LABRIS SOC ANNUAL REPORT

/// 2015
SECURITY THREAT LANDSCAPE

/// 2016
PREDICTIONS ON SECURITY

Labris NETWORKS

COPYRIGHT

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.

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.

2015

SECURITY THREAT LANDSCAPE

/// IMPORTANT HACKING AND INFORMATION LEAKS

IMPORTANT HACKING AND INFORMATION LEAKS

The Office of Personnel Management was Hacked Twice, Director of OPM Was Forced To Resign

Chinese Hackers breached the computer system of the Office of Personnel Management in December, but this was only disclosed in June 2015. 4 million current and former federal employees' personal data had been compromised. On July another hack occurred and this time Social Security numbers and other sensitive information of 21.5 million people had been leaked.

This incident shows that directors can and will be held responsible for security breaches by senators.

BRITISH AIRWAYS

British Airways frequent-flyer accounts hacked

Hackers have accessed tens of thousands of British Airways frequent-flyer accounts.

T-Mobile

15 Million T-Mobile Customers Sensitive Data Were Exposed

In September 2015, the data of 15 million people who had applied for service with telecoms carrier T-Mobile were leaked. It was announced by the T-Mobile Chief Executive John Legere that the data included names, addresses, birth dates, Social Security numbers, drivers license numbers and passport numbers.

37 MILION DATA LEAKED

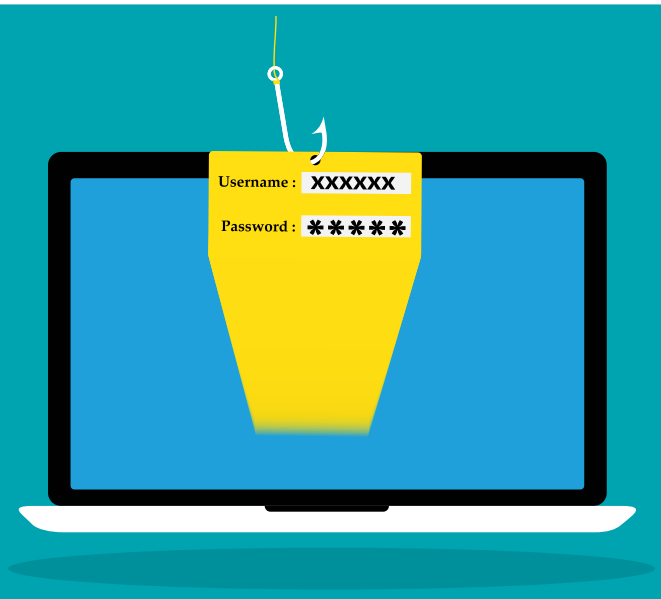
Online Cheating Site AshleyMadison Hacked

In July 2015, over 37 million member data of AshleyMadison were leaked. The leaked data included customer profiles along with the information like the secret sexual fantasies and matching credit card transactions, real names and addresses, and employee documents and emails.

Adult FriendFinder Hacked

In May 2015, the private data of 3.9m Adult FriendFinder members has been leaked, including those who had told the site to delete their accounts. The stolen data included some very private information like the sexual preferences of users, whether they're gay or straight, and even indicates which ones might be seeking extramarital affairs. In addition, the hackers have revealed email addresses, usernames, dates of birth, postal codes and unique internet addresses of users' computers.

/// CYBER SECURITY TRENDS



CryptoLocker

Throughout 2015, CryptoLocker ransomware continued to spread. It spread mostly via a phishing mail, which seemed to be coming from one of the biggest mobile network operators or postal services. The mail, which may seem as an invoice, directed the victim to download the ransomware, via a fake "Detailed information about your invoice" link. Once the ransomware is downloaded and executed, all document files (.doc, .xls, .pdf etc.) were encrypted and a ransom of about $1000 was demanded to recover the documents. Labris SOC has already identified thousands of domains containing these ransomware, and each day new domains are discovered.

Ransom Motive On The Rise

This year we have seen an increase in ransom motivated attacks not only in untargeted attacks for citizens but also for institutions. Typically, the ransoms are demanded as bitcoins. ProtonMail, the Switzerland-based encrypted email provider was hit with a DDoS attack in 2015. Interestingly, attackers reached their target as they received the ransom they demanded, which was 15 bitcoins (approximately $6,000). However, the DDoS attacks continued as if nothing had changed.

Greek banks were the target of DDoS attacks in November 2015. The attackers demanded 20.000 Bitcoin (7 million Euros) from each bank. The ransom was not paid. United Arab Emirates Bank was also demanded to pay $3 million ransom, otherwise hackers threatened to leak the customer data of the bank. As United Arab Emirates Bank didn't pay the ransom, hackers leaked the customer data.

This year the infamous Hacking Team was hacked and over 400GB of their internal data was leaked. It was found that the Hacking Team, was also using a UEFI BIOS Rootkit to keep their Remote Control System also known as Galileo, installed in their targets' systems. Even reinstalling the operating system or buying a new hard disk wouldn't help to get rid of the malware. Leaked data has shown that a lot of state entity was using the service.

Mobile Devices as Zombies

As the performance of mobile phones and the speed of mobile networks are increasing, mobile phones have begun to be used in large-scale attacks. In late August 2015, mobile devices were used to flood a website via a massive DDoS attack. 4.5 billion Requests have been made at 275,000 HTTP packets per seconds from 650,000 compromised smart phones.

IoT Security Discussions

In November, toymaker Vtech, which makes toys and tablets aimed at children was hacked. In total about 5 million customer accounts and related kids profiles worldwide were affected. The leaked data contained, name, email address, password, secret question and answer for password retrieval, IP address, mailing address and download history. In addition the database also stored kids information including name, genders and birthdates. Even, pictures of children and parents, chat logs between parents and children were leaked.

Researchers Charlie Miller and Chris Valasek have demonstrated that it was possible to control a Jeep Cherokee remotely from miles away by exploiting the car's entertainment system that was connected to the mobile data network. Not only toys and cars but also, fridges, baby monitors, sniper rifle, smart tv's were under focus of hacking and security research.

Low Security Awareness in Healthcare

The second biggest health insurance company, Anthem, revealed that, the company was the victim of what is thought to be the biggest cyberattack to hit the sector.

On February 24, 2015, Anthem, Inc. disclosed that criminal hackers had broken into its servers and potentially stolen over 78.8 million records that contain personally identifiable information from its servers. The compromised information contained names, birthdays, medical IDs, social security numbers, street addresses, e-mail addresses and employment information, including income data.

Premera Blue Cross health insurance discovered in March 2015 that 11 million patient records had been accessed almost a year previous.

Hackers targeted the UCLA Health System database in July 2015 and may have had access to over 4.5 million patients' unencrypted records.

Health institutions have now high secure software and systems development experience and open to more attacks. According NIST, Health is also a critical infrastructure and should be managed accordingly.

Security in Mobile is a Must

A new Android lock-screen-type ransomware have been spreading in the USA. After infection and setting a new PIN, the user will be prompted to pay a $US500 ransom. Unfortunately, infected users have no effective way of regaining access to their device.

Smart L7 DDOS – APT – Hacking as A Service

VPS cloud hosting provider Linode had been experiencing multiple DDoS attacks from the beginning of Christmas. The attacks were still continuing in the first days of 2016. The DDoS attack hit most of the data centers of Linode in Atlanta, Fremont, Newark, Dallas, Singapore and London. The attack caused major outages and customer frustration.It had become evident that a bad actor is purchasing large amounts of botnet capacity in an attempt to significantly damage Linode's business. The campaign was mixed with DNS, volumetric, Layer7 HTTP and router control plane attacks.

Also, Harpp DDOS CERT has statistics that show DDoS attacks have increasingly continues in the form of mixed form of attacks.

Political Motives Make Governments The Main Target: DDoS Attacks Against Turkish Critical Infrastructures

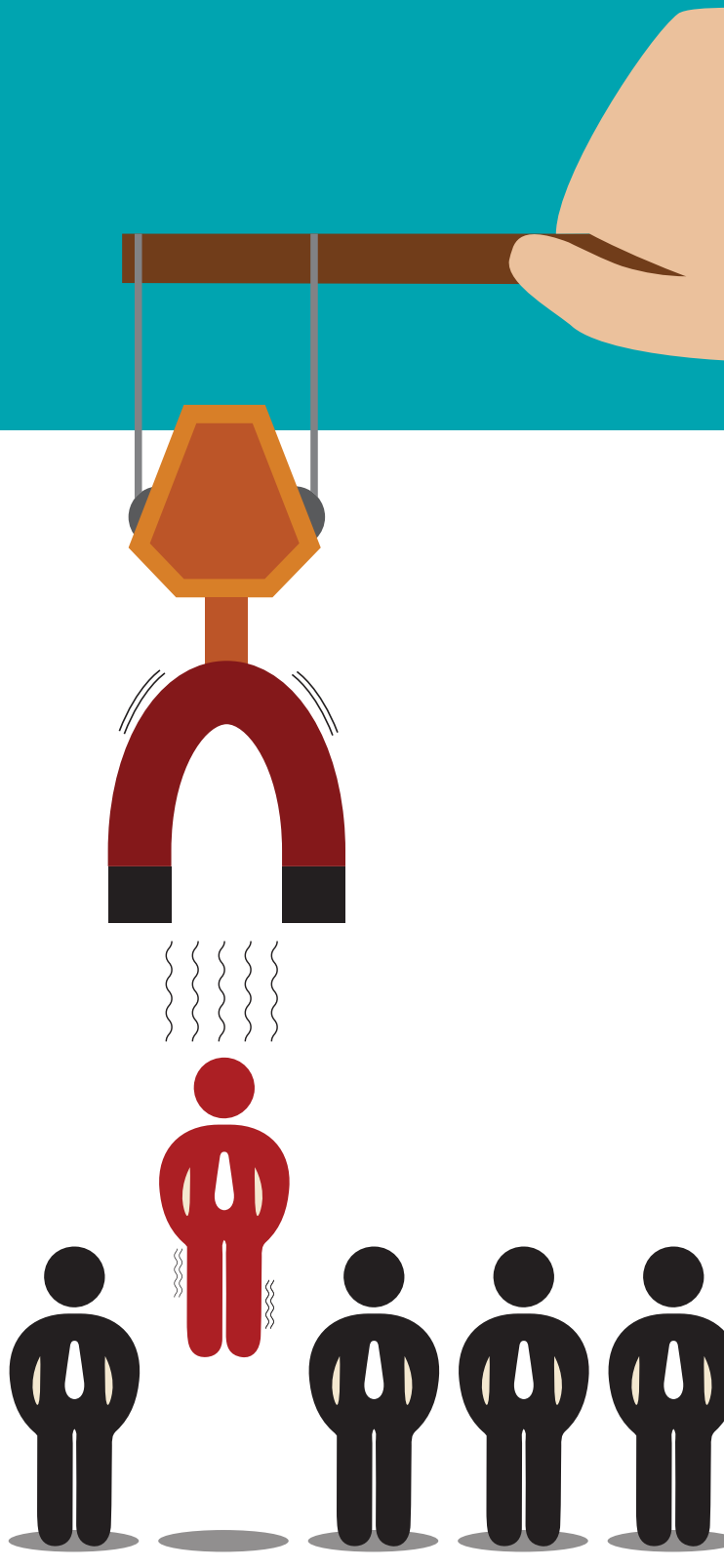
In November 2015, several Thailand government websites were the target of DDoS attacks. As a result some Thai government websites were inaccessible for several hours.

On 14 December 2015 attacks began on root DNS servers for ".tr" domains. The attacks started as DNS Amplification attacks. The main purpose of the attack was to render the ".tr" DNS servers unresponsive, thus preventing access to ".tr" websites. The attacks reached over 200 Gbps, thus overwhelming 40 Gbps fiber connections. This attack was the strongest attack Turkey has ever faced. On December 24th another attack wave targeted Turkey's top banks. Some problems in credit card transactions and banking operations occurred. Payments via credit card terminals could not be used. These attacks were claimed by the infamous hacking group Anonymous. Because of beginning of attacks was first month anniversary of Russian war plane shot down by Turkish Air Forces, these cyber-attacks were also related with Russia. Remembering 2009 Estonian cyberattack wave by Russia, signatures were very similar.

Global Router Botnets

In February a security expert in VOIDSEC noticed a strange recurring pattern on his personal website. It was a brute force attack on his WordPress site. After digging further, the attackers were mostly Italian ISPs and the attackers were all Aethra modems/routers. It was also found that the botnet was used by LizardSquad during the famous attacks on Xbox Live and Play Station Network.

Increasing attack magnitudes by Linux-Based Bots and old Protocols



In November, we have discovered an SSH brute force attack to one of our honeypots. The SSH login attempt started on 06 November 2015 and peaked on 08 November exceeding 50.000 ssh login attempts on that single day. The attack continued until 12 November with a decreasing strength. The victim had received more than 140.000 SSH login attempts from 168 unique IP addresses and after 4 days, some of the attackers managed to break the SSH password. After finding the SSH password, the attacker gains access to the system and installs a malware to the target. The malware copies itself to several directories, creates services and adds itself to the startup. The host than becomes a zombie in a botnet waiting for commands from a Command and Control server. The Command and Control server can issue the malware to start a DDoS attack. The attacks supported by this specific malware are: SYN Flood, ACK Flood and DNS Amplification attacks.

This story is one of the reasons why attacks sizes increases in 2015. Servers are becoming part of botnets. With the combined strength of multiple infected machines like these, large scale DDoS attacks are carried. It is also highly probable that these infected Linux-based bots had been used in the large scale DDoS attacks against Turkey that occurred in December.

On the other side, reflected DDoS attacks have found new vectors. We have seen Chargen and SSDP as new reflectors that increase DDoS magnitudes in 2015.

DDoS Attack Used as a Smokescreen to Hide Data Theft

Hackers launched a DDoS attack at Carphone Warehouse, a UK-based mobile phone reseller. But this attack was used as a smokescreen to disguise the stealing of personal details of 2.4 million customers. Up to 90,000 customers may also have had their encrypted credit card details accessed.

TalkTalk, a UK based Telecommunications Company which has over 4 million customers, experienced a data breach in October 2015. 56,959 customer accounts were affected by the breach, from which 15,656 sort codes and bank account numbers had been taken. This amounts to 4% of customers whose financial data is compromised. There were 28,000 partial credit and debit cards stolen. TalkTalk stated the lost data had not been encrypted, but they were not legally required to encrypt it. Again, DDoS attack was used as a smokescreen to distract security professionals, while the hackers compromised the personal data on the site through a different loophole.

Insecure Security Products Have Caused Unreliability

On January 9, someone published an exploit for an SSH backdoor affecting older versions of FortiOS. Fortinet, which claimed the issue was a management authentication bug and not a malicious backdoor.

On December 2015, Juniper discovered unauthorized code in ScreenOS that could allow a knowledgeable attacker to gain administrative access to NetScreen devices. Vulnerability was using an SSH backdoor and also another one was using an insecure VPN mode. These two issues were important and resulted distrust in security vendors.

2016

PREDICTIONS ON SECURITY

///MAIN PREDICTIONS
///OTHER PREDICTIONS

/// MAIN PREDICTIONS

DDoS Attacks Will Be Used As Smokescreen In Data Breaches

The data breach attacks in Carphone Warehouse and TalkTalk have been successful, partly due to DDoS attacks being used as Smokescreen. Attackers have learned that this is a successful technique and thus we will see more usage of DDoS attacks as smokescreen in data breaches.

Attacks Over Https

Malvertising is the use of online advertising to spread malware. Malvertising involves injecting malicious or malware-laden advertisements into legitimate online advertising networks and webpages. Even though some services and products are getting better at detecting malvertising, the bad guys are also finding new technics. In 2016, we expect an increase in successful malvertising attempts through the use of HTTPS. If your organization does not use security products that can monitor HTTPS traffic, you may be under this risk.

Mobile and IoT will be important part of botnets

Former CCTV and SmartTV inclusion in botnets were signs that IoT devices and mobile gadgets will be an important part of botnets in the near time. Thinking the speed provided by 4G-5G networks we can say attacks capacities will not be small.

ISPs should be treated as Critical Infrastructures

Linode attacks also have shown that routers on the way to the internet operated by ISPs are attacked also. Attackers were trying to block not only your own internet access but also some points in the way. Also in HARPP CERT, we have seen several examples of DDoS attacks targeting routers and also BGP peers. Control backplanes of routers gets packets and affected by the attack. Also Routing backplanes are affected after a while. We expect such attacks to continue in 2016 also. Unfortunately, most of the node routers are open for getting packets directed to them. All ISPs should also be regulated to have some level of security hardening in their network equipments.

National Security will be More Localized while More Intentional/Unintentional Vulnerabilities and Backdoors Will Be Discovered In Security Products

In 2015, we have seen vulnerabilities and backdoors in Fortinet and Juniper products. These incidents have raised questions about the security and reliability of security products. So security researchers will turn their attention on security products and more vulnerability and perhaps backdoors will be discovered. These vulnerabilities and backdoors increase concerns on national cyber security at other part of the world then America. Countries will try to develop their own national measures on cyber security.

/// OTHER PREDICTIONS

Social Engineering And Spear Phishing

Humans are the weakest part of the security chain and the attackers are very aware of this. Social engineering has always been the one of the main tactics attackers have used. As lots of data breaches occurred in 2015, these leaked data and private personal information will be used to make spear phishing emails appear legitimate. Companies should invest more in security awareness training that includes the latest social engineering techniques.

Ransomware On Mobile

In the past years we have seen many ransomware attacks mainly CryptoLocker. As encryption methods used by these malwares evolved, it has become virtually impossible to unencrypt the encrypted data. So some companies have given in to the ransoms to recover their encrypted files. In 2015 we have seen lock screen type ransomwares in Android. As Android and other mobile system usage increases for business purposes, the value of the assets on these types of devices increases. So we expect more ransomware attacks on mobile devices in 2016.

Government Sites Will Still Be One of The Main Targets

Terrorism and political motives are also the main motives behind attacks. Terrorism doesn't stop. ISIS and other terrorist organizations continue their attacks. These attacks are also on the cyber space as cyber space is also a warzone. We have seen DDoS attacks on Turkish and Thailand governments and also security breaches and data leaks in the US government systems such as the Office of Personnel Management hack made by China. As in the previous years, government sites and systems will be the main targets for terrorist organizations and other governments.

/// OTHER PREDICTIONS

IoT Usage Increases as IoT Threats increases

In 2015 we have seen many security breaches in IoT. This trend will continue and increase because more and more devices are becoming part of IoT and IoT is not ready for security in any direction. Lack of basic security protections, lack of memory and OS capabilities and very large attacks surface are main reasons for problematic IoT rise.

More DDoS To Come

The number of DDoS attacks conducted in 2015 has hit record highs. Also we have seen attacks as high as 500 Gbps in 2015. This increase in the number and strength of the attacks may be attributed to several factors: Increasing bandwidth, increasing number of compromised computer systems, the publishing of easy to use DDoS tools, and increased motives. As there are no decrease in any of these factors we can easily predict that the number and size of the attacks will increase and set new record highs.

Data Breaches Will Continue To Destroy Companies, Fire Managers and Possibly Take Lives

The data breach of Ashley Madison caused many consequences. Users whose details were leaked filed a $567 million class-action lawsuit against Avid Dating Life and Avid Media, the owners of Ashley Madison. At least three suicides have been committed by the victims of this data breach. Another company, Vtech, has suspended trading on the Hong Kong stock exchange as a result of falling share prices after the data breach. Also, the director of the US Office of Personnel Management was forced to resign after two data breaches. Seeing these data breaches have been successful and caused the downfall of many people and companies, bad actors have been even motivated. With the increased motivation and success stories behind these data breaches, we expect more of these breaches.

Mobile Apps Will Be Targeted More Frequently

Some mobile apps access our emails, contacts, phone numbers, geo locations, text messages and even photos. We have seen that popular applications like Snapchat have already been targeted. A security flaw was also found in Instapaper, the popular Android app that allows users to save and store articles for reading when they're offline or don't have Internet access. The expanding customer demand or need for mobile apps causes app writers to rush to publish their apps and this rush causes programmers to overlook security vulnerabilities. The low security quality of mobile apps combined with the valuable information they access, will make them one of the main targets in 2016.