SECIT
security consulting

ESIGURNOST
INFORMATION
SECURITY

Social Engineering - a Risk You Can't Ignore

CIO Leadership Forum
Zlatibor, Hotel Cigota, September 27th, 2019

Prof dr Igor Franc
Predavač | Digitalni forenzičar | Etički haker | Preduzetnik

Sadržaj

- Uticaj ljudskog faktora
- Profesionalizacija cyber kriminala
- War dialing
- War driving
- Phishing
- Road apple
- Impersonation

SECIT
security consulting

Uticaj ljudskog faktora

- Ljudski faktor je uzrok **više od 75%** bezbednosnih incidenata. Velika većina ovih incidenata nastala je slučajno, jer zaposleni nisu svesni posledica svojih (obično bezopasnih) akcija.
- Zato je važno **da svako razume** šta su verovatne pretnje po imovinu i kompletno poslovanje preduzeća i kako da pravilno delujemo da se smanje rizici svojstveni tim pretnjama.

SECIT
security consulting

Profesionalizacija cyber kriminala

```
General options
---------------
 --install: install server on local host and load it
 --host <host>: hostname or IP (local host if not set)
 --password <password>: server password connection (mandatory)
 --forceload: load server on local host without test

Server options
--------------
 --cmd: server command:
    dump: dump stuffs
       --sam: fetch LM/NTLM hashes
       --machines: fetch machines hashes
       --history: fetch history for LM/NTLM hashes
       --nh: fetch logon sessions hashes
       --sp: fetch security packages cleartext passwords
       --accounts: <account list>: with --sam, specify accounts to dump
(comma separated)
       --lsa: fetch LSA secrets
```

SE na delu

- War dialing
- War driving
- Phishing
- Road apple
- Impersonation

Sve je počelo sa fiksnim telefonima -War dialing

Nastavilo se WiFi mrežama
War driving

Phishing

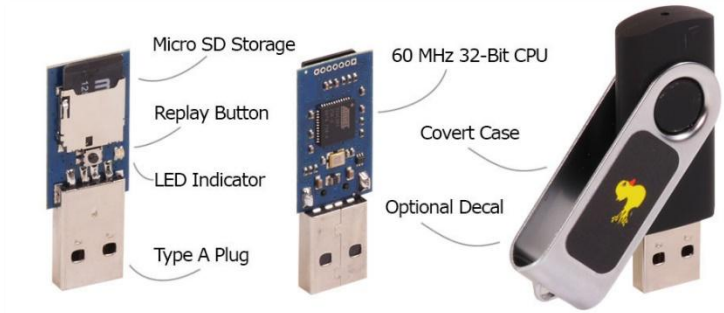
- Phishing ili u prevodu pecanje jeste upravo to
- Prevara korisnika da bi se došlo do šifri, PIN brojeva i slično
- Stigli smo na treći način prevare korisnika preko lažnih mailova web stranica

Novi kanal prevare je sada USB

- Tehnika koja se bazira na neupućenosti ili nepažnji
- Na parkingu firme ostavljen USB koji zaposleni uzima...

SECIT
security consulting

USB Rubber Ducky



SECIT
security consulting

Bash Bunny

Introducing the Bash Bunny

The world's most advanced USB attack platform.

- Quad Core CPU
- Desktop-Class SSD
- Full Linux Distribution
- Payload Select Switch
- RGB LED Status Indicator
- Plug to Pwn in 7 Seconds

Advanced Attacks

- Driverless Multi-Gigabit Ethernet
- Fast USB 2.0 Storage
- Keystroke Injection
- Dedicated Serial Console

Simple Payloads

- Extendable Bunny Scripting Language
- Centralized Payload Library

BashBunny.com

Impersonation

- Prerušavanje u nekog drugog (rukovodioca, novog radnika)
- Ovde se uglavnom radi o navođenju čoveka na neku akciju

SECIT
security consulting

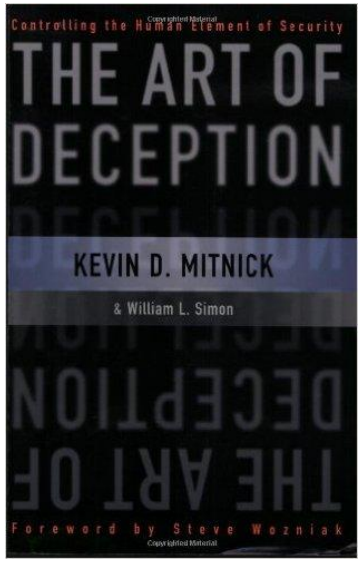
Žika i trgovinski lanac

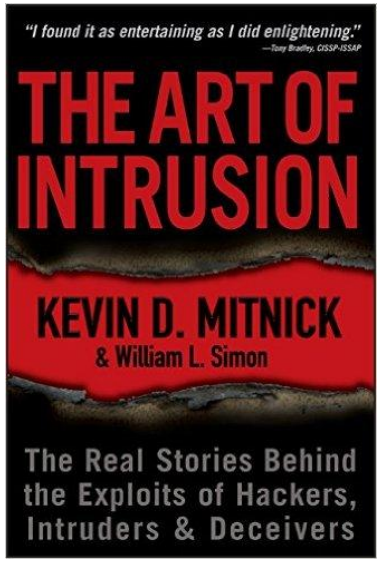
SECIT
security consulting

ESIGURNOST
INFORMATION
SECURITY

Opšte ludilo popularizacije društvenih mreža dovelo je do SE na društvenim mrežama

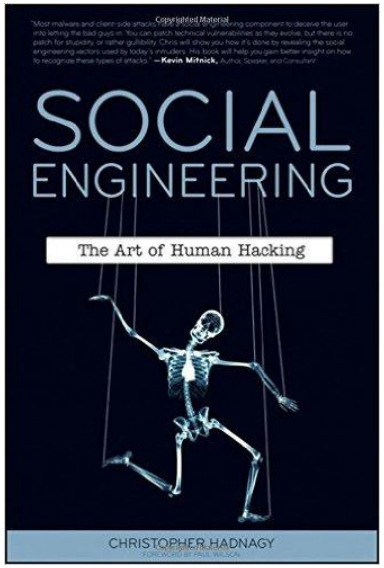
Kevin D. Mitnick

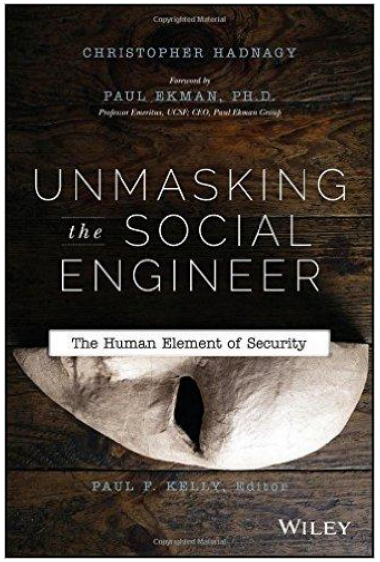




- Pionir socijalnog inženjeringa
- Sajt njegove firme

Christopher Hadnagy





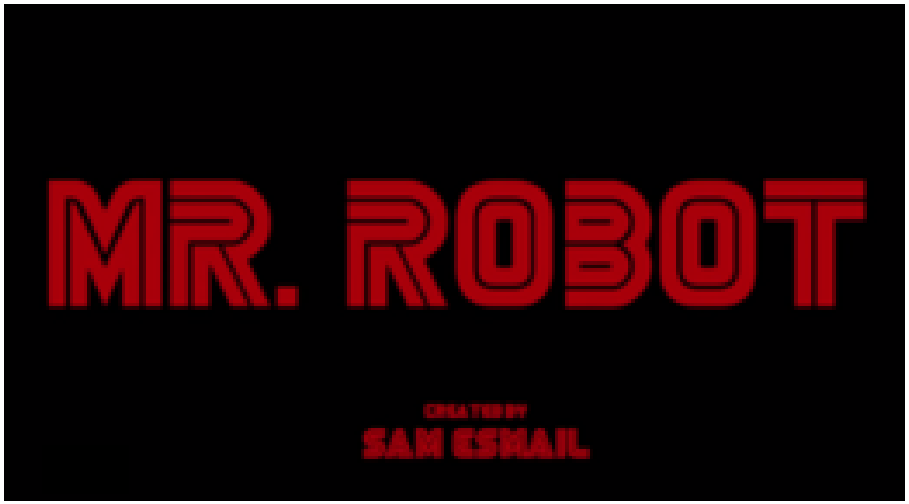
- Jedan od najvećih stručnjaka u ovoj oblasti
- Njegov sajt

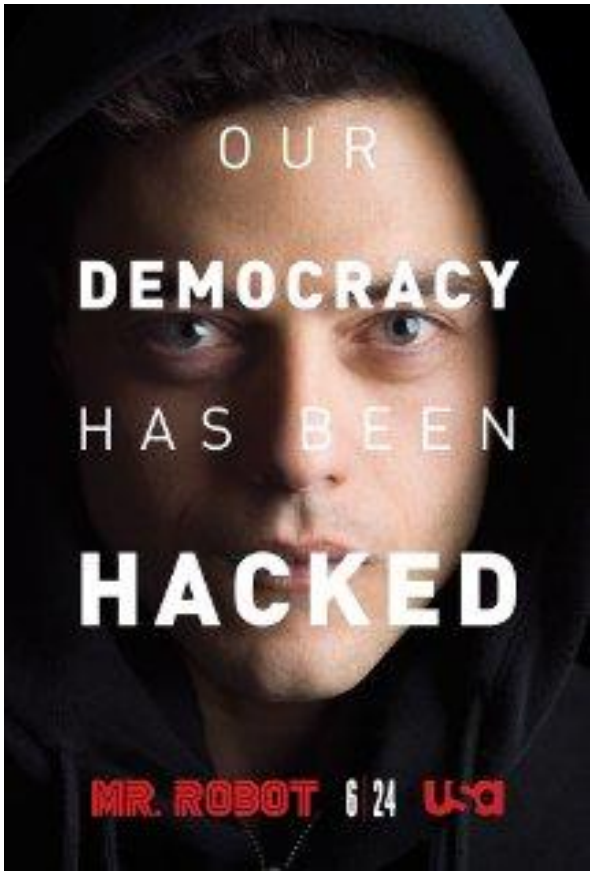
Social Engineer Toolkit

```
 The Social-Engineer Toolkit is a product of TrustedSec.

           Visit: https://www.trustedsec.com

Select from the menu:

   1) Social-Engineering Attacks
   2) Fast-Track Penetration Testing
   3) Third Party Modules
   4) Update the Metasploit Framework
   5) Update the Social-Engineer Toolkit
   6) Update SET configuration
   7) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set> 1
```

- Zvaničan sajt

Mr Robot





- IMDB serije
- Trailer

Zaključak

- Najefikasnija mera zaštite
- Treba je kontinualno obavljati a na periodično

SECIT
security consulting

Demo

ESIGURNOST
INFORMATION
SECURITY

HVALA NA PAŽNJI!

Kontakt podaci:

- Mail: ifranc@secitsecurity.com , ifranc@esigurnost.org
- Web: http://secitsecurity.com , http://esigurnost.org
- Twitter: https://twitter.com/francigorbg
- LinkedIn: https://rs.linkedin.com/in/ifranc