

Moderné hrozby v sieti vyžadujú modernú obranu

Matej Kačic, AEC
18.5.2016

Moderné hrozby - APT

- Pokročilé techniky a stratégie
- Znalosť protiopatrení
- Malware na mieru
- Zero Days zraniteľnosti
- Pretrvávajúca hrozba
- Vysoko motivovaný útočníci

Bezpečnostné prvky

- Firewall + Segmentácia
- NAC
- Application control, IDS/IPS
- Web application firewall
- Patch management
- Hardening
- Anti DoS
- SIEM

Ako vyzerá reálny útok?

- T-48h – Začal prvý DoS, využíval zraniteľnosť webového serveru, IT po 4h útok odrazili
- T-35h – druhý útok DDoS, IT útok neodrazilo, útok skončil po 7,50h
- T-33h – CIO volá o pomoc, inštaluje sa DoS protector
- T-6h – tretí útok DDoS, IT je bezradné
- **T – zverejnený status na Twitteri**
- T+1h – inštalácia DDos protectoru, útok odrazený
- T+2h – pokus o pridanie príspevku na web
- T+3h – DDos skončil

Čo ostalo skryté?

- V čase T-4h odoslal presne 10 emailov na 10 žurnalistov
- Email bol špecifický pre každého žurnalistu
- V emaili bol pokročilý malware
- Malware hľadal heslá a otvorené „sessions“ v IE
- 3 správy boli otvorené (úspešnosť 33%)
- Útočník pridáva správu na twitter a do redakčného systému



Kedy útok skutočne začal?

- Útočník musel veľmi pozorne vybrať svoje obete
- Po analýze sa zistilo, že témy v emailoch riešili 4 – 5 mesiacov pred útokom
- Predpokladáme čas začiatku na úrovni **T-6 mesiacov**
- 11.1 – Zverejnená informácia – podnet na začatie útoku
- 21.1 – čas T – zverejnenie príspevku
- Čo ale rozdiel medzi 21.1.2015 a 11.1.2015 = **10 dní**
- ☺

Stratégia

- Identifikácia zraniteľností
- Identifikácia obetí a informácie o nich
- Príprava útoku a malware
- Test odozvy IT na DoS
- Diverzia v správny okamžik
- Jasný cieľ
- Útok ako reakcia na udalosť



Kto bol obet'?



Le Monde @lemondefr
pic.twitter.com/EKU3ZO1vVU



JE SUIS CHARLIE JE SUIS CHARLIE JE SUIS CHARLIE

ATTENTION

Détails



Le Monde @lemondefr
pic.twitter.com/XELfdxSzT



CHARLIE

Détails



Le Monde @lemondefr
pic.twitter.com/90if2qegst



JE SUIS CHARLIE MANIPULÉ

Détails

Le Monde retweeted

مقربة والتختر @BachMeriem
@lemondefr
pic.twitter.com/1GgkcACPN2



حرية التعبير ليست
ارقى من حرية الدين

Je suis sur la religion de
Muhammad



Le Monde

La France et l'U.R.S.S. ont conclu un traité d'alliance et d'assistance mutuelle

prévu pour une durée de vingt ans

L'ALLIANCE franco-soviétique

Le retour à Paris du général de Gaulle

Le conseil des ministres

TEXTE DU PACTE

Le gouvernement français et le gouvernement soviétique ont conclu un traité d'alliance et d'assistance mutuelle...

TEXTE DES LETTRES ÉCHANGÉES LE 20 SEPTEMBRE 1941

Le gouvernement français et le gouvernement soviétique ont conclu un traité d'alliance et d'assistance mutuelle...

LA PROCHAINE ENTREVUE MOSCOW - CHATELAIN - ARAÏT LIE À ROME

Le général de Gaulle se rendra à Moscou...

A NOS LECTEURS

Chers lecteurs, nous sommes heureux de vous offrir ce journal...

LA CRISE GRECQUE

Les négociations se poursuivent à Athènes...

LA WEHRMACHT CONTRE-ATTAQUE aux confins belgo-luxembourgeois

Dans la plaine d'Alsace l'ennemi s'efforce d'élargir ses positions...

MOSSOLINI CROIT TOUJOURS À LA VICTOIRE DE LUXEMBOURG

Le Führer est en train d'élargir ses positions...

LA vie littéraire

LE GENERAL DE GAULLE ET SES TEMOINS

par Emile Henriot

La Guerre en Extrême-Orient

Attaques multiples contre les Philippines...

Kto útočil?

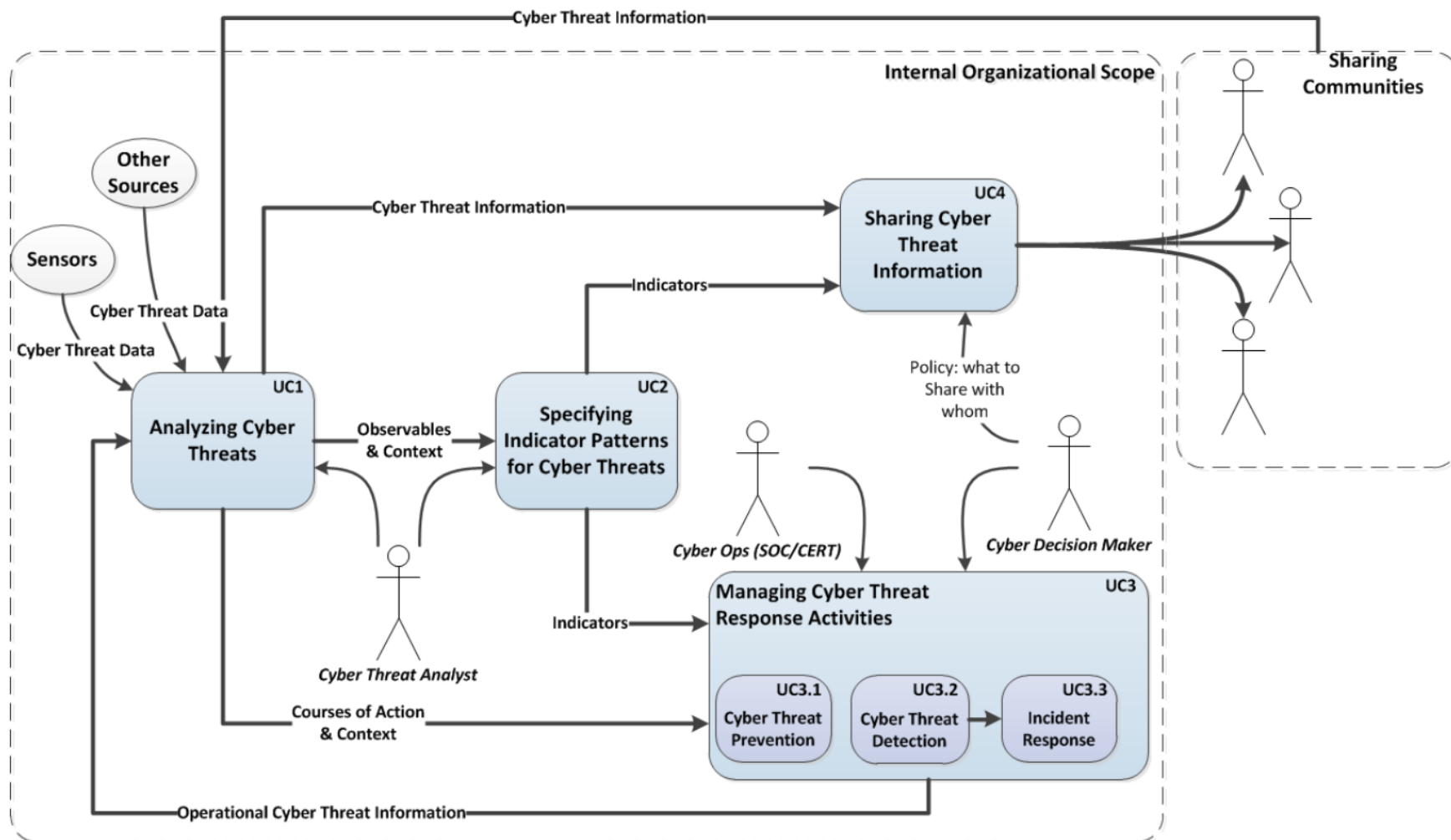


Záchrana v protiopatreniach?

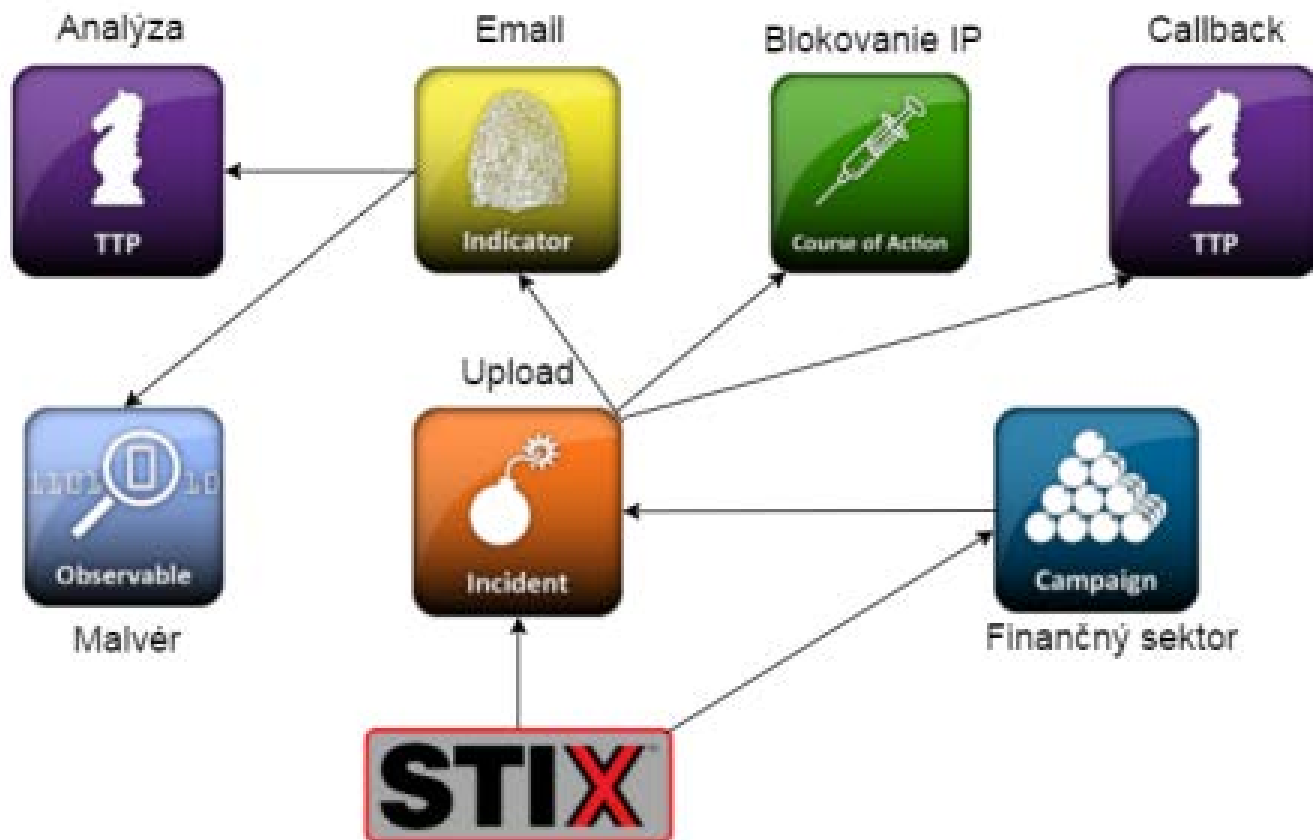
- Nemali Web Application Firewall
- Nemali ochranu proti DoS/DDoS
- Nemali sandbox
- Nemali sieťový monitoring
- Nemali NBA

Pomohli by si?

Moderná ochrana



Príklad modelovania



Príklad modelovania



Slovo záverom

Šťastie praje pripraveným

AEC

Ďakujeme za pozornost

