LABRIS SOC ANNUAL REPORT

///2016 SECURITY THREAT LANDSCAPE

///2017 CYBER SECURITY PREDICTIONS

Labris NETWORKS

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.

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.

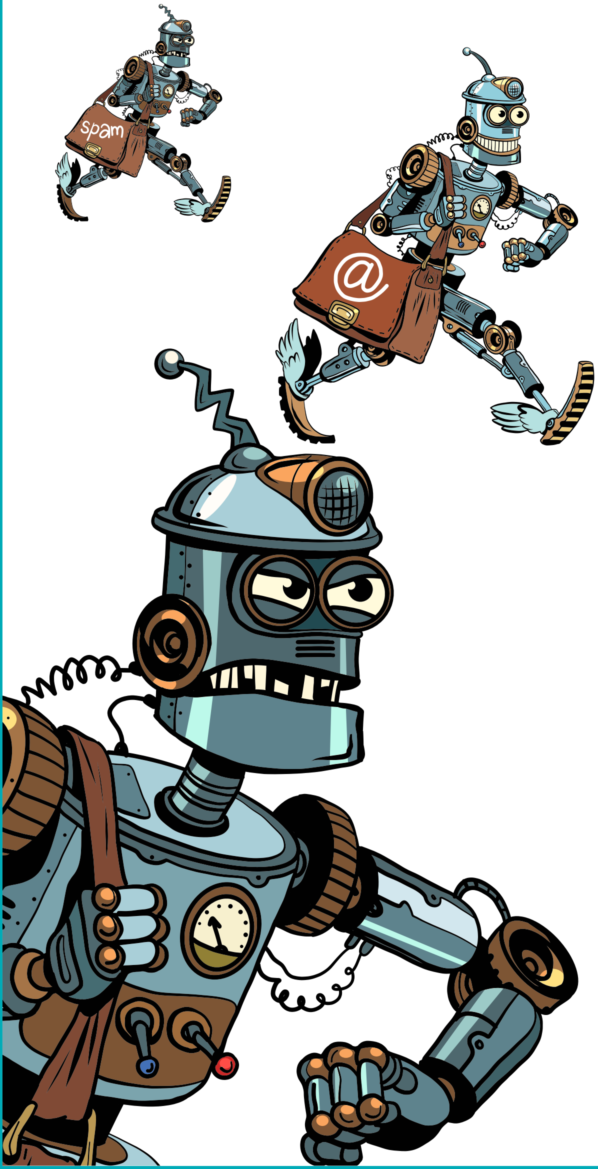
Labris with its worldwide partners is committed to the highest levels of customer satisfaction and loyalty, providing the best after-sales support through the multilingual Global Support Center. Being a rapidly growing global player, Labris offers its clients top-level security at optimal cost. Labris,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

2016

SECURITY THREAT LANDSCAPE

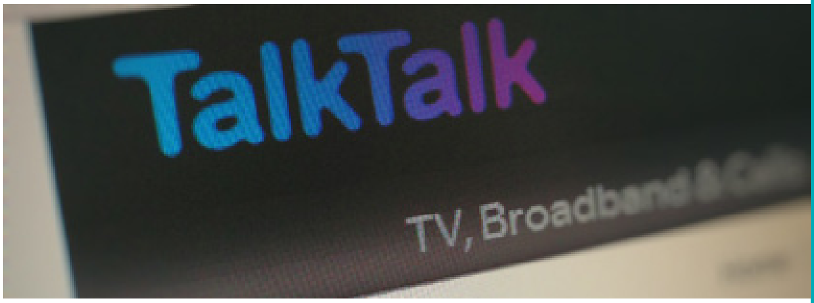
/// IMPORTANT HACKING AND INFORMATION LEAKS

200 GIGABITS PER SECOND



ISPs as Critical Infrastructures

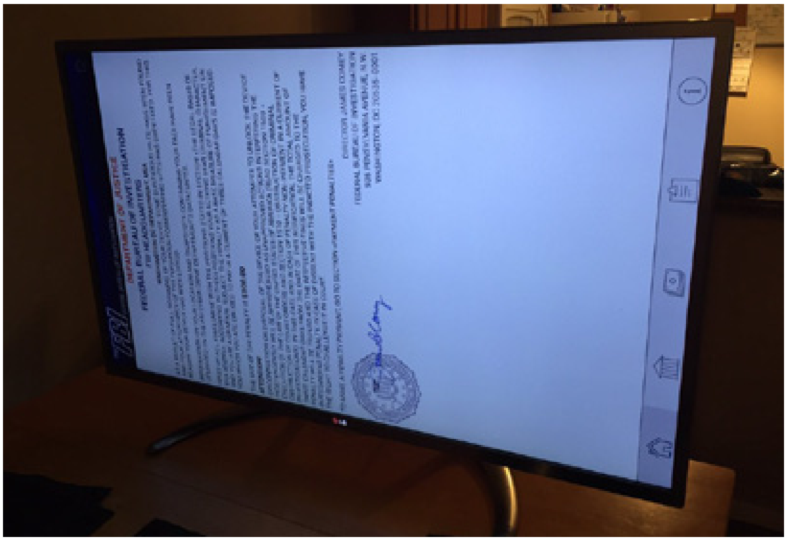
On July, September, and October 2016 Indian ISPs have been under huge DDoS attacks. The magnitude of the attack was around 200 gigabits per second. Cyber lawyer Prashant Mali said all servers of government and commercial entities access the internet via ISPs. "Thus, an attack on ISPs is an attack on the nation."



In the last quarter of 2016, British TalkTalk, Post Office, Kcom and German Deutsche Telekom was under attack and 100.000s of customer lost internet access during attacks. TalkTalk has also received a big fine from British regulatory authority for not having measures for preventing the attack.

Mobile and IoT botnets, more DDoS

On October 21, 2016, internet infrastructure DNS provider DYN had been targeted by multiple DDoS attacks. With an estimated throughput of 1.2 terabits per second, the attack is the largest DDoS attack on record. The attack disrupted traffic to hundreds of websites. Some affected sites were; Twitter, Paypal, CNN, Spotify, Reddit, eBay, Airbnb, HBO and the New York Times. The attack was a botnet coordinated through a large number of Internet of Things-enabled (IoT) devices, including cameras, residential gateways, and baby monitors, that had been infected with Mirai malware.

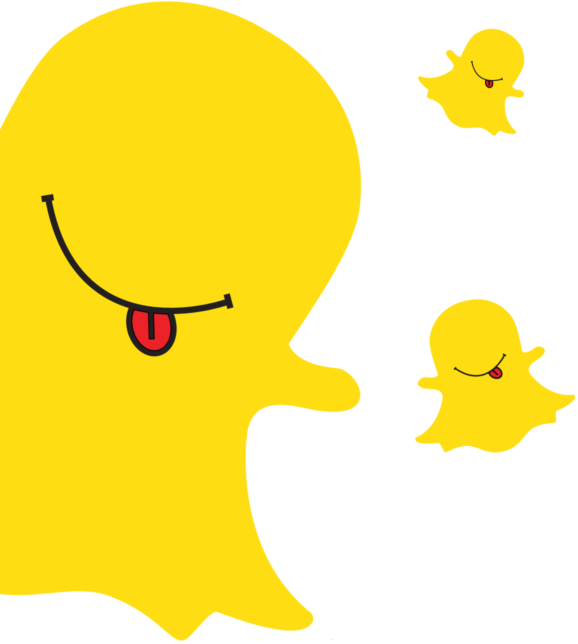


On December 2016, we have seen a smart TV infected with a ransomware called Android Locker. A Twitter user Darren Cauthon has tweeted a photo of his LG Smart TV with a warning which appears to be an FBI warning. Restoring the TV to working order was not easy as resetting the TV required access to a menu that was locked by the ransomware.

Social Engineering and Spear

WORLD
ANTI-DOPING
AGENCY

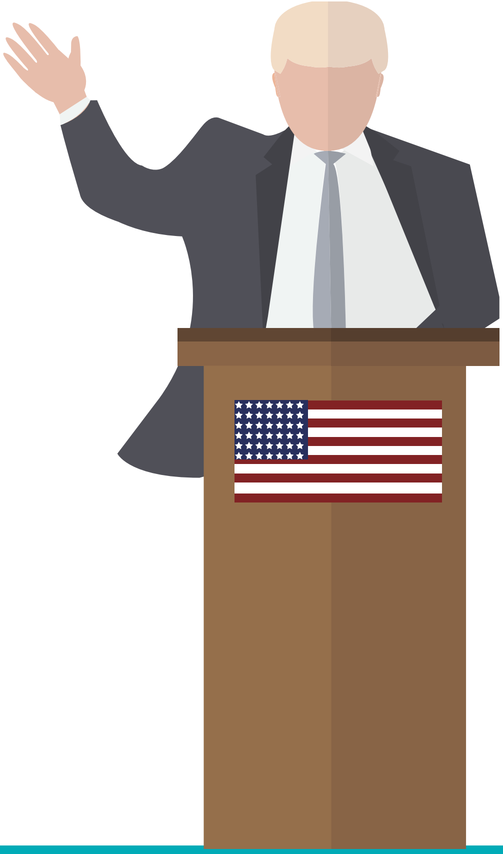
The World Anti-Doping Agency (WADA) announced that Russian hackers had illegally accessed its Anti-Doping Administration and Management System (ADAMS) database. The hackers obtained the access to the system by stealing credentials through a spear phishing attack against an "International Olympic Committee" (IOC)-created account for the Rio 2016 Games. Hackers exploited the attention on the Olympic Games in order to trick the victims with a classic social engineering attack. The hackers published some of the stolen data online and accused U.S. athletes Simone Biles, Elena Delle Donne, and Serena and Venus Williams of using banned drugs with WADA's approval.



A Seagate employee fell for a phishing email that appeared to be coming from Seagate CEO Stephen Luczo requesting the 2015 W-2 tax forms for all Seagate employees. As a result personal data including social Security numbers, their salaries and other personal information were stolen.

SEAGATE

On February 2016, a Snapchat employee fell for a phishing mail, which impersonated Snapchat's CEO Evan Spiegel, requested and reached payroll information for employees.



Government Sites were under attack

The US presidential elections were the target to cyber attacks. On July 22, 2016, WikiLeaks released approximately 20,000 emails sent from or received by Democratic National Committee (DNC) personnel. On October 7, 2016, WikiLeaks started releasing series of emails and documents sent from or received by Hillary Clinton campaign manager John Podesta. According to the U.S intelligence, these attacks had shifted the elections in favor of Donald Trump. As a result of these attacks, the U.S. expelled 35 suspected Russian spies, shut down two Russian compounds.

Mobile Apps and Ransomware On Mobile

This year it has been found that Google Play, the official market for Android applications had been hosting a ransomware application. It was called Charger and hidden inside another app called EnergyRescue. Once the application was installed, it requested too many permissions and if the permissions were granted then the malicious application locked the device and displayed a message demanding ransom.

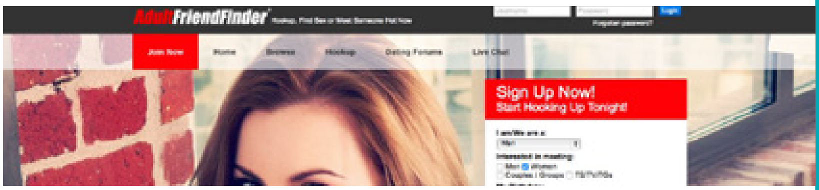
1 BILLION YAHOO ACCOUNTS WERE STOLEN

Mobile platforms have been faced with not only ransomware but also rooting malware that acquires root permissions and other types of Trojans.

Google has announced a change in application acceptance policies is planned to prevent unauthorized data collection and processing done by applications.

In general, ransomware types, modifications, and incidents had increased by multiple times throughout of 2016.

Data Breaches to Destroy Companies, Fire Managers and Possibly Take Lives



Adultfriendfinder was hacked again this year. More than 412 million accounts were exposed including over 15 million "deleted" accounts. The exposed data contained usernames, email addresses and the date of the last visit, and passwords.

On September 2016, Yahoo disclosed a data breach saying that at least 500 million Yahoo accounts were stolen from the company in 2014. Just 3 months later in December 2016, Yahoo had announced another huge security breach which dates back to 2013 and is thought to be separate from the massive cybersecurity incident announced in September. This time over 1 billion account data had been stolen including names, email addresses, and passwords.

Myspace was hacked and the database of 427 million passwords (first and secondary) and e-mails for more than 360 million users of Myspace were put to download for free.

Other big data breaches of 2016 were; Weebly 43 million, University of Berkeley 80.000, Tumblr 65 million, Opera 2 million.

Multiple data breaches including Mexican and Philippine citizens voter data

93.4 million of Mexican citizen's voter data have been exposed and was made available to download through cloud servers.

55 million of Philippines voter data had been compromised including sensitive information such as passport and fingerprint data.

Other

There have been continuous cyber attacks against the SWIFT global banking network. As a result of these attacks $81 million have been stolen from the Bangladesh central bank in February 2016. Also on December, Akbank and 2 other Turkish banks have been affected by these attacks and as much as $4 million have been stolen.

More than a dozen accounts on the Telegram instant messaging service have been compromised. Millions of Iranian Telegram users have been identified by hackers. The attack had been successful by intercepting the authorization codes via SMS. The codes enabled them to read chat histories and new messages.

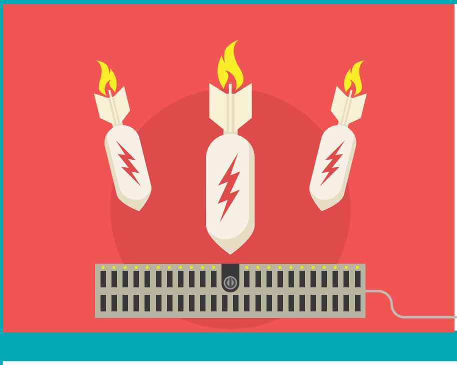
On August 2016, it was found that Oracle's Micros POS system was breached. MICROS is one of the biggest PoS vendors in the world. The hackers compromised the MICROS customer support portal. This allowed the attackers to steal MICROS customer usernames and passwords when customers logged into the support website.

1.5 million Verizon Enterprise customers' contact information was possibly compromised by a security vulnerability.

In February 2016, the Hollywood Presbyterian Medical Center paid a $17,000 ransom to unlock EMRs and the hospital´s email system.

2017

PREDICTIONS ON CYBER SECURITY



New Records for DDoS Attacks

In 2016, we have seen DDoS attacks with more than 1 Tbps, which was the biggest DDoS attack ever. This year we expect to see even bigger DDoS attacks which will be directed at critical infrastructures or maybe used to take a whole country's or a cloud infrastructure provider's Internet down.

IoT will continue to amplify DDoS Attacks

Actually, IoT is getting more secure, however, attackers are also getting familiar with previously unknown IoT devices. As we have predicted in 2016, the largest DDoS attack has been conducted using IoT devices infected with the Mirai malware. This year, we also expect IoT enabled devices to be highly utilized in DDoS attacks.

Social Engineering and Phishing will continue to be successful

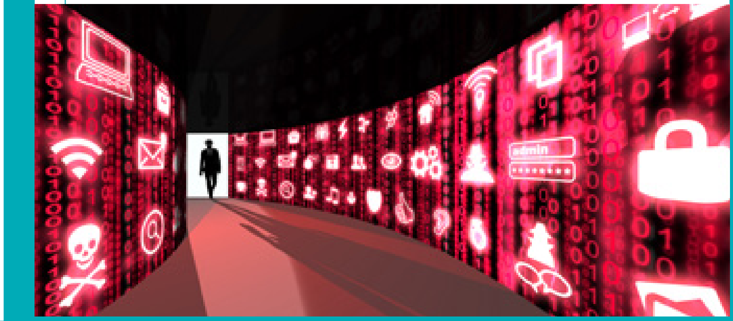
Cyber security at perimeters is getting stronger and it is easier to reach employees through side channels. Employees will continue to be the weakest link in security. Seagate, Snapchat, World Anti-Doping Agency all fell for phishing attacks. Social engineering attacks have always been a problem and it will continue to succeed this year.

Hacking for political motives will become more common

As seen in the U.S electoral campaigns, hacking and leaks of private data affect voters' decisions. We expect to see more Wikileaks-style releases of documents belonging to politicians through hacking.

AI and Cyber Threat Intelligence

Cyber threats are changing and attackers are smarter and fast moving to wear masks. AI and machine learning will start to be utilized instead of rule-based measures. However, critical information of previous activities of an attacker or attack source will be utilized to support AI based systems.



Drone Jacking

Both Amazon and UPS have announced plans to deliver packages using drones. Also both amateur and professional cinematographers are making use of expensively equipped drones for photography and video capturing. Capturing these drones, and reselling them or their cargos will be tempting for cyber criminals. Therefore, we expect to see hacking into drone signals resulting in drone-jacking this year, or in the following years.

Demand For Cyber Insurance Will Increase

Governments are increasingly paying attention to data privacy, and they are holding the businesses accountable for data breaches. As a result, companies are turning to cyber insurance. The cyber insurance market doubled in size from 2012 to 2015, topping $2 billion. As cyber attacks and their financial implications grow, so will the cyber insurance market.

Ransomware Will Evolve

Ransomware will continue to be a big problem in 2017 but we expect new and cleverer ransomware families. Organizations that have up-to-date backups of their data are less vulnerable to ransomware attacks, as they can easily restore encrypted data. Because of this, ransomware authors are getting smarter and they are trying to find backups before encrypting user files. They are trying to find and destroy local backups but it is expected that these ransomware will also access and delete cloud backups. We also expect ransomware to show worm characteristics, which means that these ransomware will clone themselves and infect the entire network. Also, we expect to see ransomware spreading according to client segment (personal, corporate) and request different ransoms programmatically.

Security as a Service and Security Operation Centers

As small and medium businesses (SMBs) have very limited IT teams and rarely any dedicated security professionals, they are frequently targeted by cyber criminals. Medium and big enterprises are open for advanced type of attacks. Such attacks require know-how and experience to mitigate. Therefore, we expect the demand for outsourcing network security will rise.

Known Vulnerabilities Will Be Continued To Be Exploited

Nothing new here as new vulnerabilities will be found every day and exploits will continue to take advantage of these vulnerabilities. Continuously monitoring for security updates and patching the known vulnerabilities will continue to be a challenge.

Europe and GDPR

Data Protection Regulation of EU will be effective in the following year and any prior work should be done will be completed in 2017. Especially, personal data acquisition, processing and storing procedures and their security will be inspected in all institutions and companies dealing with EU citizen data.

Cyber Security HR

Cyber Security human resources are scarce. It is not easy to train and reach professional know-how and experience. However, expectations are high. Inter-disciplinary position needs may also require non-technical cyber security professionals.