Prepoznavanje štetnih web sjedišta u sklopu kataloga www.hr

Valter Vasić, *Marin Vuković*

valter.vasic@fer.hr

Sveučilište u zagrebu, Fakultet Elektrotehnike i Računarstva

Sadržaj

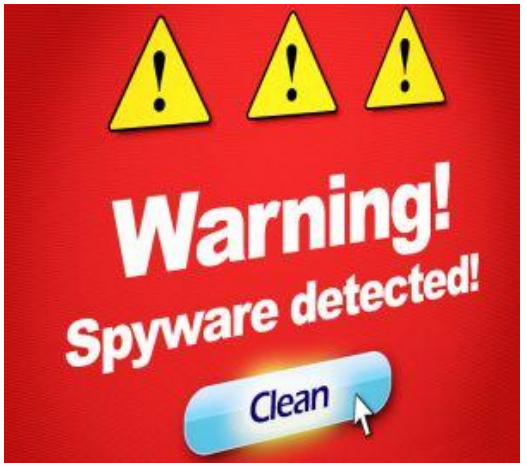
- Uvod
- Definicija štetnih web sjedišta
- Podjela štetnih web sjedišta
- Posljedice pristupa štetnim web sjedištima
- Prepoznavanje štetnih web sjedišta
- Sprečavanje pristupa štetnim web sjedištima
- Zaključak

Uvod

- Rast štetnih web sjedišta
- Zaražena računala šire zarazu
- www.hr katalog
  - Postoji 17 godina
  - Velik broj zaraženih web sjedišta
  - Namjerno dodavanje štetnih web sjedišta
- Sustav za prepoznavanje i sprečavanje dodavanja štetnih web sjedišta

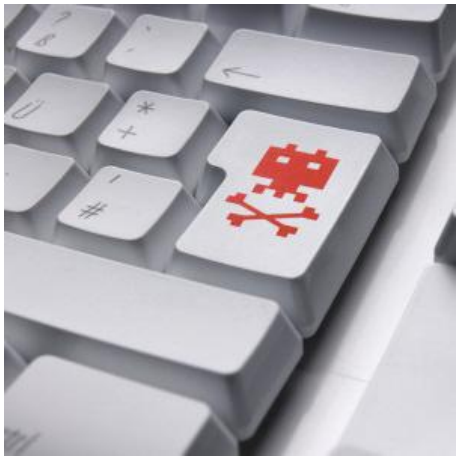
Štetna web sjedišta

- Podjela:
  - Sjedišta za dijeljenje ilegalnog sadržaja
    - *torrent* datoteke ili poveznice prema stranicama za dijeljenje sadržaja
  - Sjedišta sa lažnim bankarskim uslugama
    - glume sjedišta banke kako bi došle do povjerljivih podataka
  - Sjedišta sa lažnim uslugama uklanjanja štetnog softvera
    - lažno prikažu postojanje štetnog softvera
    - nude dohvaćanje programa koji je zapravo maliciozni softver



Posljedice pristupa štetnim web sjedištima

- Pokretanje neželjenog softvera na računalu
  - Omogućuje kontrolu računala
    - DDoS, e-mail spam, prisluškivanje prometa, krađa lozinki, krađa identiteta
- Krađa lozinke i podataka o kreditnim karticama
  - Imitacija net-bankinga
- Pretplata na reklamne e-mail poruke
  - Lažne prilike za zaposlenje, …



Prepoznavanje štetnih web sjedišta

- Podjela:
  - Pregledavanje i kontrola koda
    - JavaScript, reklame, flash animacije
    - Velik broj poveznica → imitacija drugog sjedišta
  - Web adresa sjedišta
    - http://net.banka.hr
    - http://net.banka.hr.account-update.com
  - Korištenje baza podataka sa štetnim web sjedištima
    - Google Safe Browsing, StopBadware

JavaScript - primjer skrivanja koda

Običan JavaScript kod	Izmijenjen JavaScript kod

function Cart(){
  this.citems=new Array();
  this.numberOfItems=0;
}
Cart.prototype.addCartItem =(citem){
  this.citems[this.numberOfItems++]
=citem;
  alert(citem.name+"added to cart");
}
	function t(){
	  this.v=new Array();
	  this.c=0;
	}
	t.prototype.E=function(D){
	  this.v[this.c++]=D;
	  alert(D.name+"\141\144\144\145\144
	  \164\157\143\141\162\164");
	}

Korištenje baza podataka

- Projekti za suzbijanje štetnih web sjedišta
  - Google Safe Browsing
    - Je li sjedište sumnjivo?
    - Što se dogodilo kad je Google posljednji put posjetio sjedište?
    - Je li sjedište štetno i širi li štetan softver?
    - Je li sjedište sadržavalo poveznice prema štetnom softveru?
  - StopBadware

Google - www.fer.hr

Safe Browsing
Diagnostic page for www.fer.hr

Advisory provided by Google

What is the current listing status for www.fer.hr?

This site is not currently listed as suspicious.

What happened when Google visited this site?

Of the 50 pages we tested on the site over the past 90 days, 0 page(s) resulted in malicious software being downloaded and installed without user consent. The last time Google visited this site was on 2011-07-23, and suspicious content was never found on this site within the past 90 days.

This site was hosted on 1 network(s) including AS2108 (CARNET).

Has this site acted as an intermediary resulting in further distribution of malware?

Over the past 90 days, www.fer.hr did not appear to function as an intermediary for the infection of any sites.

Has this site hosted malware?

No, this site has not hosted malicious software over the past 90 days.

Next steps:

- Return to the previous page.
- If you are the owner of this web site, you can request a review of your site using Google Webmaster Tools. More information about the review process is available in Google's Webmaster Help Center.

Updated 2 hours ago

Google - hygicare.nl

Safe Browsing
Diagnostic page for hygicare.nl

Advisory provided by Google

What is the current listing status for hygicare.nl?

Site is listed as suspicious - visiting this web site may harm your computer.

Part of this site was listed for suspicious activity 3 time(s) over the past 90 days.

What happened when Google visited this site?

Of the 1123 pages we tested on the site over the past 90 days, 50 page(s) resulted in malicious software being downloaded and installed without user consent. The last time Google visited this site was on 2011-07-27, and the last time suspicious content was found on this site was on 2011-07-23.

Malicious software includes 121 scripting exploit(s), 3 trojan(s). Successful infection resulted in an average of 4 new process(es) on the target machine.

Malicious software is hosted on 60 domain(s), including personalpgpmaster.findhere.org/, strongsentinelrw.tk/, 188.229.90.0/.

38 domain(s) appear to be functioning as intermediaries for distributing malware to visitors of this site, including top-weholder.findhere.org/, 188.229.89.0/, personalpgpmaster.findhere.org/.

This site was hosted on 1 network(s) including AS38930 (FIBERRING).

Has this site acted as an intermediary resulting in further distribution of malware?

Over the past 90 days, hygicare.nl did not appear to function as an intermediary for the infection of any sites.

Has this site hosted malware?

No, this site has not hosted malicious software over the past 90 days.

How did this happen?

In some cases, third parties can add malicious code to legitimate sites, which would cause us to show the warning message.

Next steps:

- Return to the previous page.
- If you are the owner of this web site, you can request a review of your site using Google Webmaster Tools. More information about the review process is available in Google's Webmaster Help Center.

Updated 1 hours ago

Sprečavanje pristupa web sjedištima

1. Početna detekcija pomoću baza podataka

2. Postavljanje sustava za detekciju štetnih web sjedišta

3. Prijava novih štetnih sjedišta u baze podataka

4. Stvaranje nove kategorije zabranjenih web sjedišta

5. Onemogućen unos štetnih sjedišta i bolji katalog

Zaključak

- Zbog vjerodostojnosti potrebno je ukloniti štetna web sjedišta iz kataloga
- Pregled napada i načina borbe protiv napada
- Rješenje u obliku sustava
  - Uklanjanje postojećih štetnih sjedišta
  - Provjera prilikom unosa sjedišta
- Bolji katalog uz jednostavnije održavanje