20th Annual FIRST Conference
Cyber Fraud Trends - Authentication

Ralph Thomas - iDefense Malcode Intelligence
rthomas@idefense.com, +1.571.723.1978

June, 2008
Cyber Fraud Disruptors

• Anti-virus
  - Stopped static malware
  - Packers and scrambling is now common practice

• Windows XP SP2 Firewall
  - Enabled by default
  - Stopped malware from coming to the computer
  - Start of drive-by installs via browser exploitation (get the victim to go to the malware)

• Windows Vista Firewall
  - Outbound filtering enabled by default (incl. phishing filters)
  - Limit drive-by installations
  - Limit malware from phoning home
  - Essential for attackers to maintain untainted/volatile hosting
    --> Bulletproof Hosting

• 2FA Deployment
  - Underground economy changes
    --> Adjusted Behaviour
Cyber Fraud Disruptors

- Essential for attackers to maintain untainted/volatile hosting
  --> **Bulletproof Hosting**
- Underground economy changes
  --> Adjusted Behaviour
Bulletproof Hosting

- **The Truth About RBN**
  - All public customers on one network
  - Not secretive at all, heavily spammed ads on many forums
Bulletproof Hosting

• The Post-RBN Era
  - Most popular providers existed well before the fall of RBN
  - Competitors to RBN, no proven connections to leadership
  - Common customers is NOT evidence of common leadership
    • McColo
    • AbdAllah
    • RentaBL
Bulletproof Hosting - AbdAllah

• Reseller of a coalition of bulletproof hosts
• Controls one network, resells the rest
Bulletproof Hosting

Продукты и услуги

Выделенные серверы США
- Дата-центр hospcel.net EAST or WEST USA
- Дата-центр pcnet.net, Parsippany, NJ, USA
- Дата-центр ColorDallas, Dallas, TX, USA
- Дата-центр Burst.com, Scranton, PA, USA
- Дата-центр Layer1.com, Dallas, TX, USA
- Дата-центр Softlayer, EAST or WEST USA

Выделенные серверы Европа
- Дата-центр NetDirect, Frankfurt, Germany
- Дата-центр hezzner.de, Hamburg, Germany
- Дата-центр BTCCOM, Moscow, Russia
- Дата-центр EasyServe, Haarsholm, Denmark
- Дата-центр Czech
- Дата-центр Steinsel, Luxembourg
- Дата-центр Dragonnet, Zurich, Switzerland
- Дата-центр LeaseWeb, Amsterdam, Holland

Выделенные серверы Азия
- Дата-центр Pacific Inc, Hong Kong, China

Виртуальные выделенные серверы
- VPS Virtualse VPS & VPS USA, UK, JAPAN

Виртуальный хостинг
- Alpha DC ColorDallas, Dallas, Texas, США
- Расширенные тарифы VPS DC Morgan.net, Иран, Бирмингем, США
- Delta DC Morgan.net, Иран, Бирмингем, США
- Gamma DC Lesaweb, Amsterdam, Голландия
- Rebohost.co DC Nac.net, Макао, Нью-Джерси, США
- Rebohost.co Windows (пакет PICS), Tokyo, Япония
- Rebohost.org DC Netdirect.de, Frankfurt, Германия

Тарифы виртуального хостинга

SSH250 disk 250Mb 3000Mb traffic
- 1280 Disk space, Mb
- 3 Traffic, Gb
- 1 Domain
- 25 Subdomain
- 999 Database
- 999 Email
- $ 12.00/месяц, Услуги (включая)

SSH50 disk 50Mb 1500Mb traffic
- 500 Disk space, Mb
- 1.5 Traffic, Gb
- 1 Domain
- 999 Subdomain
- 5 Database
- 5 Email
- $ 4.69/месяц, Услуги (включая)

SSH300 disk 300Gb 3000Gb traffic
- 5000 Disk space, Mb
- 10 Traffic, Gb
- 10 Domain
- 25 Subdomain
- 999 Database
- 999 Email
- $ 16.99/месяц, Услуги (включая)

SSH1000 disk 1000Gb 10000Gb traffic
- 10000 Disk space, Mb
- 10 Traffic, Gb
- 10 Domain
- 999 Subdomain
- 999 Database
- 999 Email
- $ 24.99/месяц, Услуги (включая)
"Bulletproof Hosting" - Fastflux
Cyber Fraud Disruptors

• Essential for attackers to maintain untainted/volatile hosting
  --> Bulletproof Hosting

• Underground economy changes
  --> Adjusted Behaviour
Adjusted Behavior

• Fraud is more difficult/complex
  – give up! (not going to happen anytime soon)
  – keep current tactics and change targets
    • go for the smaller fish, drastic increase of phishing attacks against smaller institutions, which are now faced with a 'new' problem
  – stay with current targets and adjust tactics
    • due to 2FA, stolen credentials are stale
    • move from phishing/pharming to malware

• All internet users are affected
  – financial (e-banking, e-brokerage)
  – e-commerce, e-recruitment, communication (e-mail, IM, blogs/forums/groups, ...)
  – persistent environments, social networks, and gaming
Ambush: e-Consumers Under Attack

1) WLAN: Invite for eavesdropping
2) Fake User: I am not me
3) Detour into the bandit's camp: DNS spoof
4) Deceptive Guidepost: The hosts file

1) Trojan: Bogus Software
2) With counterfeit passport into the vault
3) Enter PIN: The crooks read along
Ambush: e-Consumers Under Attack

• Phishing & Pharming
  – Lure victims via social engineering and tempering with DNS to fraudulent webpage designed to steal personal identifiable information (PII)

• Man-in-the-middle (MITM)
  – Fraudulent webpage designed to instantly defraud victims in order to circumvent temporary 2FA means

• Malware
  – Hostile software installed on the victim's computer designed to steal PII or to perform MITM. This compromises the consumer's communication endpoint.
Strong Authentication

• Many choices for client-side authentication
  - Smart card
  - USB Token
  - Virtual Token
  - OTP Token
  - Scratch Pad
  - Certificate
  - Biometrics
  - Phone/Cell/SMS
  - etc.

• Mutual (2-way) authentication

• Account vs. Transaction Authentication

• Implementation is key
  - e.g. cell phone as OTP Token vs. mTAN
  - e.g. OTP token timeout at BR bank
  - e.g. weakness in business process: change phone number
Strong Authentication
Q + A

Ralph Thomas - iDefense Malcode Intelligence
rthomas@idefense.com, +1.571.723.1978

May 28, 2008