

IAB mainonnan työryhmä

Flash-haittaohjelmat

Mitä tehdä, kun viruksia levitetään miljoonille verkkomainoksien katsojille?

media
reaktori

Olli Erjanti

13.5.2008

Mediareaktori Oy

- Perustettu 2001, liikevaihto ~350 t e, 11 työntekijää
- Verkkomainonta
 - Verkkomainonnan trafikointi ja tekninen konsultointi
 - Mainosten toteutus
- Visuaalinen tuotanto
 - AV-tuotanto, graafinen suunnittelu
- Verkkotuotanto
 - Digitaalisten kokonaisuuksien suunnittelu ja toteutus

Flash-haittaohjelmat mainosbannereissa

1. Flash-haittaohjelmat
2. Ennaltaehkäisy
3. Kriisitoiminta
4. IAB:n rooli

1. Flash-haittaohjelmat mainosbannereissa

- Maailmalla viime syksystä, Suomessa tänä keväänä
- Aktivoituu
 - Kun mainosta katsotaan selaimella
 - Avaa linkin haittaohjelmisivustoille (valevirustorjunta)
- Pahantahtoinen
 - Piilotettu
 - Suunnattu suomalaisiin verkkomedioihin suomen kielellä
- Verkkomediat levittävät
 - Pahimmillaan miljoonille käyttäjille
 - Leimaa verkkomedian levittäjäksi

1. Flash-haittaohjelmat historia

- Flash saastuttaa muita flashejä
 - 2002: SWF.LFM.926 virhe korjattu
- Bufferin ylivuoto
 - 2006: Koneen täydellinen kaappaus, virhe korjattu
- Tietokalastelu
 - 2007: Naamioitu PayPal flash
- **Linkin avaus haittasivuille mainosbannerista**
 - Syksy 2007 maailmalla, Suomessa kevät 2008
 - Ei voida estää
 - Aktivoituu: kaikki käyttöjärjestelmät, kaikki selaimet
 - Kuuluu Flashin perusominaisuuksiin, vrt. sandbox
- Kriittinen haavoittuvuus
 - Huhtikuu 2008
 - Mahdollistaa tietokoneen haltuunoton hyökkääjän toimesta
 - Tietoturvapäivitys uudessa Flash-player versiossa (9.0.124.0)

2. Ennaltaehkäisy

- Ei varmaa torjuntakeinoja
 - Paitsi adblockerit (ei lainkaan mainoksia)
 - Virusskannerit eivät tunnista selaimessa olevaa mainosta
 - F-Secure paikallisella levyllä: *Trojan:SWF/.Redir.A*
 - Selainskanneri, palvelin- tai välityspalvelinskanneri
 - Mainonnanhallintajärjestelmät
- Epäilyttävää
 - Ulkomailta, pieni mainostaja, Eurooppa, Kanada
 - Mainostajan ensimmäinen kampanja
 - Hirveä kiire
 - Maksuosoitetta tai tapaa muutellaan viime tingassa
 - Laskua ei koskaan makseta
 - Asiakkaaseen ei saada yhteyttä

2. Ennaltaehkäisy

- **Olkaa tarkkana!**
- Käyttäjäpalautteen aktiivinen seuranta
- Henkilökunnan koulutus ja ohjeistus
- Epäilyttävien aineistojen käsin skannaus ja tarkistus
- Aineisto-ohjeisiin kiello piilotetusta flash-koodista
 - Koodin häivitys (obfuscation) kielletty
- Windows-käyttöjärjestelmän / antivirusohjelmien päivitykset ajan tasalla

3. Kriisitoiminta

- Medialle erittäin arkaluontoinen asia
 - Saastutetaan pahimmillaan satojatuhansia tai miljoonia koneita (Suomessa)
 - Vastuu- ja korvauskysymykset
- Kriisitiedotus ja -johto
 - Kriisiryhmä
 - Saastunen kampanjan tunnistus ja poisto
 - Tilanteen vakavuuden arviointi esim.
 - Vakava uhka
 - Suoria taloudellisia haittoja, tietokalastelu, koneen haltuunotto
 - Haitallinen
 - Imagohaittoja, palvelunestohyökkäykset
 - Väärä hälytys
 - Tiedotus

3. Tietoturvaverkosto

- www.cert.fi viestintävirasto
 - Ilmoitus nimettömänä eteenpäin
 - Apua tilanteen vakavuuden arvioinnissa
 - Tarvitaanko poliisitutkinta?
 - Ylittykö yleisen viestinnän kynnys?
- www.poliisi.fi
 - KRP keskus (09) 8388 661
 - Tietotekniikkarikoksien ryhmä (Vantaa)
 - Rikosilmoitus paikalliselle poliisilaitokselle
- Onko vastuu vahingoista viruksen tekijällä vai levittäjällä?

4. IAB:n rooli

- Mainosbannerivirukset yleistyvät tulevaisuudessa
 - Ammattimaisen rikollisuuden ja virustehtailijan unelmajakelukanava
 - Roskaposteja osataan varoa, verkkomainontaa ei
 - Uhkaa ei pystytä kokonaan torjumaan lopettamatta verkkomainontaa
 - Suuri imago-ongelma medialle ja mainostajalle
- Puolueeton osapuoli
 - Yleinen tiedotus
 - Tapausten nimetön kirjaus
 - Luotettavat tägitoimittajat?
 - Ohjeistus, koulutus, suositukset

4. IAB:n rooli

- Verkkomedioiden käyttöehdot

- Tietosuoja

- Korvausvelvollisuus

- Hyvä esimerkiksi:

”Helsingin Sanomat tai sen lisenssinantajat eivät missään olosuhteissa vastaa mahdollisista vahingoista, jotka aiheutuvat käytettävälle tietokonejärjestelmälle tai siinä oleville tiedoille mukaan lukien tietoturvallisuusriskit (virukset, tietovarkaudet yms).”

<http://www.hs.fi/kayttoehdot/> 25.3.2008

(esimerkki ei liity mitenkään tämän esityksen virustapauksiin)

Linkkejä

- Tapauksia maailmalla

- (Huomioi, että ongelma on yleinen, ei vain DoubleClickin)
- <http://consumerist.com/consumer/badvertising/flash+based-malware-ad-sneaks-onto-legitwebsites-via-doubleclick-323718.php>
- <http://www.wired.com/techbiz/media/news/2007/11/doubleclick>
- <http://click.comms.doubleclick.com/?ju=fe5d15777d61047b7315&ls=fdf815737464027c7c1479fdf815737464027c7c14797c&m=fef91175736402&l=fec71574766c017e&s=fe2e15787264017d741778&jb=ffcf14&t=>
- http://blog.washingtonpost.com/securityfix/2006/07/myspace_ad_served_adware_to_mo.html

- Flash ActionScriptin piilotustekniikka

- <http://pentaphase.de/index.php?/archives/28-SWF-in-a-nutshell-and-the-malware-tragedy.html>

- Flash-tietoturvakysymyksiä

- https://www.flashsec.org/wiki/Main_Page

- Palvelinpuolen flash-monitori

- <https://www.owasp.org/index.php/Category:SWFIntruder>

Kiitos!

Lisätietoja:

Olli Erjanti, Mediareaktori, palvelupäällikkö

oli.erjanti@mediareaktori.fi

040 501 9770

www.mediareaktori.fi