NCC group

NCCConX

LISBOA 2020

NCCConX Lisboa 2020 is inspired by our internal conferences and features talks from a host of speakers across the globe.

With a selection of the best talks and research highlights from our internal conferences, this event will cover recent trends, threats and best practices within cyber security.

10:30am
Tuesday

10.03.20

Venue
H10 Duque de Loulé
Av. Duque de Loulé 81-83
1050-088 Lisboa

Collaborative resilience building in Europe

John Morgan Salomon, Regional Director EMEA, FS-ISAC

This session will give an overview of how the European financial sector has been developing collective preparation and defence through information and collaborative resilience mechanisms. It will provide a short intro to FS-ISAC, a member-owned non-profit consortium built to protect the financial sector and the billions of people who rely on it.

FS-ISAC's John Salomon will discuss general threat trends, and segue into resilience-building mechanisms such as sector-wide exercises, playbooks, and support for European testing standards, as well as how supervisors and regulators are being increasingly involved in supporting such efforts.

TIBER-EU: why should you care?

Philippe Roy, Security Consultant, NCC Group

TIBER-EU is a framework designed to strengthen cyber resiliency for European companies in the financial sector. The framework challenges organisations to perform red teaming tests in a live environment, in order to assess their processes, people and technical capabilities. Based on current real-life threats, these tests are tailored to the individual organisation, and hence far more realistic than an off-the-shelf red team test.

In this talk, Philippe Roy will give you insights into how you can use the TIBER-EU framework as knowledge-sharing tool, a means to take your cyber resilience far beyond compliance, and a way to enhance your reputation.

TIBER and community threat intelligence

John Morgan Salomon, Regional Director EMEA, FS-ISAC

We will discuss the drivers behind collective information sharing and resilience in the financial sector, and touch on the ORX-FS-ISAC cyber risk framework as a means to map information security requirements and realities to business risk. The session will then move on to intelligence-based resources for security testers, drawing inspiration from the development of a generic threat landscape report for TIBER-DK in collaboration with the Nordic financial CERT. We will conclude by talking about opportunities for, and value from, future red teaming resource development in the sector.

An update on the notorious FIN6 group

Maarten Van Dantzig, Lead Intelligence Analyst, Fox-IT (part of NCC Group)

FIN6, most well-known for breaching the retailer Target and getting away with over 40 million credit cards in 2013, is an infamous threat group which hasn't stopped evolving since.
During this talk, insight will be provided into the methods and techniques that the group adopts to monetise their operations to the fullest. These techniques include Point-of-Sale malware, targeted ransomware and even extortion.

13:00 - 14:00 Lunch

14:00 Introduction

The Research of Tomorrow: Printers, Cloud & Machine Learning

Xavier Garceau-Aranda, Senior Security Consultant, NCC Group

In this talk, Xavier Garceau-Aranda will take you through our printer research project, which was presented at DEF CON, HITB and 44CON, and uncovered a large number of zero-day vulnerabilities (over 50 CVEs) in the process.

You will be introduced to two cloud research projects presented at BlackHat USA: Scout Suite, an open source multi-cloud security auditing tool enabling security posture assessment of cloud environments, and Azucar, a plugin-based tool to help assess the security of Azure Cloud environment subscriptions. Last but not least, you will learn how machine learning techniques might form part of a web application tester's standard toolkit with an insight into Project Ava.

Evidence-driven security

Philippe Roy, Security Consultant, NCC Group

How do you know where to focus your valuable resources and how to achieve the best ROI?

Prioritising scarce resources is one of the biggest challenges that organisations face when manoeuvring IT security. Poorly-planned or reactive security strategies often have severe consequences for organisations. But how do you create a successful security strategy? First and foremost, you will need to acquire an overview of your current situation – i.e. an understanding of your risks, critical assets, weak spots and outside threats to your business. Based on this information, you should create a strategy that includes a prioritised list of actions, and learn how to measure your success and benchmark against your peers. Philippe Roy will show you how to get started.

From Wire Fraud to High Impact Targeted Ransomware

Maarten Van Dantzig, Lead Intelligence Analyst, Fox-IT (part of NCC Group)

In 2014, the first large-scale ransomware operation, Cryptolocker, saw the light of day. Since then, many imposters have written their variant of ransomware, all following the same principle of encryption and extortion. Now, in a new trend, the usual suspects of the financial fraud eco-system have moved away from traditional wire fraud, to conducting targeted attacks with the goal of distributing ransomware to the entire network of a specific target. During this talk, Maarten van Dantzig will take you through the history of ransomware, from simple attacks locking the victim's screen, to the highly-targeted destructive attacks of today.

16:00 Wrap up and Q&A