

# Virustrendit ja virustorjunnan haasteet

- **Päätrendi:** siirto harrastajapainotteisesta viruslevittäjästä ammattilais- ja gangsteritoimintaan.
- **Päämotiivi:** RAHA.
- **Keinot:** VERKKO kaikissa toimintamuodoissa: webbiserverit, sähköposti, file sharing, tcp/udp protokollat (code red, nimda, Slammer..), IRC-kanavat, p2p, Instant Messenger, soitinohjelmistot, etc.. ja jopa kännykkä.
- **Hyökkäysvektorit:** Ohjelmien ja käyttöjärjestelmien haavoittuvuudet. Social Engineering. Huonot konfiguraatiot. Useiden käyttöjärjestelmien haavoittuvuuksien hyväksikäyttö.

# Unprotected PCs can be hijacked in minutes (4 min)

- From Sept. 10 to Sept. 25, online intruders made 305,922 attempts to break into six computers connected to the Internet via broadband DSL. Attackers successfully compromised the Dell Windows XP computer using Service Pack 1 nine times, and the Dell Windows 2003 Small Business server once. No other machines were breached.

Platform	Total attacks	Attacks / day	Attacks / hour
XP SP1	139,024	8,177	341
OS X	138,647	8,155	339
Win SBS	25,222	1,400	61
XP SP2	1,386	82	3.4
XP with ZoneAlarm	848	50	2.1
Linspire	795	46	1.9

# Suckit rootkit ja Internet Explorerin IFrame turvareikä.

- Ensin valloitetaan haavoittuvia Apache webbiservereitä ja sinne asennetaan Suckit rootkit.
- peitetään tehokkaasti jäljet. Rootkitin paljastimet eivät pysty enää havaitsemaan asennettua takaporttia.
- sitten tartutetaan sellaisia windows koneita jossa on IE:n Iframe haavoittuvuus (Windows 2000, xp < sp2). Microsoftin patchi ei ollut vielä saatavilla. (julkaistiin 01.12.2004)
- Tämän jälkeen asennetaan saastuneeseen koneeseen erilaisia takaporttia. ([http://www.vitalsecurity.org/xpire-splitinfinity-serverhack\\_malwareinstall-condensed.pdf](http://www.vitalsecurity.org/xpire-splitinfinity-serverhack_malwareinstall-condensed.pdf)).

# Miten paljastuu?

- <http://www.finlandforum.org/bb/viewtopic.php?t=7685>
- Saturday, 20th November 2004 Falk eSolutions clients using AdSolution Global experienced problems with banner delivery between 6.10pm and 12.30pm GMT. ...
- Early on Saturday morning some banner advertising served for *The Register* by third party ad serving company Falk AG became infected with the Bofra/IFrame exploit. *The Register* suspended ad serving by this company on discovery of the problem.
- Matt: "It's not Bofra but in fact Backdoor.Win32.Agent.ec. This was a carefully planned attack and not a virus."

# Kuka takana?

- Internet Storm Center jäljitti ketkä ovat takana:  
<http://isc.sans.org//diary.php?date=2004-11-24> ”So it appears that the people in the spyware industry have taken a cue from the spammers and they use throwaway accounts and hosting services to do their dirty work. And just like with the spammers, by the time we get around to filtering and blocking a server, they've moved on to another. ”
- Vielä eteenpäin selviää: ” Therefore, in honor of the season, I hereby nominate Sanford "The Spam King" Wallace (siis kuuluisa spammeri Sanford Wallace Kamal) for the first annual "ISC Tin-Pot Turkey" award for (allegedly) being both a low-life spammer and a scummy purveyor of spyware. Let's hope he spends some time in an orange jumpsuit, "married" to whoever has the most cigarettes. ”

# "Phishing"tapaus (29.11.2004)

<http://www.websensesecuritylabs.com/alerts/alert.php?AlertID=85>

- Koko Kiinan verkkoalue (218..) IIS webdavin haavoittuvuuden skannaus.
- Jos haavoittuva serveri löytyi, sinne asennettiin small http serveri ("All hosts are running a small HTTP server in addition to IIS on port 880. The HTTP server (<http://home.lanck.net/mf/srv/index.htm>) has been used in the past to host Phishing attacks several times on non port 80 sites. The small HTTP server was developed in Russia and has legitimate use, however the small profile of it and multiple features such as: built-in email capability, FTP, and CGI capability make it tool for Phishers also.")
- Tämän jälkeen massapostitettiin väärennettyjä Earthlink ja MSN Phishing viestejä.

# Mihin pyritään?

- Zombie botnetin rakentaminen!
- Takaporttien asentaminen käyttäjien koneisiin tulevaisuutta varten. (spyware, adware, keyloggers, ym. troijalaisia)

# Mihin botnetit tarvitaan?

- Spammien lähettämiseen
- kiristysyrityksiin ja muihin DOS hyökkäyksiin: (pelottelu palvelunestohyökkäyksillä)
- Verkkokaistan käyttöön toisten kustannuksella sekä jälkien peittämiseen (relayt, proxyt yms..).

# Virus ja spammin epäpyhäsuhte

- Messagelabs (skannaa n. 2 miljardia sähköpostia/kk) ilmoitti lokakuun tilastossa, että spammien %-määrä kaikista posteista on noussut 1,5 vuodessa 25% --> n. 80% (eli yli 3 kertaistunut). Samanaikaisesti, virusten ja matojen suhde saapuvaan sähköpostimäärään on noussut 1 /250 --> 1 virusviesti/32 viestiä (eli 8 kertaistunut).
- Hyppönen Avar konferenssissä SOBIG variantteista:
  - All variants were connected to spamming
  - All downloaded and installed an email proxy
  - Some of the variants were very succesful

# Spämmi kannattaa

- Jeremy Jaynes joka tuomittiin 9 vuodeksi vankilaan spammilevityksistä, lähetti 10 - 20 miljoonaa roskapostiviestiä/päivä. Onnistuneen huijauksen "osumatarkkuus" oli n. 1/30000. Arvioitu tulo \$750 000/kk: "In a typical month, prosecutors said during the trial, Jaynes might receive 10,000 to 17,000 credit card orders, thus making money on perhaps only one of every 30,000 e-mails he sent out. But he earned \$40 a pop, and the undertaking was so vast that Jaynes could still pull in \$400,000 to \$750,000 a month, while spending perhaps \$50,000 on bandwidth and other overhead, McGuire said. "When you're marketing to the world, there are enough idiots out there" who will be suckered in, McGuire said in an interview

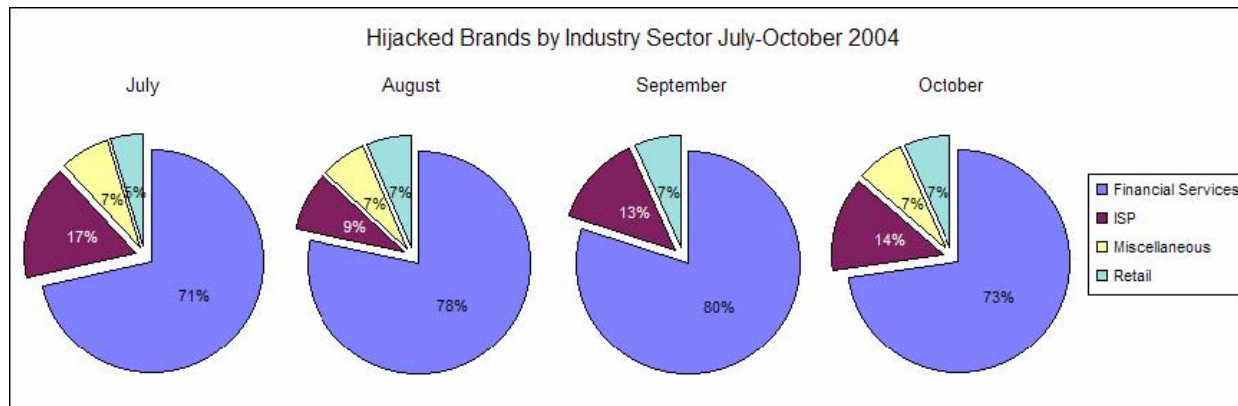
# Suojeluraha

- “Two prominent UK-based online gambling sites, Tote.com and Sportingbet.com, were hit with denial-of-service (DoS) attacks October 21, 2004 and knocked offline. Likely motivated by blackmailing scams, the attacks shut Tote.com down for more than 16 hours, while causing only a few minutes of outages on Sportingbet.com. Security firm Netcraft said in a statement that websites conducting a large volume of transactions are becoming an increasing target for such attacks. In March, 2004, a sustained campaign of DoS attacks was launched against the UK's top 20 gambling sites after blackmailing demands were not met. (<http://www.merit.edu/mail.archives/netsec/msg00158.html#internal16204>)”

# Phishing:

[http://www.antiphishing.org/APWG\\_Phishing\\_Activity\\_Report-Oct2004.pdf](http://www.antiphishing.org/APWG_Phishing_Activity_Report-Oct2004.pdf)

- Number of active phishing sites reported in October: 1142
- Average monthly growth rate in phishing sites July through October: 25%
- (Sähköpostin puhdistuspalveluita tarjoava Messagelabs kertoo, että yhtiö poisti kesäkuussa noin 250 000 phishing-viestiä, mutta marraskuussa määrä oli jo 4,5 miljoonaa. Reilu vuosi sitten syyskuussa määrä oli vielä vaivaiset 279 viestiä. Messagelabsin mielestä phishing-hyökkäykset ovat tämän vuoden merkittävin kehityssuuntaus netin tietoturvasa ([http://www.tietokone.fi/uutta/uutinen.asp?news\\_id=22480](http://www.tietokone.fi/uutta/uutinen.asp?news_id=22480))
- The most targeted industry sector for phishing attacks continues to be Financial Services...”



# Toimiiko virustorjunta? Riittääkö?

- Toimii jos hyökkäys on tiedossa ja tuntomerkit selvinä. Virustorjunnassa ollaan yleensä jälkijunassa. USA:n National Security Agency on tutkinut yli 30 laajalti levinnyttä matoa mm. badtrans, blaster, codered, swen, klez, Loveletter, Magistr, Nimda, sobig.f, slammer, yaha etc...(<http://www.nsa.gov/snac/support/WORMPAPER.pdf>). Näissä madoissa, NSA havaitsi 14 eri hyökkäysominaisuutta (Attack attributes), joista virustorjunta pystyi torjumaan vain 2 ominaisuutta!! Muut hyökkäysominaisuudet piti torjua muilla työkaluilla.

# Virustorjunnan rajallisuudet

## 7.1 The Defense Matrix

Key: B=Blocks; R=Reactively Blocks; P=Protects partially; D=Detects

Defense Attribute	Packet Filtering FW	Stateful FW	Application Proxy FW	IDS	Host FW	VM	Configuration	AV with Heuristics	HIPS	Integrity Check	Stackguarding
Attack Attribute											
Exploits vulnerable network code (infection)	R	R	B	R	R		B				B
Tricks a user (infection)			B		B		P				
Exploits vulnerable configuration (infection)	B	B	B		B		B				
Exploits previously installed backdoor (infection)	B	B	B		B			B			
Changes file system							B		B	D	
Changes system settings							B		B	D	
Modifies some process							B		B		
Accesses the network	P	P	P		B				B		
Requires system privilege							B		B		B
Performs anomalous queries							B		B		
Invokes crucial APIs						B			B		
Causes network flooding	B	B	B		B				B		
Slows local system									P		
Contains worm signatures			P	P				B			

Table 6 - Detailed Defense Matrix