KASPERSKY SECURITY INTELLIGENCE SERVICES

Fabio Sammartino

Pre-Sales Manager

Kaspersky Lab Italia

KASPERSKY LAB MAJOR DISCOVERIES

	Duqu	Flame	Gauss	miniFlame	Red October	NetTraveler	Careto/The Mask
Threat							
Classification	Cyber-espionage malware	Cyber-espionage malware	Cyber-espionage malware	Cyber-espionage malware	Cyber-espionage campaigns	Series of cyber-espionage campaigns	Extremely sophisticated cyber-espionage campaigns
Detection	September 2011	May 2012	July 2012	October 2012	January 2013	May 2013	February 2014
Active	Since 2010	Since 2007	Since 2011	Since 2012	Since 2007	Since 2004	Since 2007
Facts	• Sophisticated Trojan • Acts as a backdoor into a system • Facilitates the theft of private information	• More than 600 specific targets • Can spread over a local network or via a USB stick • Records screenshots, audio, keyboard activity and network traffic	• Sophisticated toolkit with modules that perform a variety of functions • The vast majority of victims were located in Lebanon	• Miniature yet fully-fledged spyware module • Used for highly targeted attacks • Works as stand-alone malware or as a plug-in for Flame	• One of the first massive espionage campaigns conducted on a global scale • Targeted diplomatic and governmental agencies • Russian language text in the code notes	• 350 high profile victims in 40 countries • Exploits known vulnerabilities • Directed at private companies, industry and research facilities, governmental agencies	• 10,000+ victims in 31 countries • Complex toolset with malware, rootkit, bootkit • Versions for Windows, Mac OS X, Linux • Considered one of the most advanced APTs ever

KASPERSKY lab

How the Carbanak cybergang stole $1bn

A targeted attack on a bank

1. Infection

Carbanak backdoor sent as an attachment

Bank employee

Emails with exploits

Credentials stolen

100s of machines infected in search of the admin PC

2. Harvesting Intelligence

Intercepting the clerks' screens

Hacker

Cash transfer systems

Admin

Rec

3. Mimicking the staff

How the money was stolen

Online-banking
Money was transferred to fraudsters' accounts

E-payment systems
Money was transferred to banks in China and the US

Inflating account balances
The extra funds were pocketed via a fraudulent transaction

Controlling ATMs
Orders to dispense cash at a pre-determined time

MALWARE FINANZIARIO NEL 2014

Attacchi Phishing

Gli attacchi di phishing, compresi quelli diretti a banche, sistemi di pagamento e shop online rappresentano il **28.73%** di tutti gli attacchi di phishing

Attacchi Malware

Nel 2014 i prodotti Kaspersky Lab hanno bloccato **22,9 milioni** di attacchi effettuati da malware finanziario.

Il **75,63%** di questi attacchi miravano alle credenziali per siti di online banking

KASPERSKY lab

LA MAPPA DEI SERVIZI

Per applicare le conoscenze
Consulenza

Per integrare i prodotti
Servizi Professionali

Ricerca
Per aumentare le conoscenze

Servizi Operativi
Per estendere le funzionalità dei prodotti

INTELLIGENCE REPORTING

INTELLIGENCE REPORTS

I vantaggi

- **Early Warning** per le minacce finanziarie
- Tutte le informazioni sulle campagne malware, metodi di propagazione, indicatori di infezione rilevati da Kaspersky Lab

L’abbonamento al servizio comprende

- Sommario esecutivo
- Descrizione delle minacce più recenti
- Statistiche generali sulle minacce informatiche per il mondo finanziario

CYBERSECURITY EDUCATION

CYBER SAFETY TRAINING PROGRAM

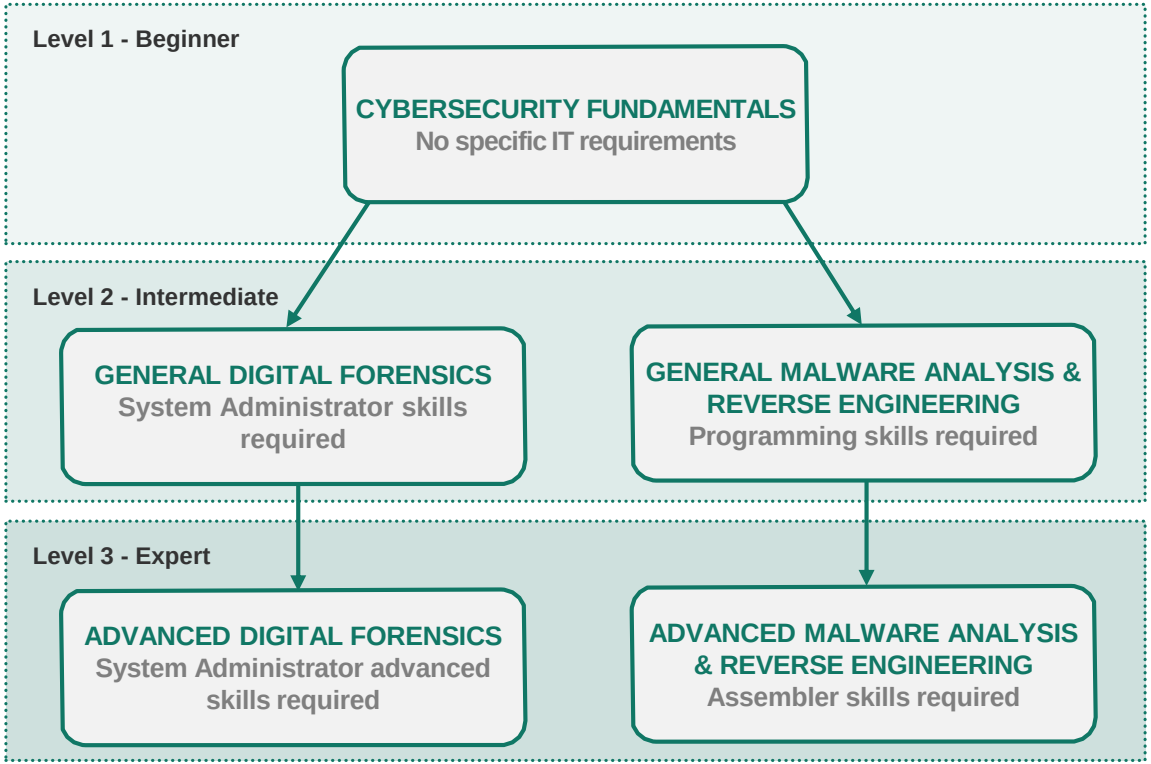
Cyber Safety: Onsite

- Gioco interattivo a squadre che affronta 9 temi di cybersecurity.
- Impersonare il Cybercriminiale, giocare in squadra per aumentare la security awarness.
- Almeno10% dello stafff

Cyber Safety: Online

- Training Online che affronta 11 temi diversi .di cybersecurity
- Analisi delle competenze raggiunte
- Maeriale sulla Sicurezza informatica fornito a support (posters, email templates, screensaver)

CYBERSECURITY EDUCATION



PAYMENT SYSTEMS THREAT INTELLIGENCE

ATM AND POS SECURITY ASSESSMENT

Security assesment per apparati di rete, applicazioni, processi e interfacce

Penetration test con tool di exploiting e sfruttamento vulnerabilità

Verifica della compliancy con le best practice del settore

Guideline per la messa in Sicurezza dei terminali

Informazioni sulle vulnerabilità dei sistemi POS/ATM, incluse le 0-Day e quelle hardware

Report dettagliato sui flussi operativi e applicativi, su rischi e contromisure

PAYMENT SYSTEMS IT INFRASTRUCTURE PENETRATION TESTING AND SECURITY ASSESSMENT

Analisi della rete e dell'infrastruttura IT dal punto di vista di un intruso esterno. Assesment delle configurazioni degli apparati, desi sistemi operativi e della rete

Analisi indipendente del livello di resistenza agli attacchi intrusivi della rete

White Box assesment degli OS, database e degli strumenti di sicurezza installati per verificarne l'efficienza

PAYMENT APPLICATION SECURITY TESTING

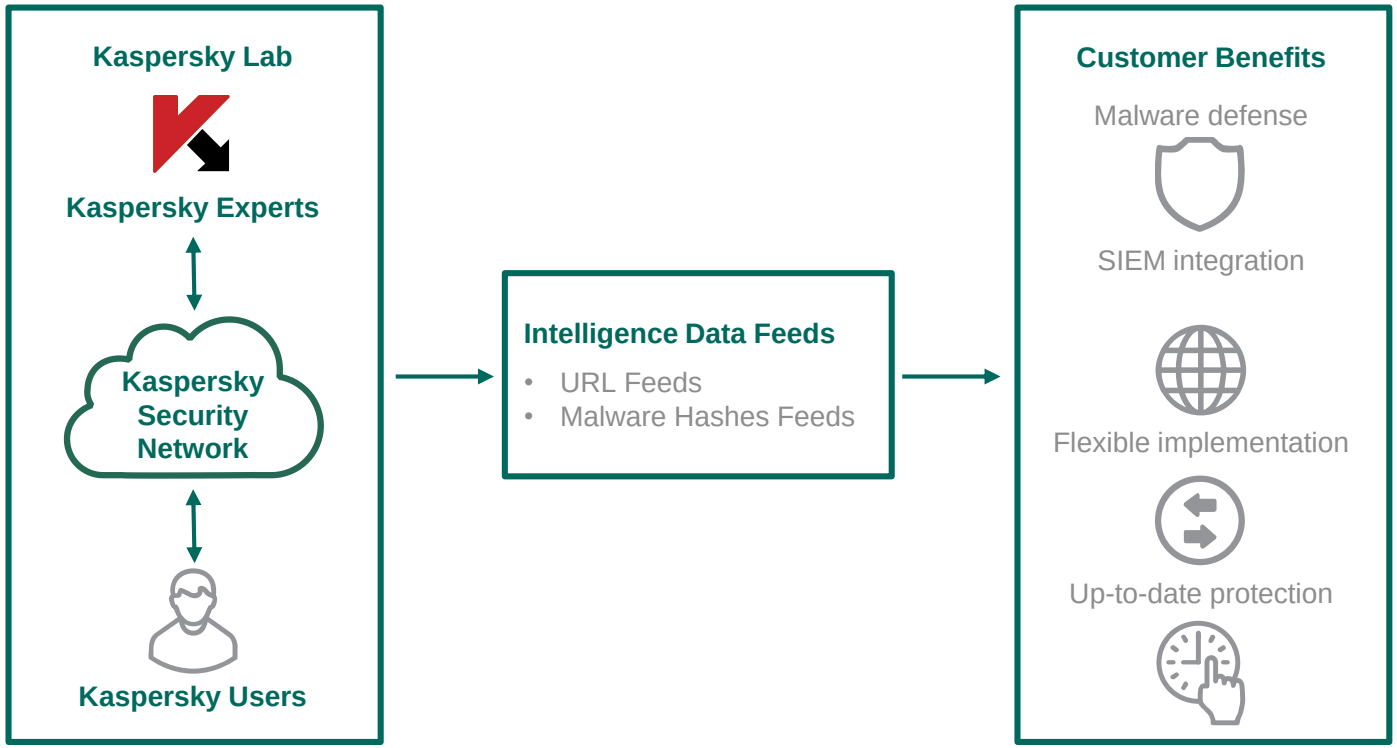
Asssment di Sicurezza indipendente dei sistemi client-server, backend, delle applicazioni Web e mobile.

White-box testing, Grey-box testing e Black-box per rilevare le vulnerabilità e i potenziali attacchi possibili

Raccomandazioni sull'eliminazione delle vulnerabilità rilevate e sugli errori di per aumentare il livello di sicurezza generale

THREAT DATA FEEDS

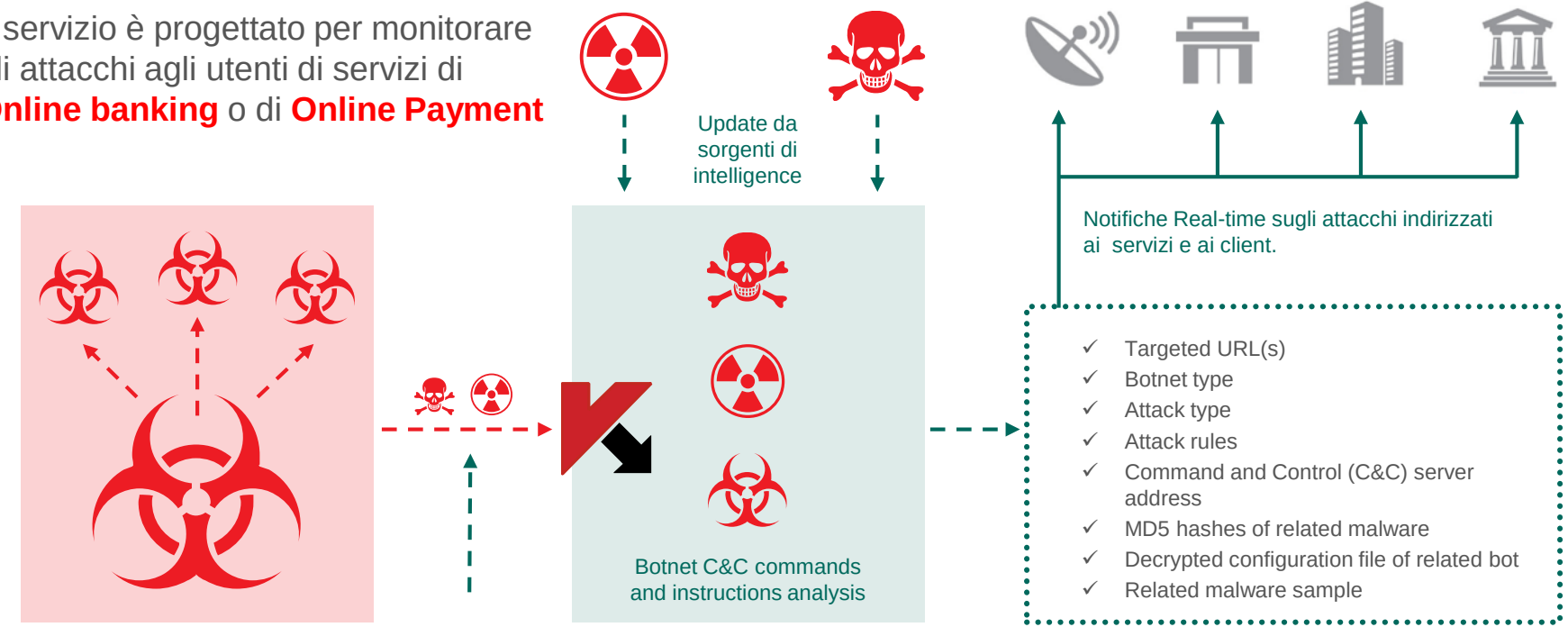
THREAT DATA FEEDS: ARCHITETTURA



BOTNET THREAT TRACKING

BOTNET TRACKING: ARCHITECTURE

Il servizio è progettato per monitorare gli attacchi agli utenti di servizi di **Online banking** o di **Online Payment**



INCIDENT INVESTIGATION

INCIDENT INVESTIGATION: FRAMEWORK

SUCCESS STORIES

SUCCESS STORY

Partnership on foundation forensics center

- **Country** – Singapore
- **Partner** – Interpol

Ongoing subscription to intelligence services

- **Country** – Spain
- **Customer** – Telefonica
- **Scope of Intelligence services** – 1-year subscription to: Feeds, Botnet Tracking, Reports

Paid education services

- **Country – UK**
- **Customer – The City of London Police (COLP)**
- **Training type – Level 2 General Cyberforensics & MA**

GRAZIE

Fabio Sammartino

Pre-sales manager Kaspersky Lab