HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL

FHO Fachhochschule Ostschweiz

COMPASS SECURITY

Cyber Security Kung-Fu

mit Big Data

Vortrag von Ivan Bütler, CEO Compass Security
Lehrbeauftragter der HSR im Fach InfSi3

Cyber Security Kung-Fu

HSR
HOCHSCHULE FÜR TECHNIK
RAPPERSWIL
FHO Fachhochschule Ostschweiz

Kann Big Data helfen, einen Cyber-Angriff zu vereiteln?

Agenda

EDA & RUAG
Swiss Bank
Facebook

APT
E-Banking Trojan
Social Engineering

EDA & RUAG APT

Cyberangriffe aus Moskau

Hinter einem Datenklau beim staatseigenen Schweizer Rüstungskonzern Ruag werden russische Hacker in Staatsdiensten vermutet.

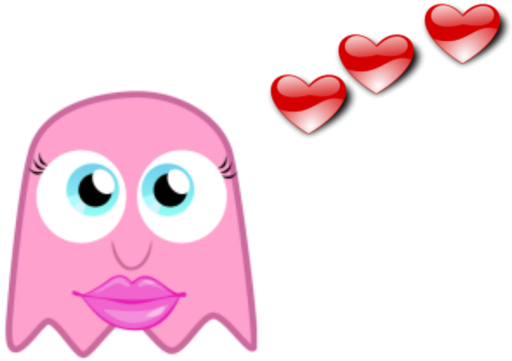
2 | 5 Der NDB hatte bemerkt, dass es seit längerem Attacken auf die Server von Ruag gegeben hatte. Rundgang bei Ruag Space. Bild: Nicola Pitaro

Hacker dringen in EDA-Computernetzwerk ein

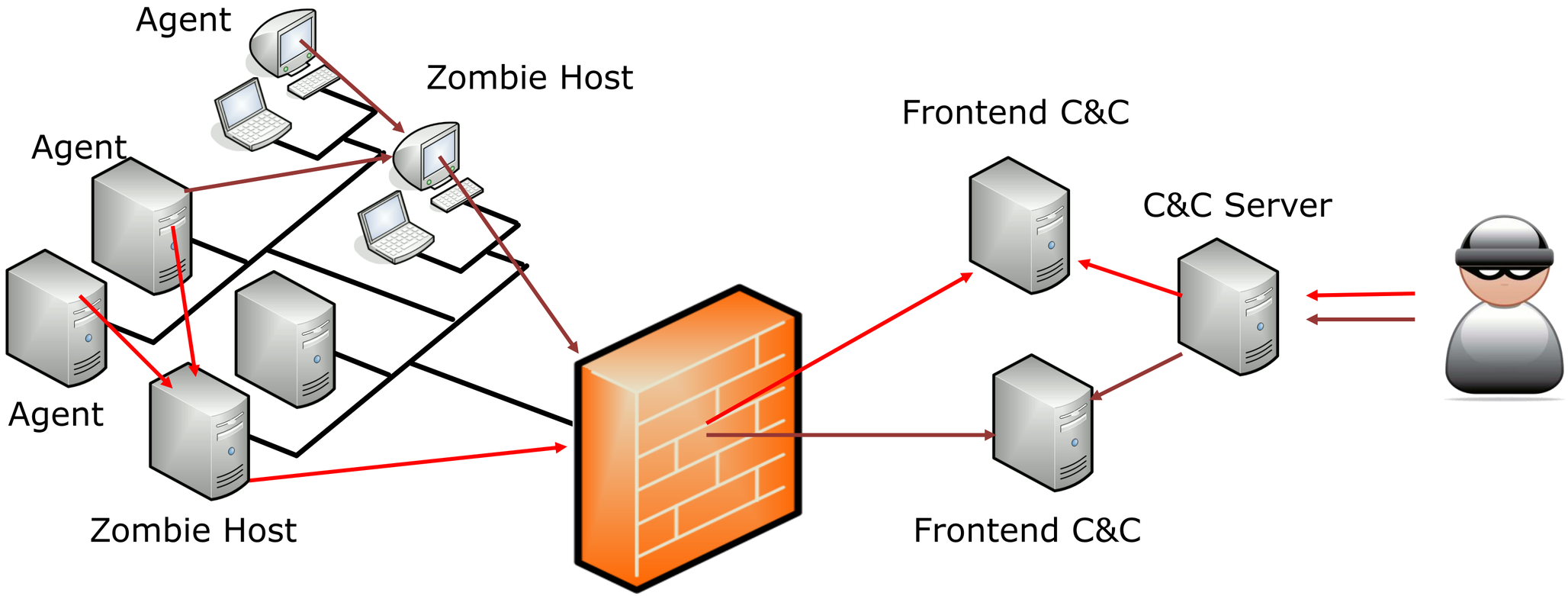
Das Departement für auswärtige Angelegenheiten ist erneut Opfer von Cyberkriminellen geworden: Bereits zum dritten Mal in fünf Jahren haben Unberechtigte auf Daten des EDA zugegriffen – die Täter sind unbekannt.

Quelle: http://www.tagesanzeiger.ch/schweiz/standard/cyberangriffe-aus-moskau/story/10479446

Wie ist das möglich?



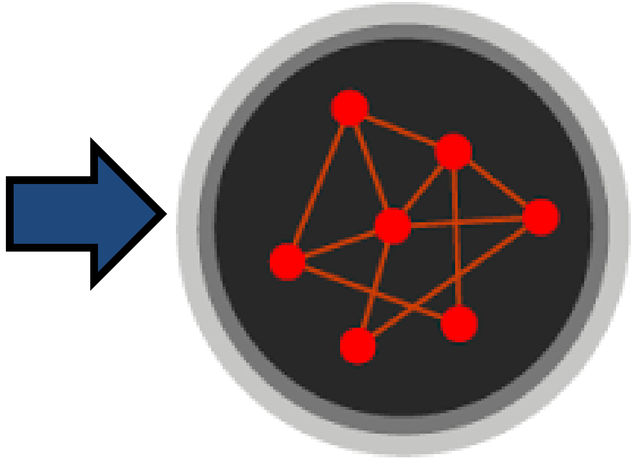
Advanced Persistent Threat (APT)



FIND NETWORK ANOMALY
FIND COMPROMISED CLIENTS
STOP DATA EXFILTRATION

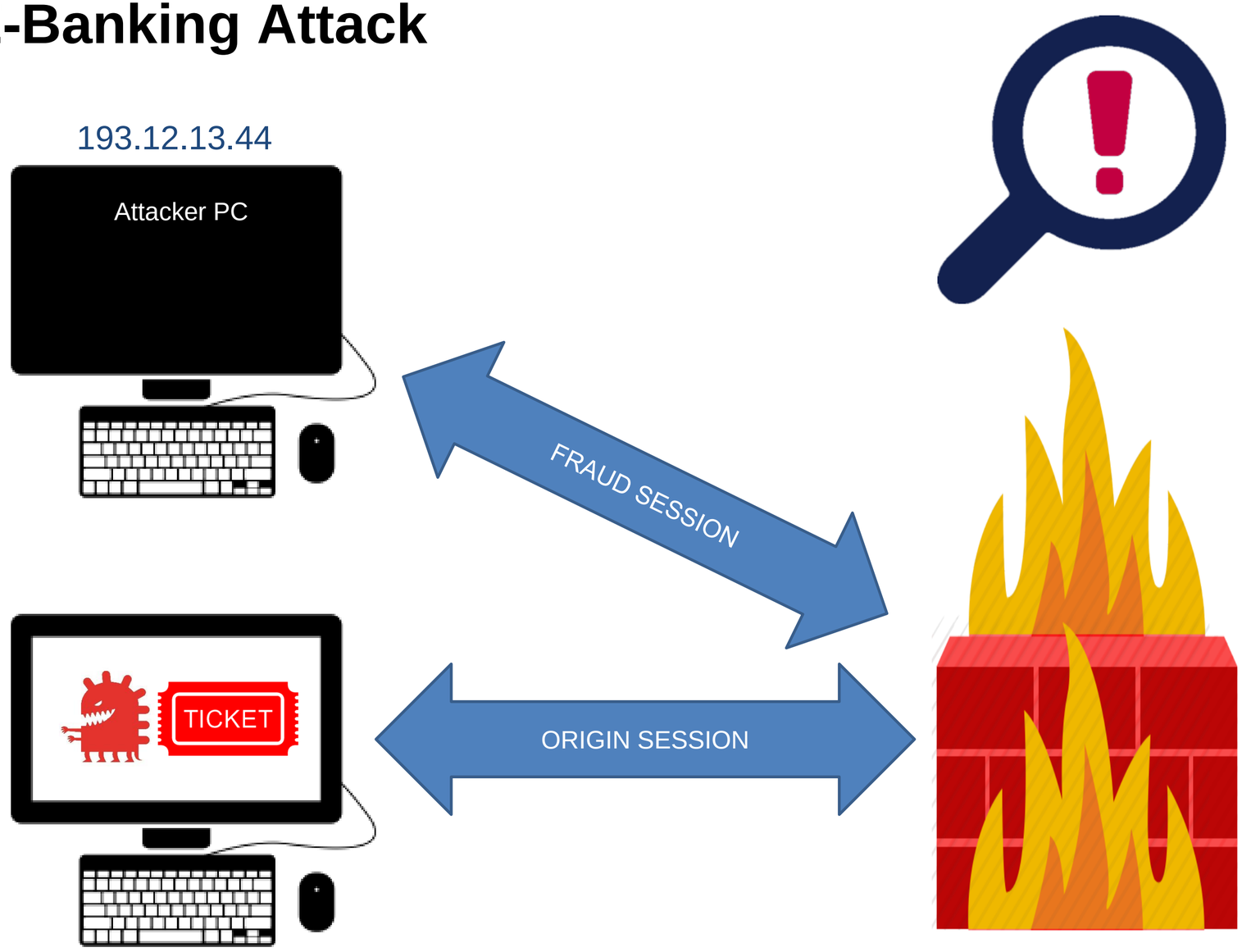
Detection of Compromise (Data Exfiltration)

Internet IOC



Swiss Bank E-Banking Trojan

E-Banking Attack



E-Banking Fraud Detection

Indices of Compromise (IOC)

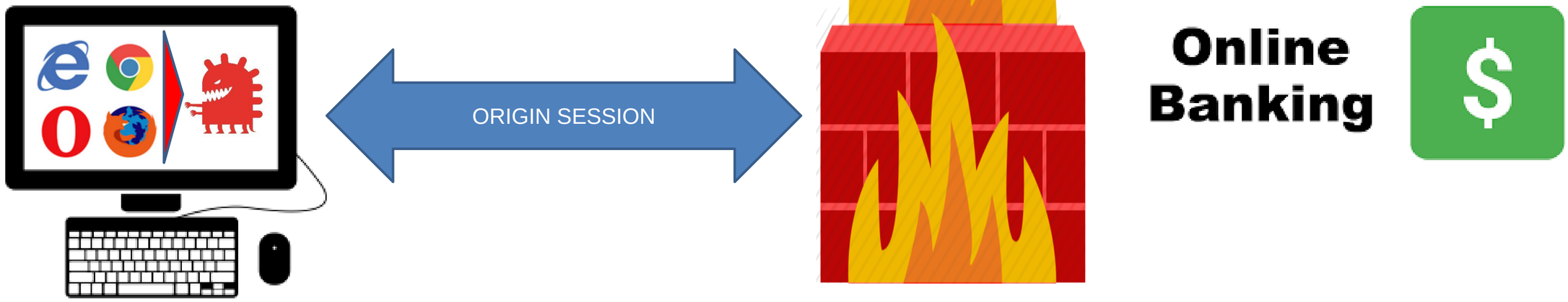
• IP Address	193.12.13.44
• Browser	User Agent
• Screen Resolution	1900x1400
• Browser Fingerprint	{64 char}
• Beneficiary	HSR Ltd.
• Amount	$100’000

Online Banking

Man-in-the-Browser Attack

E-Banking Fraud Detection
Indices of Compromise (IOC)

- Clickstream Analysis
- Outliner Detection
- Keystroke Typing Speed
- URL Frequency Analysis

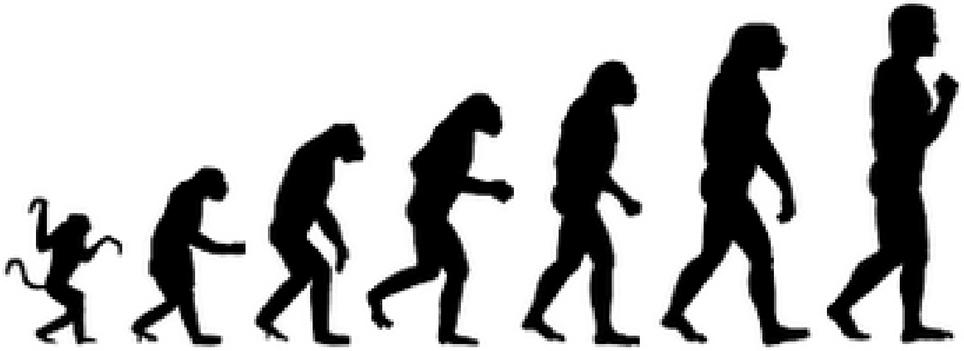


SWIFT 2016 - Bangladesh Bank robbery

Five transactions issued by **hackers**, worth $101 million and withdrawn from a Bangladesh Bank account at the Federal Reserve Bank of New York, succeeded, with $20 million traced to Sri Lanka and $81 million to the Philippines

https://en.wikipedia.org/wiki/Bangladesh_Bank_robbery

Kann Big Data helfen, einen Cyber-Angriff zu vereiteln?



Ja, aber wir stehen noch extrem am **Anfang** und die **Modelldaten** müssen für eine effiziente Nutzung erst generiert und aufgezeichnet werden. Das heissst, es muss noch sehr viel **aufgezeichnet** werden!

Vielen Dank für Ihre Aufmerksamkeit

Ivan Bütler, Compass Security AG
Ethical Hacking & Penetration Testing
Incident Response

ivan.buetler@compass-security.com
https://www.compass-security.com/

InfSi3 Lehrbeauftragter der HSR

ibuetler@hsr.ch