



# Hacking Trends

Mark “Simple Nomad” Loveless  
Security Architect

**Autonomic**  
Networks



# Hello

- Security Architect for Autonomic Networks
- Founder of Nomad Mobile Research Centre

# Agenda

- “The sky is falling...”
- Attacker Business Basics
- How I’d Get Into Your Network
- Mitigation
- Q/A

# “The sky is falling...”

- In late 2006 I made some predictions for a press release Vernier Networks did. Let's see how I did...

# Predictions

- Usage of Zero-Day attacks to get “botnet” software into computers will dramatically increase. Black-market prices for these remote exploits requiring no target-user intervention sold for \$5,000 in 2004 but have skyrocketed to as much as \$80,000 in 2007.
- Yes

# Predictions

- Business-oriented social networks, such as LinkedIn and ZoomInfo, will gain the attention of malware writers, particularly those who target specific businesses. Hackers will use these networks to penetrate organizations starting with human-resources departments. Expect more phishing-like attacks to target these social networks.
- No

# Predictions

- Hackers will continue to focus attacks on stealing identities and corporate data, instead of disrupting IT services.
- Yes (easy one)

# Predictions

- Vista intrusions will take center stage despite the massive improvements in the product's security. Don't be surprised to see hackers drive home the point by creating a "Month of Vista Bugs," as they did with the "Month of Browser Bugs" (<http://browserfun.blogspot.com/>) and "Month of Kernel Bugs" (<http://kernelfun.blogspot.com/>) projects.
- Yes and no, and I was late by 8 days.

# Predictions

- Aggressive criminal attacks will double in 2007 for two main reasons. First, there are a finite number of available PCs to compromise and "zombify" into becoming spam relays and other malicious conduits. Second, cyber criminals face little law-enforcement risks but increased competition for the millions of dollars available, so hackers will take greater risks and employ more aggressive tactics. The centerpiece of cyber crime are "botnets" – a group of compromised computers that enable coordinated, remote manipulation by an attacker who has compromised a large group of computers and installed remote-controlled, backdoor software. The battle for control of large botnets will result not only in an escalation of cyber crime, but an increase in online criminals attacking each other – both with casualties on innocent users' computers.
- Yes

# Predictions

- The Apple community, which is currently in denial over security issues, will suffer a rude awakening from the “Month of Apple Bugs” (<http://projects.info-pull.com/moab/>). Apple will react poorly but show much improvement at handling such issues for the long term.
- No, unless you count in the iPhone, and even then, not really

# Predictions

- Phishing and identity theft will move from the consumer market to the corporate market, and internal identities (i.e., names and passwords) will be hijacked. Hackers will use these identities to penetrate corporate networks and steal high-valued trade secrets and customer information and sell it on the black market.
- Yes

# My New Prediction

- From the current Info Sec Magazine in the article titled “The View from Visionaries”:
- “While the main short-term security threat still appears to be compromised home systems as a part of a botnet sending spam, spreading malware, and DDoS, these issues will begin to surface more and more in a corporate environment. This can be symbolized in the case [earlier this year] of Viagra spam being sent from zombified desktop computers in the Pfizer corporate network (ironically the makers of Viagra) to systems on the Internet. With the dynamic nature of networks, systems that are not protected by sophisticated networks that regulate access will find themselves targeted more frequently as potential unwilling botnet participants. I would expect with the recent trend of sales of zero-day security flaws in modern software to criminal elements that the overall zombification process will make greater gains in corporate networks than ever before.”

# Attacker Business Basics

# Disclosure Cycles

- Vendor releases patch
- Researcher releases advisory
- Unpatched and patched versions of “fix” files are reverse engineered
- Exploit code is developed based upon flaw
  - Whitehats use this to develop IDS/IPS signatures
  - Blackhats use this to develop attack code
  - Both hats look for “silent” patches

# Underground Trends

- The botnet is king
  - Botnets in excess of 1.2 million computers have been discovered “in the wild”
  - 15,000 to 50,000 compromised computers in a botnet is not uncommon
- Botnets can be leased, sub-leased, and are multi-functional
  - Can perform automated attacks against new systems
  - Can send spam
  - Launch denial of service attacks
- Botnets are grown via a combination of 0day and recently uncovered flaws

## Underground Trends (pt. 2)

- In 2002, a remote access 0day could be sold to iDefense for \$3500, or on the black market to the Russians or the Chinese for \$5000
- Today, a remote access 0day could be sold to iDefense for as much as \$15,000, and by using a broker (who takes a cut) sold to “private buyers” for as much as \$80,000 (asking prices of \$120,000 have occurred) One of the largest purchasers? Paying huge bucks? The U.S. Government.
- Virus and malware writers are offering subscription services to ensure future releases of new viruses are not detected by anti-virus packages

# Underground Trends (pt. 3)

- Botnets use spam techniques to launch phishing scams, and are using rapidly changing IP addresses of fake servers to prevent blacklisting.
- Botnets are using peer-to-peer technology to issue commands, preventing the possibility of dismantling a central server to stop the botnet. Encryption is also being used.
- State-sponsored hacking is becoming more prevalent.
  - China, Russia, USA, and France are amongst the big players
  - Hacking by these sponsors is sometimes outsourced, sometimes unknowingly

# 0Day Relevance

- This is how important 0day currently is
- Early 90s 0day was discovered in the wild by admins trying to figure out how they were compromised
- In late 90s to early 00s it was via full disclosure mailing lists
- Now it is reverting back to discovery in the wild, due to the money involved

# The Market

- Freelance and fulltime blackhat researchers discover 0day flaws
- The flaws are sold, sometimes in auction, usually through a broker, mainly to organized groups building and growing botnets
- The botnets are used thusly:
  - DoS extortion attacks, typically against people that depend on uptime for their money
  - Spam is sent in huge amounts
- Attacks against other system (via the botnets, like a worm) are not as common as the goal is to compromise machines not alert antivirus companies
  - The attacks are targeted and slow to prevent detection

# Skill Segmentation

- Virus and rootkit writers all used to have to worry about deployment and infection, controlling the systems, and were consumers of their own work to meet their own ends
- Now malware writers write their software to order and sell it, botnet herders are responsible for deployment and maintenance, spammers and phishing lease capacity from the botnet herders, and everyone is making money
- Entire shops with release schedules, product marketing personnel, sales forces etc all are formed around this market
- The processing of stolen goods is even segmented into money launderers, brokers, testers and all done in Ebay-like forums where criminals are ranked according to how “honest” they are and easy to deal with

# How I'd Get Into Your Network

# Over the Firewall

- Egress firewall rules are still not enforced
  - How many people are using web proxying to control web surfing?
- Client-side attacks are becoming more and more popular
  - These bypass corporate and personal firewalls
  - As long as the web site isn't in the "blocked" list, users accessing malicious web sites are not stopped by web proxying
- Email-based attacks are another popular vector
  - Are you blocking outbound POP3/IMAP access?

# Bypass the Firewall

- VPN

- How secure are your users' accounts and passwords?
- How easy is it to get a password reset remotely?

- Dialup

- Still around, still a viable attack vector, same old rules apply

- Wireless

- Can I sit in your parking lot, neighbor's office building, lobby, or public restroom and attack?

# Exploit Your Trust in Others

- Corporate subsidiaries and divisions
- Trusted clients
- Trusted vendors
- Outsourced services
  
- I would simply pretend to be one of the above, and walk right in through your firewall
  - I could break into one of the above
  - ISP compromises, GRE tunnels, short-lived BGP announcements etc and I *am* at the IP addresses you trust

# The Road Warrior

- Attackers know all the public addresses of all the major hotel chains, and which ones use firewalls/router ACLs
- Attackers can attack entire industries via trade shows at hotels remotely
- Company-wide meetings can attract attackers when the corporate base is widespread
  - All of the out-of-town users are at the nearest hotels to the site of the meeting
- Hotel address ranges are good for just plain old low hanging fruit

## The Road Warrior (cont.)

- Most road warriors regard their laptop as their own computer, as opposed to a corporate-issued desktop system
- At nighttime in the hotel, the same bad habits from home translate onto the corporate laptop
  - Online gambling
  - Porn
- Many times they are VPN'ed into work
  - This can lead to realtime “inside” attack as the attacker uses the laptop as the conduit in
- Once compromised, the road warrior's machine gives up hashes, PKI keys, VPN passwords, WPA/WEK keys etc
- And of course, hello rootkit and welcome to the botnet...

# The Road Warrior (cont.)

- My talk from this stage in 2006 regarding issues while on the plane
  - Still relevant
  - Google “Hacking the Friendly Skies”, and find the ShmooCon video of my presentation (NSFW, hacker con with cursing)
- Was recently interviewed over new issues with the Boeing 787 Dreamliner
  - A sidenote is that computer-to-computer hacking, MITM web attacks, sniffing, etc all become more relevant than ever

# Mitigation

# The Challenge

- Prevent 0day
- Detect attacks before they happen
- Assume attacks will come from the inside as well as the outside

# Things That Help

- Defeating 0day is impossible, and every decent security person knows it
  - You can get close, but you will never reach 100% prevention
  - Anyone telling you they stop 0day is lying if they tell you 100% reliability
  - Ask for tangible guarantees, and watch them run away
- Patch immediately, don't "test the patches"
  - Half the time when testing you roll out the patch and things still break, just get good at fixing the breaks
- Use personal firewalls on all desktop/laptop systems
  - Never assume that porous perimeter is safe, unless you do not allow systems to talk to the Internet at all, including email

# Things That Help (cont.)

- Understand that perimeter security is dead
- Anti-virus, anti-spyware, IDS/IPS etc are all nice things to have
- Locking down (hardening) workstations will provide more bang for your buck than anti-virus, anti-spyware, and IDS/IPS systems
  - Being able to enforce this helps prevent “near 0day” compromises
  - If you use NAC and enforce policies before allowing network access, check for patches, firewall, anti-virus, but also that the system is locked down

# Questions?

- **Contact:**

- [mloveless@autonomic-networks.com](mailto:mloveless@autonomic-networks.com)
- [thegnome@nmrc.org](mailto:thegnome@nmrc.org)

- **Presentation**

<http://www.nmrc.org/~thegnome/ISACA-IIA-2008.ppt>