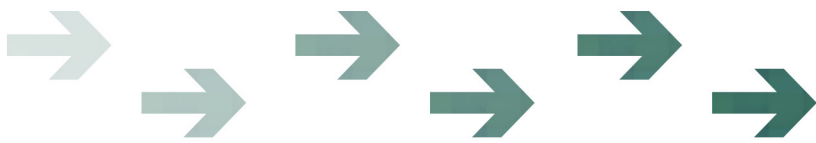




CYBER
SECURITY

2014 Report

2015 Predictions



Copyright

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of Labris Networks.

Disclaimer

Neither the author nor the publisher makes any representation or warranty of any kind with regard to the information contained in this book. No liability shall be accepted for any actions caused, or alleged to have been caused, directly or indirectly from using the information contained in this book.

About Labris Networks Inc.

Labris Networks Inc. has been an R&D-focused and rapidly-growing provider of network security solutions since 2002 through its globally proven products. Labris ensures ultimate network security through its extensive product line, including firewall/VPN, web security, E-mail security, lawful interception and availability protection solutions on Labris UTM, Labris LOG, and Harpp DDoS Mitigator appliances. Next-generation solutions are developed to detect and identify all kinds of real-time threats, our applications provide a smart shield against intrusions, viruses, spam, malware, and availability attacks.

Labris products protect networks of all sizes with various topologies and deployment scenarios. Through Labris FLEX firmware options, customers have the privilege of getting the security software they need as well as extra modules such as wireless guest authentication, detailed internet reporting, lawful interception, and logging. Having a customer-focused, future-oriented, and flexible approach, Labris also offers its state-of-the-art security software as a cloud service.

Having operations in a rapidly growing global network of more than 20 countries, Labris products protect enterprises, brands, government entities, service providers, and mission-critical infrastructures.

Labris with its worldwide partners is committed to the highest levels of customer satisfaction and loyalty, providing the best after-sales support through the multilingual Global Support Center. Being a rapidly growing global player, Labris offers its clients top-level security at optimal cost. Labris, headquartered in Ankara, Turkey, has offices that serve Europe, Middle East, North Africa, Caucasus, and Southeast Asia.

2014 Security Threat Landscape

Malware and Ransomware Year

Several cyber espionage campaigns ran in 2014, and these campaigns included malware aimed at money theft, ransom, and cyber espionage.

Espionage malware: After learning methods on Duqu and Stuxnet, the working steps of Regin malware have been disclosed. Several antivirus vendors have published reports on the working principles of Regin. The malware dated back to 2008 or was maybe older. Careto (The Mask) malware was one of the latest espionage malware discovered in 2014, and its target lists included diplomatic and governmental organizations of specific North African countries.

Ransomware malware: 2014 was a year of high propagation of CryptoLocker ransomware in some geographical regions, the United States being in first place. Early versions of CryptoLocker had problems with encryption, and there were methods for opening files encrypted by these versions. Afterward, these vulnerabilities were fixed. Data encrypted by CryptoLocker are not currently reversible and the ransom campaign is more powerful.

Distribution methods used for that type of malware include distribution from command and control centers to bots planned to be binned and distribution through email and the web. Java executables were the most used methods for distribution by email and the web. Despite security improvements in Java, its reputation for being insecure defines its reputation as a platform, also.





New Limits on DDoS

The DDoS attack landscape has set some new records. DDoS attacks of 400 Gbps in February and 500 Gbps in November were the largest recorded attacks in internet history.

These attacks mostly used old protocols such as DNS and NTP that were based on UDP. L7 HTTP and HTTPS forms were added on the latter attack run during the "Occupy" protests in Hong Kong.

Cyber Espionage Normalizing

Snowden documents revealed that Belgacom (Belgian Telecom) networks remained hacked for a long time. Regin and similar malware were used for such activities in Belgium, EU Central, and several European networks. In late 2014, it was disclosed that U.S. and U.K. intelligence agencies would be participating in joint cyber activities.

The U.S. has begun to reorganize its cyber security efforts and gave orders to DISA on cyber defense, forming a new joint force.

Truecrypt, which was an old and trusted open source data encryption software, ended its life with a short, but suspicious statement. It became a highly controversial topic as to whether certain legal

entities were linked to that statement or not. Truecrypt users stopped using the software even though there were some other forks of the open source project.

Careto malware operated mostly in Morocco and perhaps this aided affiliation with Spain made by Bruce Schneier..

China-supported espionage activities, targeting Western and Asian states, were disclosed under the name of Operation SNM. The disclosure affirms that targets were selected to gather information for China to use in domestic and international relations.

Epic Turla (Uroborus) and Energetic Bear malware had been previously disclosed. In late 2014, the APT28 campaign was disclosed. This campaign was announced as being affiliated with the Russian state according to information extracted from malware and effected computers, such as code compiling time zone. The APT28 campaign targeted Eastern Europe governments and military organizations, the defense industry in Europe, and NATO-affiliated personnel in several countries such as Turkey.





Hacking and Information Leaks



iCloud: Apple iCloud service application interfaces have been under brute force dictionary attacks, and iCloud users with easy passwords were hacked. Intimate photos of celebrities were publicized.

Google: Some Gmail servers were hacked and about 5 million usernames and passwords were leaked in underground forums.



Ebay: In June, the passwords of 140–230 million users of eBay were stripped off. This was the largest information leak of 2014 based on affected user count.
Target: The credit card information of 70 million Target store customers was obtained by hackers through a software installed on agent machines in the cash register network.



JPM: Identification data about 80 million household and small business accounts of JPM Bank has been leaked.



JPMorgan

HSBC Turkey: The Turkey branch of HSBC bank leaked the credit card information of all customers in the last months of 2014.



Sony PS and Xbox Gaming Networks: Gaming networks have been taken down by a group named Lizard Squad using DDoS methods.

SONY

Snapchat: The account information, including phone numbers, of about 4 million individuals was leaked on the last day of 2014.





Setting Sights on Companies

Sony was attacked from several sides during the whole year. Sony Playstation networks were attacked several times during the year, resulting in outages lasting several days. In November, Sony Pictures was hacked, and the hacker group leaked information on Sony employees, budgets, salaries, and copies of unreleased Sony films.

Cyber Attacks Resulting in International Conflicts

The Sony attack turned into a U.S.–North Korea conflict after the hacker group requested that Sony cancel the release of the film, “The Interview,” which is on the leader of North Korea. The U.S. declared they found signs the Sony attack and threat was supported by North Korea. This continued with a statement that the U.S. will retaliate for the hacking and begin sanctions against North Korea.

Formerly U.S. had already declared as a doctrine, “Cyber space would be all other war domains like land, the air and seas.” The North Korea case is the first significant example of cyber attack resulting in international conflict.



Attacks on Old Friends

2014 was a difficult year and revealed crucial vulnerabilities in de facto open source software and some proprietary software. One morning, we waken up to find that we’ve been living amongst “bombs” for years.

Openssl Heartbleed: A critical vulnerability was found in OpenSSL resulting in leakage of private keys on a vulnerable SSL server. The vulnerability number is CVE-2014-0160.

Openssl Poodle: Poodle was an MITM type exploitation of vulnerabilities in Openssl by using fallback support to old and vulnerable SSL 3.0 protocol in clients and servers. The vulnerability numbers are CVE-2014-3566 and CVE-2014-8730.

NTP: NTP is an ancient protocol designed in first ages

of the internet. Ntpd is the most often used NTP service daemon for servicing time information. An attacker could use the “monlist” command to get a very lengthy reply from the ntpd. Lately, this vulnerability was exploited in large DDoS attacks. The vulnerability number is CVE-2013-5211.

Shellshock: Bash shell, which is widely used with Unix/Linux/BSD operating systems, was found to have a critical vulnerability that allows remote users to run codes on the shell. Several related vulnerabilities were used for taking ownership of servers and there are unpatched servers already.

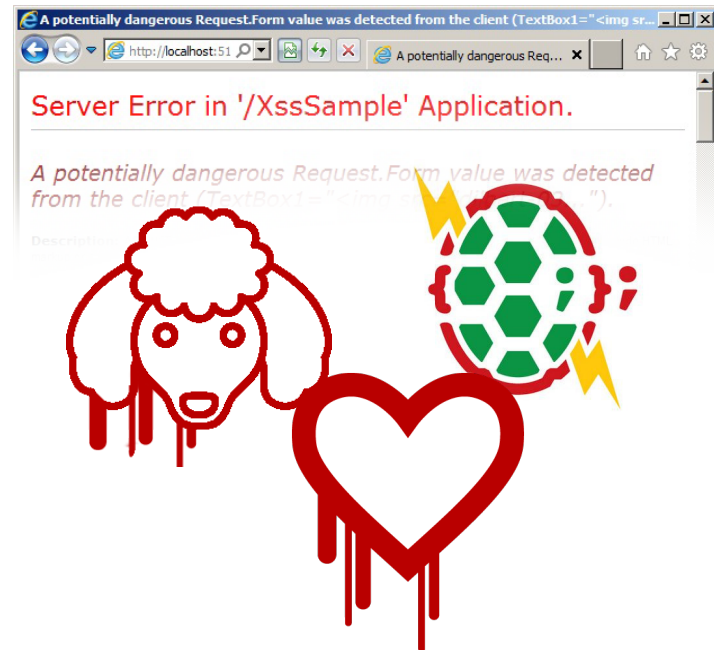


Attacks on Old Friends

The vulnerability numbers are CVE-2014-6271, 6277, 6278, 7169, 7186, 7187.

Doubledirect: Doubledirect is a full duplex exploitation of old ICMP protocol. Platforms accepting ICMP redirect-type packets are vulnerable to MITM attacks by attackers from the same network. Mostly Android platforms were shown to be vulnerable by default.

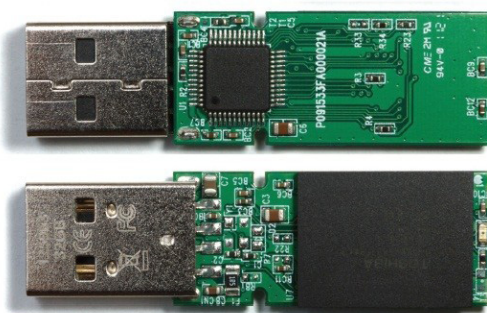
IE VB Scripting: The VBScript engine in Internet Explorer browsers was announced to have a vulnerability that allows remote code execution. That is, for more than 10 years, much of the world has been using an internet browser with a vulnerability that can be triggered by any bad website. The vulnerability number is CVE-2014-6363.



Problems with Hardware

While the industry was dealing with vulnerabilities in higher-level software and services, researchers found vulnerabilities in low-level software domains.

Bad USB: USB devices have different “personalities” like data storage, keyboards, cameras, and modems. A firmware is loading when a USB is plugged in and managing these personalities. Exploitations were released for reprogramming a USB device that makes them unreliable with unknown codes inside. Thanks to other vulnerabilities in operating systems, an altered USB can be used to hack a computer, even if it is locked, by simply plugging it into the computer. Such exploitation was revealed to the public.



EFI and UEFI: EFI and UEFI are used for rich booting a more programmable, low-level computer firmware than BIOS. New attack vectors were established by using EFI and UEFI. The Thunderstrike attack was an example concerning Thunderbolt interfaces in Apple computers and was used for injecting malicious code into the computer boot sequence. Later, other methods for hacking UEFI on several hardware platforms not only Apple, but other vendors, were developed.

Intel BIOS: BIOS of Intel chipset computers were declared to have vulnerabilities that result in bypassing write locks in BIOS areas. BIOS produced by AMI and Phoenix were discovered to be vulnerable as well.

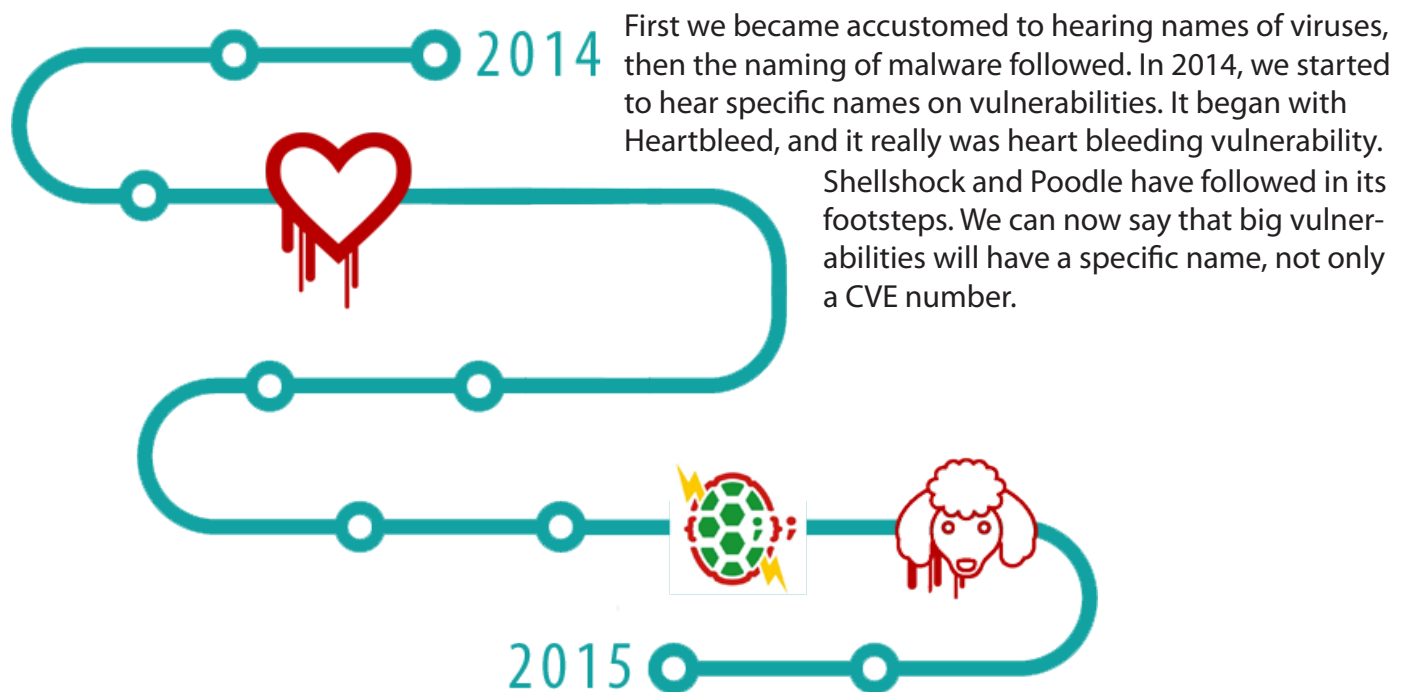


Critical Infrastructure

German mill Stahlwerks: BSI 2014 cyber security report has disclosed that a steel mill named Stahlwerks has been hacked, and the hack resulted in physical damage to production systems.

Dragonfly cyber espionage group has used Havex (Energetic Bear) class of malware to target European industrial factories. Information about damages made was very limited.

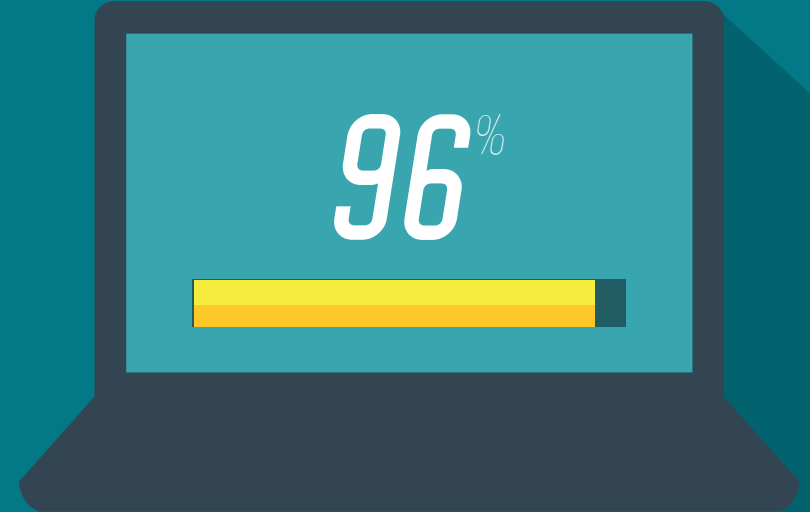
Vulnerability Naming



Some Figures from LABRIS SOC



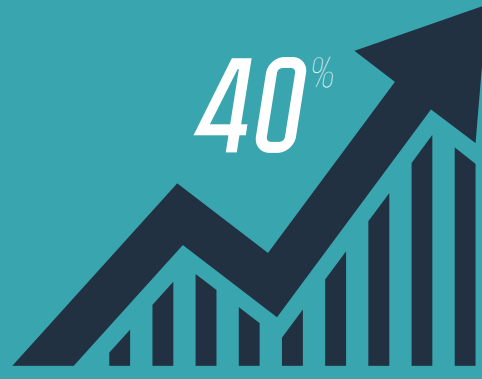
97% of mobile malware targeted **Android**.



96% of malware attacks targeted **Microsoft Windows** platforms.



E-mail **spam-virus** rate of 84% on average was achieved.



From the beginning of the year to the end, an increase of 40% occurred in the total number of **spam**.



Labris spam sensor network is blocking



80% of spam without the need for smart methods.

Most spam sent topics



Online Product Sales



Phishing and Malware Distribution Mask E-mails



Corporate Offers

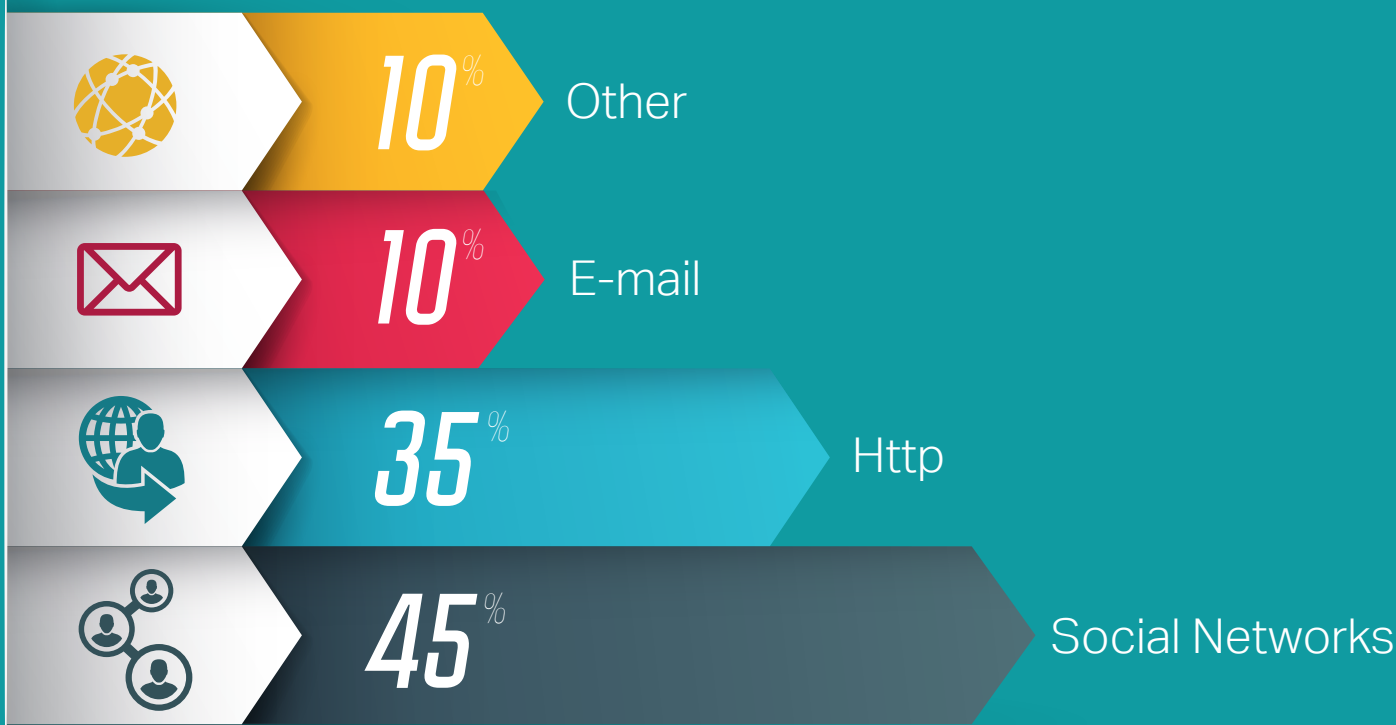


Friendship Networks



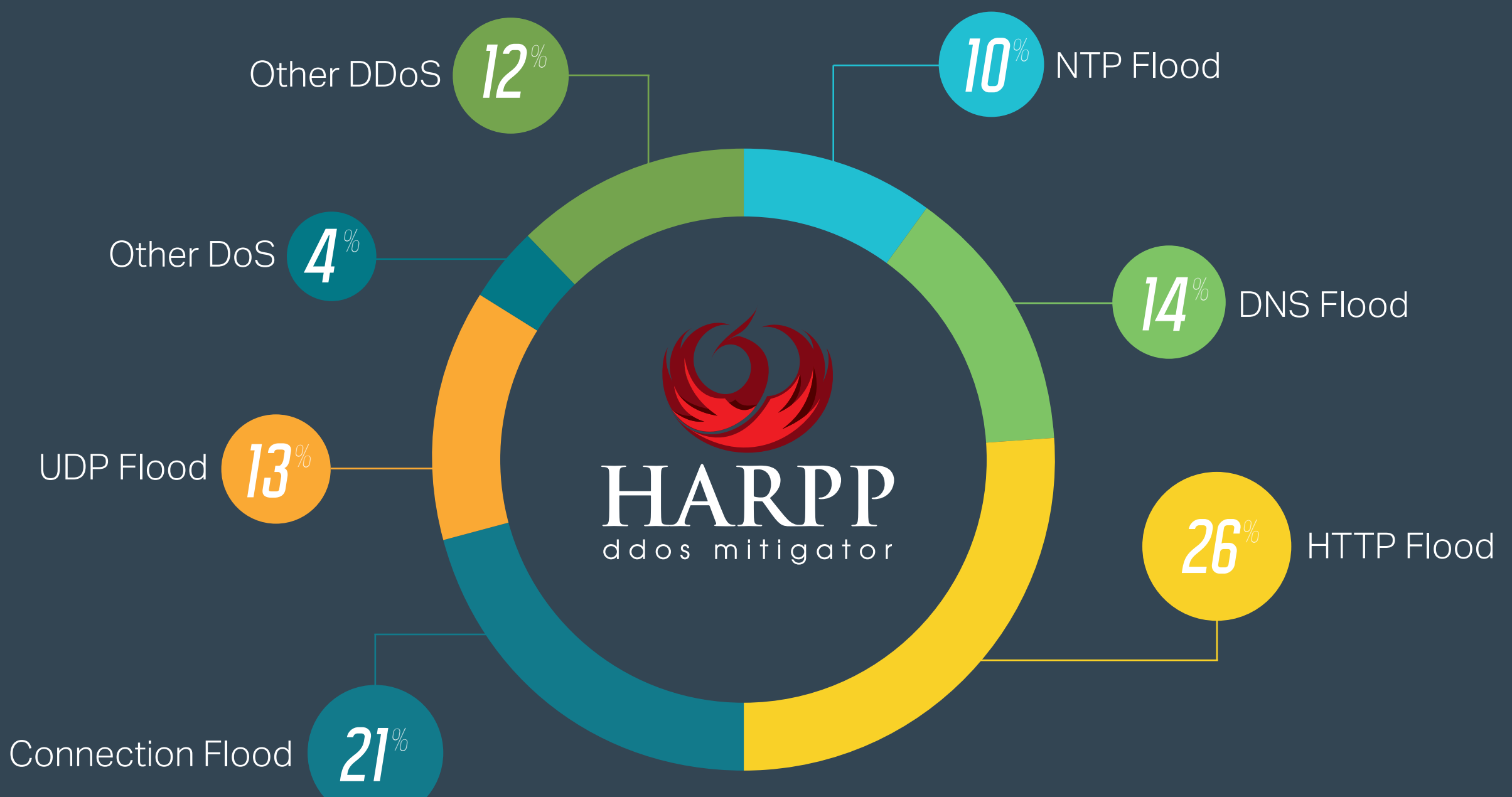
Sexuality

Applications in corporate use

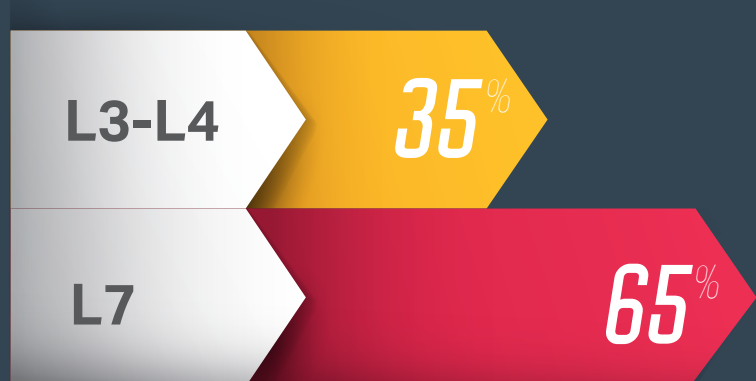


Alarms produced by the threats increased 10% over the previous year.

Some statistics from HARPP DDoS CERT



DDoS by Layers



APT Character in DDOS



Average Attack Duration



Attacks by Sector



2015 Predictions





Trust Will be More Wounded

Trust on open source and de facto legacy software is getting low, and we will be faced with more vulnerabilities on this widely-used software and protocols.



Malware is in the Hands of Ordinary Cyber Criminal Gangs



First, ZeuS source codes were leaked in 2011. Later, Citadel and Carperb-type malware had opened their code. CryptoLocker was also provided in "Do It Yourself" kits. Just as ransomware creation kits appeared to build a campaign, targeting the mass public, we expect malware creation kits to appear. Cyber criminals will use them to create specific APT campaigns to attack single targets in finance, industry, government, and military.

UEFI

Low-level hardware and firmware and hacking of that firmware are on the rise. Firmware attacks will increase. More firmware attacks, just by physical access, may be expected in mobile platforms, cars, and Smart TVs.

Mobile Devices as Zombies

There was no full-scale campaign that used mobile devices as an attack vector. We are expecting full-scale campaigns using mobile devices for sending attack packets through high-speed 3G and Wi-Fi connections. This will remind users that mobile gadgets are also computers.



IoT Security Discussions

IoT is rising, and implementations are being realized. We will see transformation of hacking PoCs into real hacking of IoT applications such as smart watches, Smart TVs, home automation systems, and cars.

Critical Infrastructure and SCADA

Campaigns attacking critical infrastructures were real. Sensors are very susceptible to security vulnerabilities by design. SCADA networks and their connection to other networks are not secure. Users of SCADA networks are not well-trained in cyber security. SCADA software is not designed with security in mind. SCADA is used in nearly all managed critical infrastructures and is a medium for espionage run by opponent states. We are expecting more attacks in critical infrastructure SCADA. On the other hand, it should not be forgotten that telecommunications infrastructure is also a critical infrastructure.



Global Router Botnets

The routers through which most end users are connected to the internet, are not very secure. There are disclosures concerning backdoors put out for easy management by vendors. Also, changing default passwords is not a wide habit, and some botnets were created just by using default passwords for hacking the routers.

Home router vendors are not used to providing frequent updates. However, there were some serious vulnerabilities in the open source software and Linux that most routers are based on. We expect more home routers and other routers will be owned by botnets and will be used in global DDoS and other types of attack campaigns. We know the Lizard Squad group and some other teams have begun gathering bots.

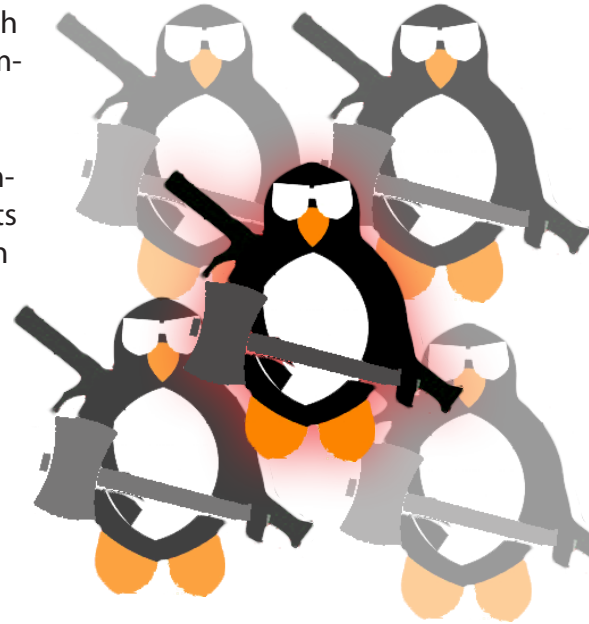


Linux-Based Bots

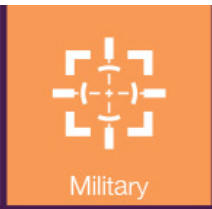
Linux-based systems are at significant locations with wide bandwidth and possess a great reputation. The systems are also powerful in computing resources.

Poodle, CryptoPHP, Revslider, and Shellshock all helped criminals embrace Linux servers. Criminals will be building more powerful botnets using Linux systems connected to the internet with large pipes. Even some focused effort, to establish a Linux-based botnet through Java based application servers, was observed in 2014. These bots will be used for several criminal purposes.

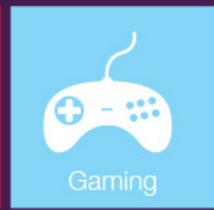
Some innovation is also expected on expansion methods of shell-based botnets. Self-expansion characteristics that we use to see in Windows-based malware will begin to be used by shell botnets running on Linux systems with rich libraries, system resources, and always-on characteristics.



Smart L7 DDOS



L3 DDoS attacks started to be a part of scrubbing provided by ISPs and data centers. However, attackers are set to find methods to take their target down. We have already experienced attacks lasting more than 2 months with 10 different attack types within the last year. The attacker is more persistent. L7 characteristics are increasing in the attacks as time passes.



Ubiquity in connected devices is increasing. Content on the internet requires lower round-trip times. Internet architects have already designed new protocols like SPDY/HTTP 2.0 to allow multiplexed requests in a single connection. L3 DDOS prevention provided by mainstream telecommunications will not help inspection of attacks in these new protocols because of small L3/L4 trace.



We expect better designed L7 attacks mostly in hybrid forms. Some of these attacks are expected to mimic real user behavior. Industry may again set new records in attack size, but complexity of the attacks will also be on the rise. Widely used protocols like DNS, SMTP, SIP, HTTP, and HTTPS will be the top attack mediums.



Cyber Weaponization

We see that specially crafted espionage malware and malware-based surveillance operations started to address countries other than the U.S., U.K., China, and Russia. We expect cyber espionage will be a standard method for non-war interstate espionage relations. The geopolitical landscape will interfere with cyberspace more.

Also, some incidents were recorded as having been carried out by non-governmental patriotic or terrorist groups. Syrian Electronic Army and ISIS groups were examples claiming responsibility for such incidents. At the moment, these incidents are at the level of getting control of some web pages and Twitter accounts; these and other non-governmental groups may increase the depth of attacks.

We can say cyber weaponization has started and will continually increase in 2015.



Low Security Awareness in Healthcare



Software and system design in the healthcare sector is far from being secure. Excluding a few countries, regulations and standards are not widely accepted. A wide range of personal information about patients is stored in healthcare institutions, including social security numbers, mother's maiden name, family information, and credit card information.

It is becoming popular in medical centers and labs to provide web interfaces for getting information on medical tests and health records to their patients. Also, most IT professionals in healthcare are not well trained in cyber security.

We expect more exposure of patient data in 2015.

Security in Mobile
is a Must



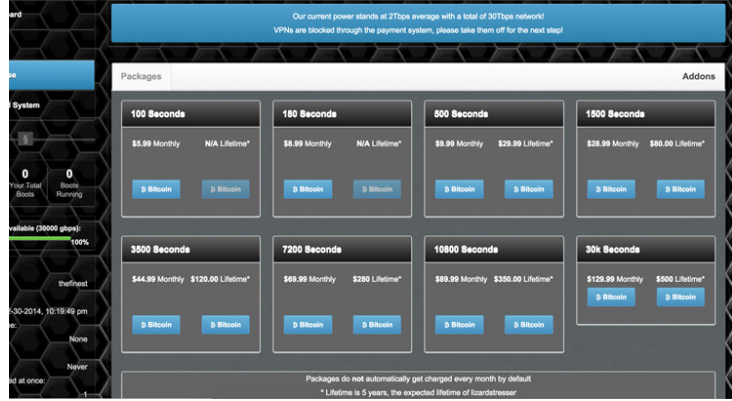
Koler and Slocker were examples of the first ransomware on mobile devices in 2014. There was also malware running on PC platforms, phishing iPhone users to give Apple ID and passwords for the purpose of locking their iPhones. Luckily, this malware campaign featuring activation lock was seen only in some geographical areas.

While PC usage is declining, mobile technology is becoming more precious to owners and is the single place of authentication information for all services. We should expect more types of mobile ransomware, requesting ransom, selling personal information like authentication information or photos gained from any mobile device.



Attack as a Service

Lizard Squad, who is charged with the Christmas PlayStation and Xbox attacks, started a service named Lizard Stresser. This was a service to make DDoS go anywhere you want. Cyber criminals were selling cybercrime kits that use acquired information to get money from victims and sell cybercrime theft goods like personal or industrial information. We expect the "attack as a service" concept to increase in 2015.



IPv6

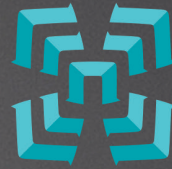
The use of IPv6 is increasing and it will be used more in 2015. Some protocols are inherited from IPv4 and implemented in IPv6 including weaknesses. Also, as it is a new protocol, IPv6 is not exposed much to the public until now. We expect to see significant vulnerabilities in IPv6 in 2015.



Security Operation Centers

We predict security operation centers will increase in 2015. However, the context will change a bit. SOC's were known as human-based operation centers for discovering and counteracting against security incidents. We expect automated computer systems to be positioned in SOC's to collect, analyze, and correlate in order to mine incident visibility and data. SOC is not SIEM, SOC is the whole input, processes, systems and outputs including people.







Labris
NETWORKS

Close Security in Cyber War



*Labris*speed 

*Labris*supportive 

*Labris*sage 

*Labris*safe 