APT eli kohdistetut hyökkäykset

2.10.2017 Julkisen hallinnon digitaalisen turvallisuuden teemaviikko

Tietoturva- ja kyberturvallisuusluennot

Kohdistetut hyökkäykset

- Kybervakoilu on oleellinen osa tiedustelupalveluiden keinovalikoimaa
- Tavoitteena on yleensä laiton tiedonhankinta
  - » Voi olla myös disinformaation levittäminen tai fyysinen vaikuttaminen
- Hyökkääjän varma tunnistaminen on lähes mahdotonta
  - » Internetissä on helppo peittää jälkensä riittävän hyvin
- Kohteena on erityisesti valtionhallinto
  - » Mutta myös teollisuus ja media, jopa yhteisöt ja yksilöt

Esimerkkejä hyväksikäytettävistä kohteista

Hyökkäyksen toteutuksen vaiheet

Kohdistettujen hyökkäysten menetelmiä

- Menetelmät perustuvat pääasiassa ihmisen huijaamiseen
- Yleisin menetelmä edelleen kohdistetut sähköpostihyökkäykset (spearphishing)
  - » Haitalliset liitetiedostot
  - » Haitalliset linkit

Esimerkki Spearphishing-viestistä 1

Defence iQ CustomerServiceDefenceIC Oct 28 (5 days ago)

to

Väärennetty lähettäjä

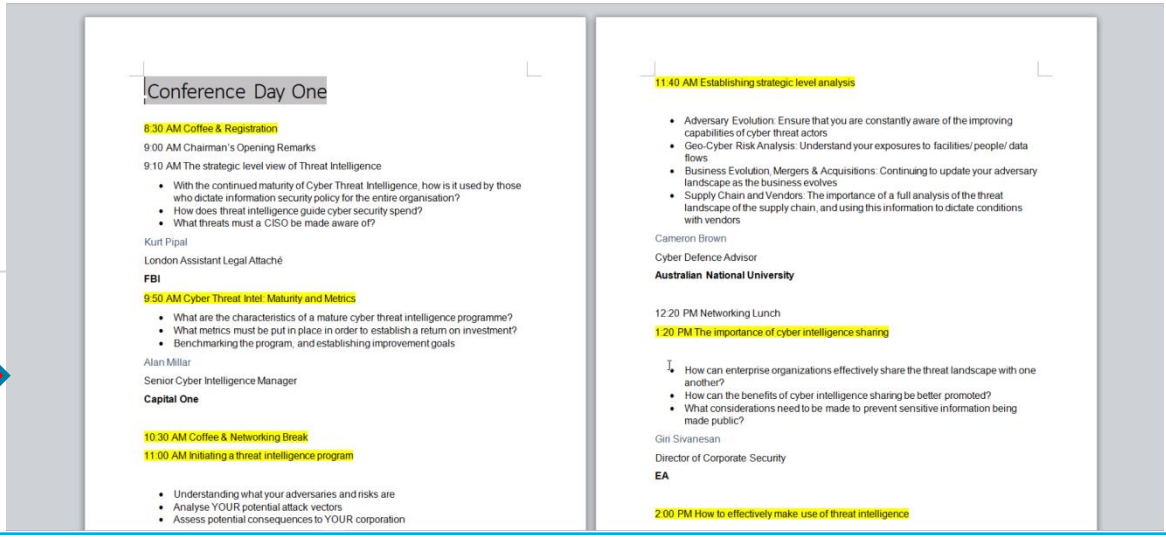
We are pleased to offer you to visit our Cyber Threat Intelligence and Incident Response conference in November.

Mielenkiintoinen aihe

Defence IQ, a division of IQPC
2016 All rights reserved.

Programm_Detail...

Kopioitu dokumentti, johon lisätty haittaohjelma



Conference Day One

8:30 AM Coffee & Registration

9:00 AM Chairman's Opening Remarks

9:10 AM The strategic level view of Threat Intelligence

- With the continued maturity of Cyber Threat Intelligence, how is it used by those who dictate information security policy for the entire organisation?
- How does threat intelligence guide cyber security spend?
- What threats must a CISO be made aware of?

Kurt Pipal

London Assistant Legal Attaché

FBI

9:50 AM Cyber Threat Intel: Maturity and Metrics

- What are the characteristics of a mature cyber threat intelligence programme?
- What metrics must be put in place in order to establish a return on investment?
- Benchmarking the program, and establishing improvement goals

Alan Millar

Senior Cyber Intelligence Manager

Capital One

10:30 AM Coffee & Networking Break

11:00 AM Initiating a threat intelligence program

- Understanding what your adversaries and risks are
- Analyse YOUR potential attack vectors
- Assess potential consequences to YOUR corporation

11:40 AM Establishing strategic level analysis

- Adversary Evolution: Ensure that you are constantly aware of the improving capabilities of cyber threat actors
- Geo-Cyber Risk Analysis: Understand your exposures to facilities/ people/ data flows
- Business Evolution, Mergers & Acquisitions: Continuing to update your adversary landscape as the business evolves
- Supply Chain and Vendors: The importance of a full analysis of the threat landscape of the supply chain, and using this information to dictate conditions with vendors

Cameron Brown

Cyber Defence Advisor

Australian National University

12:20 PM Networking Lunch

1:20 PM The importance of cyber intelligence sharing

- How can enterprise organizations effectively share the threat landscape with one another?
- How can the benefits of cyber intelligence sharing be better promoted?
- What considerations need to be made to prevent sensitive information being made public?

Giri Sivanesan

Director of Corporate Security

EA

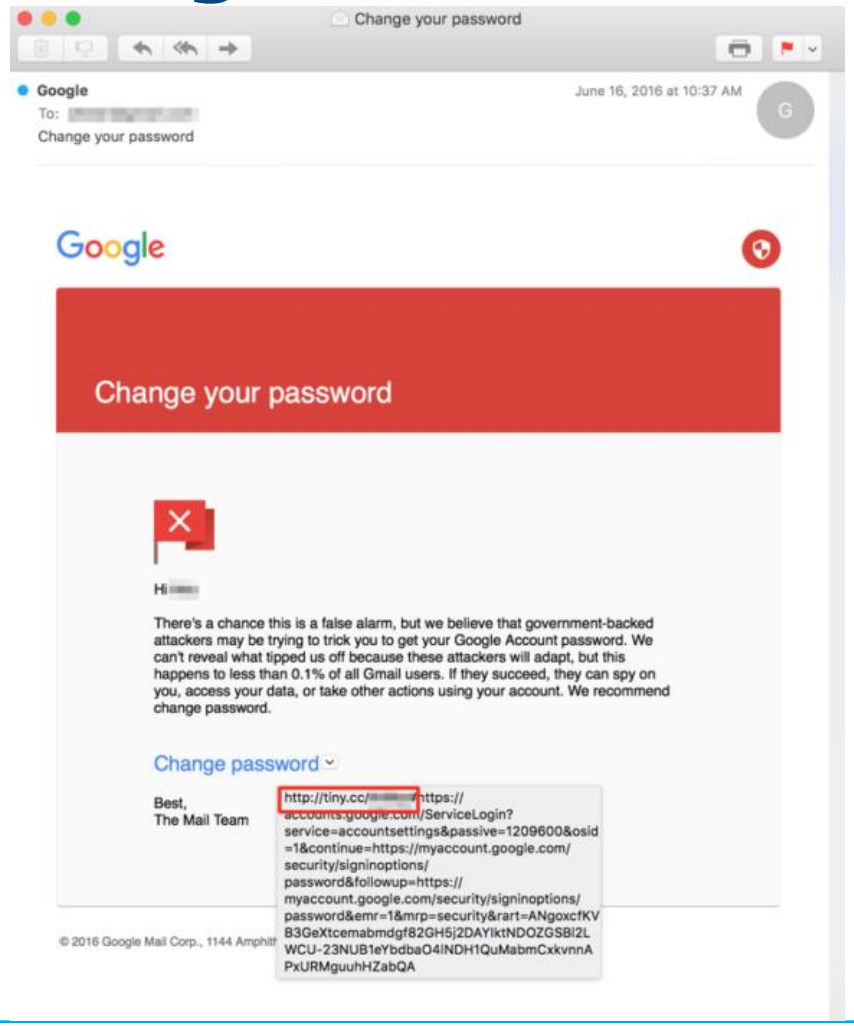
2:00 PM How to effectively make use of threat intelligence

Esimerkki Spearphishing-viestistä 2

Lähettäjäksi väärennetty Google

Vakooja käyttää Googlen varoitustekstiä vakoojista

Salasananvaihtolinkki vie väärennetylle sivustolle

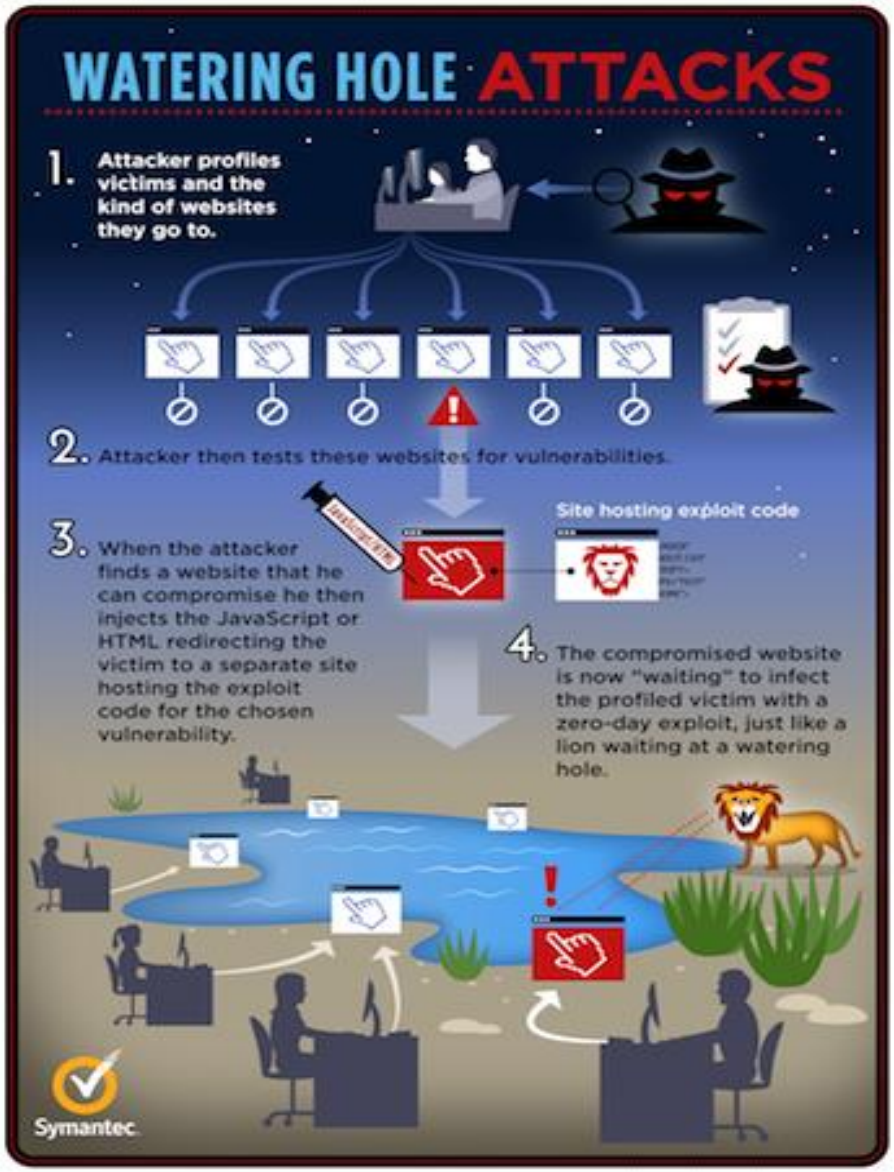


Kohdistettujen hyökkäysten menetelmiä

- Kirjautumisia etäkäyttöpalveluihin varastetuilla tunnuksilla
  - » VPN, Microsoft Outlook Web Access (OWA), Webmail
- Myös murrettuja sivustoja hyväksikäytetään (Watering Hole)

Murretut sivustot

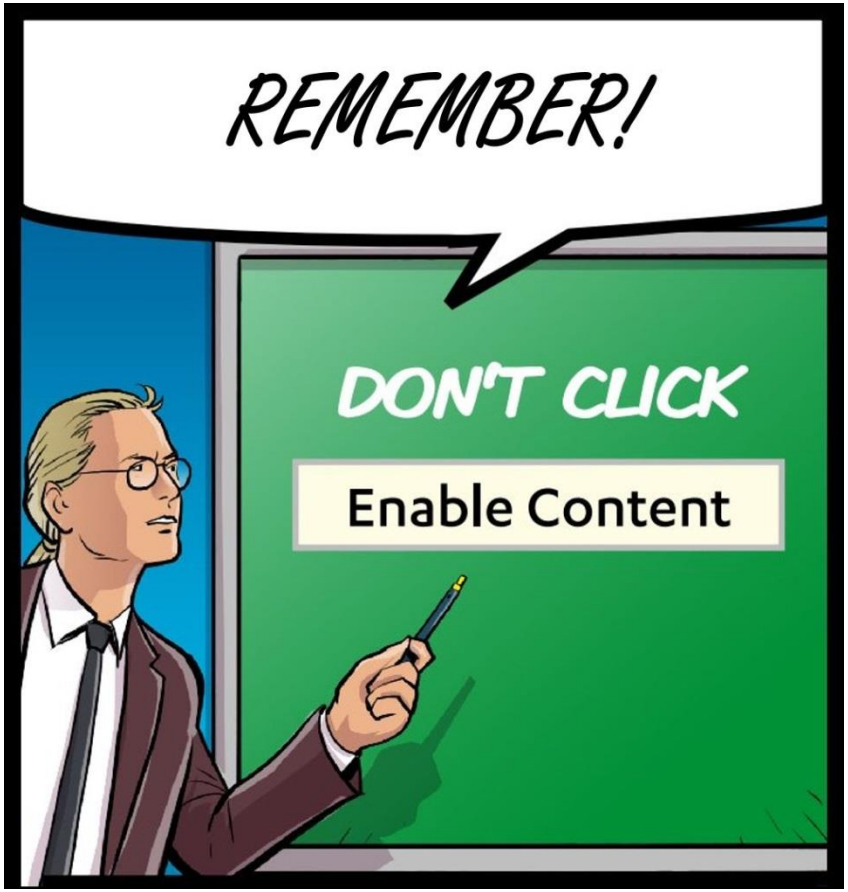
- Työhön liittyvät sivustot
  - » Valtiollinen
  - » Ammatillinen
- Järjestöjen sivustot
  - » Tutkimusorganisaatiot
- Harrastussivustot



Vastuita

- **Organisaation tietohallinto**
  - » Selvityksen käynnistäminen
  - » Organisaatiokohtaiset toimenpiteet
  - » Viranomaisille ilmoittaminen
- **Kyberturvallisuuskeskus**
  - » Tietoturvaloukkausepäilyn vahvistaminen
  - » Teknisen selvityksen avustus
- **Suojelupoliisi**
  - » Valtiollisen vakoilun rikostutkinta
- **Tietoturvayritykset**
  - » Tekninen apu tapauksen selvittämiseen

Miten käyttäjän tulisi toimia?



Twitter 18.11.2016: @mikko

Mitä käyttäjän pitää muistaa?

- Muista vastuusi omasta laitteestasi
- Mieti, ennen kuin klikkaat
- Noudata oman organisaatiosi ohjeita
- Ilmoita, jos huomaat jotain epäilyttävää

Havainnoista ja epäilyistä ilmoittaminen

- Jos havaitsette tietoturvaloukkauksen, kertokaa siitä meille
- Jos epäilette tietoturvaloukkausta, ottakaa meihin yhteyttä
- Jos teillä on kysyttävää kyberturvallisuudesta, kysykää meiltä
- Sähköposti cert@ficora.fi tai cert@viestintavirasto.fi
- Yhteydenottolomake https://www.viestintavirasto.fi/asioikanssamme/yhteydenotto.html
- Arkisin kello 9.00–15.00 voi myös soittaa numeroon 0295 390 230

Viestintävirasto
Kyberturvallisuuskeskus

www.kyberturvallisuuskeskus.fi
www.viestintävirasto.fi