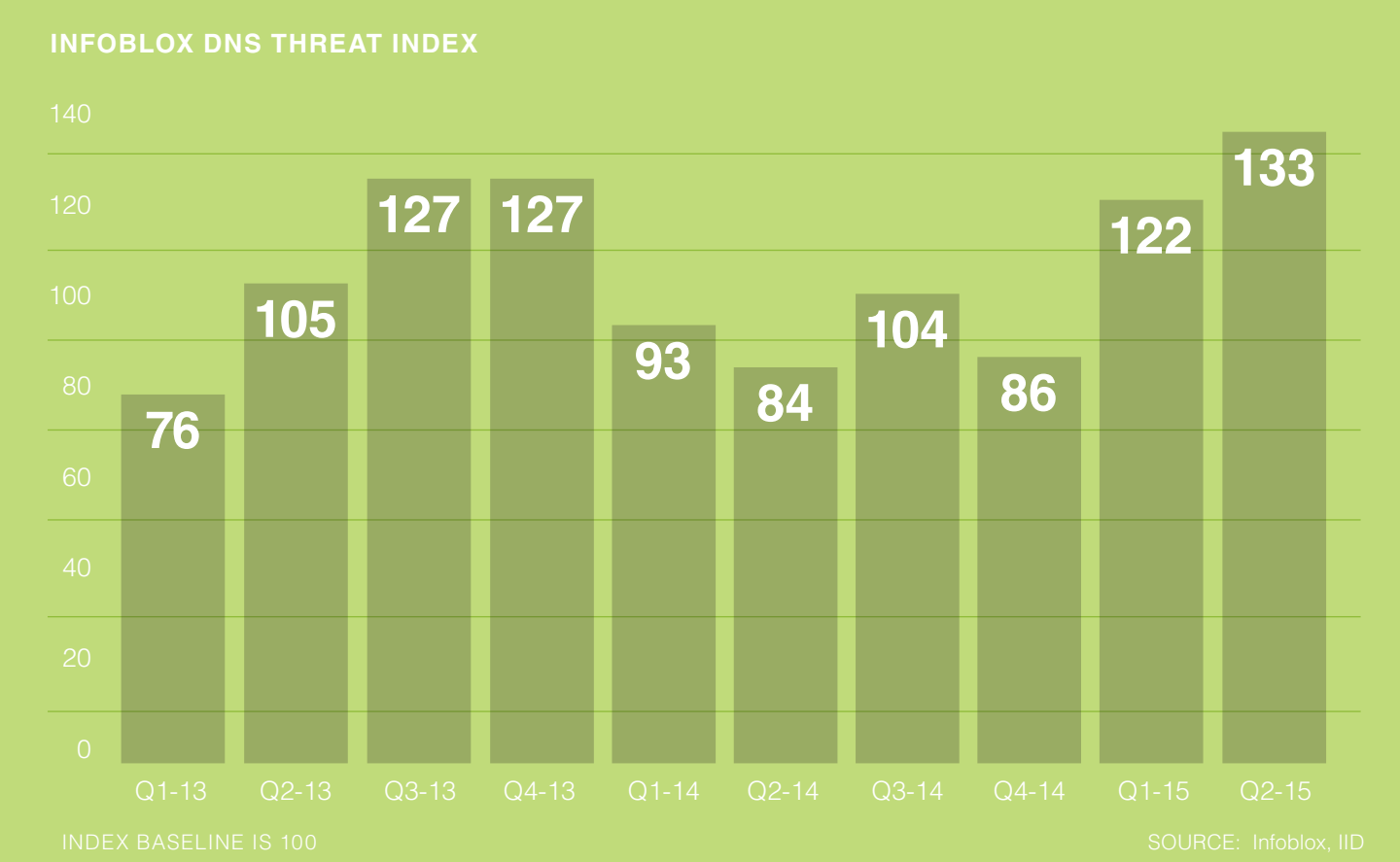
These types of malware often use DNS as a communication path for command and control as well as exfiltrating sensitive data. Knowing the threat level of DNS-based malware can help an organization to prepare by prioritizing investments between perimeter protection and other technologies that provide visibility into infections, protection, and post-breach response.

PHISHING

Phishing attacks are launched through emails containing domain names that are deliberately crafted to look like those of well-known sites. The goal is to lure unsuspecting users into clicking on the misleading links, sending them to web sites that in some cases are indistinguishable from the real ones. When users enter their authentication credentials, credit card numbers, or account information, the details are captured and used later to steal either money or proprietary data.

Phishing has been around for a long time, and the most recent index numbers show attackers are using it enthusiastically. Criminals stick with phishing because it works, and because it's often easier to trick humans into giving up sensitive information than to overcome increasingly sophisticated cybersecurity systems. Teaching internal users to be diligent and aware of the links they are clicking on is one level of protection. But with such important information at risk once exploited, organizations should also deploy technology that leverages current threat data to block traffic to and from these malicious sites.

PHISHING WAS THE BIGGEST GAINER IN Q2, UP 74%



EXPLOIT KITS

Exploit kits are collections of malicious software that take advantage of security holes in operating systems and popular applications such as web browsers. When a user unintentionally visits a malicious or compromised website, the exploit kit is delivered and a malicious payload is subsequently downloaded and executed on the victim's computer. Infrastructure for exploit kits accounted for 41 percent of malicious domain creation in the second quarter of 2015. Exploit kits have ranged from less than 20 percent to more than 70 percent of the index, and this quarter's volume was roughly the average across the previous 11 quarters. Although far from being the only set of threats within the index, changes in the number of observed new exploit-related domains is highly correlated with a change in the overall index.

THE ENDLESS CYCLE OF PLANTING AND HARVESTING

Attackers and malicious agents are waging a constant cat-and-mouse game with threat researchers. Malicious actors rapidly create 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, that doesn't mean that 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 has risen consistently for the last three quarters. This could indicate cybercriminals are expanding the infrastructure to leverage in targeted attacks for spreading malware and/or exfiltrating data. DNS is critical network infrastructure that can be used as a detection and enforcement point to disrupt communications to these malicious domains. Infoblox and IID will continue to monitor new malicious domain creation activity to help their customers better prepare to handle these threats.

INDEX METHODOLOGY

The Infoblox DNS Threat Index, powered by IID, is intended to reflect the level of new malicious domain creation within the quarter. The baseline for the index is 100, which is the average for threat activity 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 IID utilizes on a daily basis. Malicious domain indicators from a broad network of partner organizations, Internet infrastructure players and law enforcement agencies are added. This is not a comprehensive list of bad domains, but rather a representative sampling.

Domains that have been observed as malicious for the first time during that quarter are factored into the index. Domains that are still active, but were first observed in previous quarters, are factored out.

Next, the data is categorized by threat type. 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. These threats include distribution and command-and-control for a wide variety of malware, phishing, pharmaceutical scams and malvertising.

Because the index can be artificially inflated or distorted by the activities of domain generating algorithms (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 the reality.

THIS ENDLESS CYCLE OF PLANTING AND HARVESTING CAUSES THE INDEX TO EBB AND FLOW

Infoblox
CONTROL YOUR NETWORK

Infoblox delivers network control solutions, the fundamental technology that connects end users, devices, and networks. These solutions enable more than 8,100 enterprises and service providers to transform, secure, and scale complex networks. Infoblox helps take the burden of complex network control out of human hands, reduce costs, and increase security, accuracy, and uptime. Infoblox (www.infoblox.com) is headquartered in Santa Clara, California, and has operations in over 25 countries. 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.