
Stopping Tomorrow's Cyber Attacks Today

By: Chris Brenton
www.chrisbrenton.org

Proactive Cyber Defense Seminar

Before We Start

- What makes a system “vulnerable”?
- Which systems on your network would you define as susceptible to remote attack?

Open Listening Sockets

```
[cbrenton@mail cbrenton]$ netstat -an
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp      0      0 129.170.248.227:110    129.170.249.142:1338   TIME_WAIT
tcp      0      96 129.170.248.227:22     129.170.76.173:1096   ESTABLISHED
tcp      0      0 129.170.248.227:6011  129.170.248.227:2265  ESTABLISHED
tcp      0      0 129.170.248.227:2265  129.170.248.227:6011  ESTABLISHED
tcp      0      0 129.170.248.227:22     129.170.248.37:1038   ESTABLISHED
tcp      0      0 129.170.248.227:22     129.170.248.31:1035   ESTABLISHED
tcp      0      0 129.170.248.227:53    0.0.0.0:*              LISTEN
tcp      0      0 127.0.0.1:53          0.0.0.0:*              LISTEN
tcp      0      0 0.0.0.0:110           0.0.0.0:*              LISTEN
tcp      0      0 0.0.0.0:22            0.0.0.0:*              LISTEN
tcp      0      0 0.0.0.0:25            0.0.0.0:*              LISTEN
tcp      0      0 0.0.0.0:23            0.0.0.0:*              LISTEN
tcp      0      0 0.0.0.0:21            0.0.0.0:*              LISTEN
udp      0      0 129.170.248.227:53    0.0.0.0:*
udp      0      0 127.0.0.1:53          0.0.0.0:*
udp      0      0 0.0.0.0:514           0.0.0.0:*
```

What If There Are No Listening Services?

- It's about "remote access to software"
 - Not just accessible sockets
- Some additional examples
 - Desktop running a Web browser or mail client
 - Firewall, NIDS, NIPS with no open sockets
 - Management system using a Web interface
- In each case software is accessed remotely without the need of open listening ports
- System may still be exploitable

Permission Issues

- What can attacker do from a desktop?
 - Limited by the user's permissions level
 - If Admin equivalent, all bets are off
 - If not, may be able to leverage a local privilege escalation
- What about from security gear?
 - Tend to run with high level permissions
 - Tend to be ignored as "trusted" devices

What We Will Talk About

- *Why the rise in Malware*
- Why we are loosing the battle
- What we need to do in the future

History Of Malware

- The business model for some/many Malware writers changed around 2001
- It was about mass propagation, now its about money/power
 - But we still have script kiddies
- The new models mean the nastiest Malware sees limited release
 - Only release it when profit can be made
 - Fewer chances for signature generation

Malware Opportunities

- Extortion
 - Steal info then sell it back
- Espionage
 - Steal info for a business competitor
 - Change/delete existing info for competitor
- Steal data with value in the wild
 - Malware which trolls & transmits .doc, .xls, bank info, etc. becoming more common
- Conduit for 3rd party attacks
 - Its all about the desktops

Making Money With Malware

- Botnet access = \$.5/bot/month
- Host fast flux (phishing) = \$1,500/month
- 1 million e-mail addresses = \$60
- Spam 1M addresses = \$175
- On-line store credentials = \$12
- Bank account info = \$1-\$1,500
- Address & SSN = \$7
- Adware install = \$1.5/system
- Low prices due to industry competition

Malware Writer's Salary

- Assume a small bot army of 50K
 - \$2,000 sending spam
 - \$2,00-\$3,500 performing DDoS
 - \$1,200 for Phishing services
 - \$3,000 for Adware
 - \$1,500 for misc (ID theft, acc info, etc)
- Malware writer would conservatively earn about \$120,000/year
- Would be 3rd on SANS salary survey

How Big Are The Botnets?

- Per NetworkWorld on July 22nd
 - Zeus = 3.6M hosts
 - Koobface = 2.9M hosts
 - TidServ = 1.5M hosts
 - Trojan.Fakeavalert = 1.4M hosts
 - TR/Dldr.Agent.JKH = 1.2M hosts
- These are US only numbers

State Sponsored Attacks

- The Internet has become the great equalizer
 - Cold war = Biggest army wins
 - Modern = A smart 14 yr old can gain access to critical services/info
- Quicker learning curve
 - Easier to be persistent when you're not worried about jail time
- Plausible deniability
 - State can claim victim status as well
 - Just don't attack from whitehouse.gov

Is It Getting Better Or Worse?

Nuclear secrets stolen for 2+ yrs before detection:

<http://www.theinquirer.net/default.aspx?article=23870>

<http://www.securityfocus.com/news/11222>

BBC buys DDoS network & credit cards:

http://news.bbc.co.uk/2/hi/programmes/click_online/7932816.stm

6+ years of China stealing US government secrets:

http://en.wikipedia.org/wiki/Titan_Rain

China controls high value systems in 103 countries:

<http://en.wikipedia.org/wiki/GhostNet>

The electrical grid is 0wn3d:

<http://www.informationweek.com/news/internet/showArticle.jhtml?articleID=205901631>

<http://online.wsj.com/article/SB123914805204099085.html>

Contractors moving from bombs to bits:

http://www.govinfosecurity.com/articles.php?art_id=1595

What We Will Talk About

- Why the rise in Malware
- *Why we are loosing the battle*
- What we need to do in the future

Increased Signature Rates

- Symantec
 - 11,000 per day
 - 1 new signature every 8 seconds
- F-Secure
 - 20,000 per day
 - 1 new signature every 4 seconds
- Do you update your A/V sigs every 4-8 seconds?
- A/V vendors are being DoSed

A/V Software & How It Works

- A/V is *primarily* signature based detection
 - Pattern matching, similar to NIDS & NIPS
 - Based on application black listing
 - Match the pattern and the software gets blocked
- A large number of infections increase the chance a signature gets generated
 - “Acceptable losses” to generate signatures
 - Assumes a business model of mass propagation
 - Can also be generated if the code gets posted

Problems With A/V

- Assumes some level of fallout
 - Reactive technology
- Change the signature and Malware goes undetected
 - The treadmill of signature updates

http://packetstormsecurity.org/papers/virus/Taking_Back_Netcat.pdf

- No access to the signature language
- Little customization capability
 - What if I need to run Netcat or a password cracker but don't want to be wide open?

What About Heuristics?

- Based on behavioral analysis
- Looks for suspect activity
 - Managing user accounts
 - Opening a network socket
- Tends to flag custom or 3rd party apps
 - Goes back to customization issues
- Has potential if not distracted by signatures
 - Focus needs to be on apps, not sigs
 - Can be thought of as rudimentary app control

What About Policy Enforcement?

- Enables the kernel to enforce specific behavior on specified applications
 - SELinux is a good example
- Works by defining what an app can do
- Example: An SMTP application
 - Open TCP/25 locally and remotely
 - Read configuration files
 - Write to the log
 - Read/write to the queue

SELinux Targeted Vs. Strict

- Targeted
 - Control only certain processes
 - Those holding open a socket
 - Rely on system to secure the rest
 - Defined as “unconfined_t”
 - Simplifies the creation of policies
- Strict
 - All processes must have a defined policy
 - Most secure but most complex config

Problems With Policy Enforcement

- If you run targeted, undefined apps can still misbehave
- If you run strict, **every** application needs a policy
 - Logon and VB scripts, batch files, etc.
- Better suited for servers rather than desktops
- But has desktop possibilities discussed in a later slide

What About Standards?

- Heartland Payment Systems was hit in 2008
 - Process 100M credit & debit cards/month
 - Magic number stolen - cards can be cloned
- Did PCI DSS help?
 - Requires A/V but customize Malware used
 - Informed of breach by Visa & Mastercard
 - Occurred just after passing a validated PCI audit
 - Passed another audit just after breach detection
- Standards are lowest common denominator
 - We focus on passing the test, not risk assessment

Management Vs. Security

- Next Gen Firewalls (UTM)
 - Increase features trading off security
- VLANs
 - Done across security zones creates alternate paths
- Virtualization
 - Physical connectivity between hosts creates alternate paths

What We Will Talk About

- Why the rise in Malware
- Why we are loosing the battle
- *What we need to do in the future*

What Is Application Control?

- Also referred to as application white listing
- Defines which applications can be executed on the system
 - Can leverage an extensive file database
- Usually permits far more customization capability than A/V software
 - Admins can run Netcat & password crackers
- Downside is once a program is allowed to execute, its uncontrolled
 - Will discuss this more in a later slide

What's It Good For?

- Blocking malicious code infections
 - Has AV software been superseded?
 - You may not know what Malware you blocked
 - Since there are so many names, do you care?
- Enforcing acceptable use policy
 - No more blocking IM at the border!
 - Can usually define app use at the user level
- System remains in an approved state
 - Goes far beyond UAC capability

Is White Listing More Economical?

- Problem in the past
 - More legit software than Malware
- The metrics have changed
 - Approximately 150,000+ pieces of new Malware expected this year
- How often do you deploy new applications?

What To Look For

- Good Active Directory integration
- Customizable enforcement options
 - Sales can run only safe software
 - IT is prompted when its dangerous
- A huge file database
 - Multiple hash ID's
 - Option to deal with custom software

Case Study: Securing SCADA

- Used for everything from water treatment to energy generation and dissemination
- Many systems run very old software
- Usually attempt to isolate network
 - Can easily be compromised
 - Makes management difficult

Securing SCADA With Application Control

- Deploy as an isolated network
- Install an application control system which supports signed software
 - Digitally sign all authorized software
 - Enforce authentication prior to execution
- Sign new software as needed
- Any malicious applications (backdoors, keystroke loggers, etc) are now blocked

Where Am I Still Vulnerable?

- Remotely exploiting “approved” software running on the system
 - Only execution is checked
- Attacks that are memory resident only
 - Depends on the software
- Both problems can be mitigated with Host Based Intrusion Prevention
 - Kernel level policy enforcement

What About Desktop Suites?

- Many A/V vendors are (slowly) moving to application control
- Products may include
 - A/V signature detection
 - Some HIPS capability
 - Some application control
- Focused products seem to be doing a better job right now

Specific Recommendations

- Risk assessment of security zones
 - Do servers & desktops belong on the same network segment? Management systems?
- Leverage good defense in-depth
 - Outbound accepts are most interesting
- Wider deployment of application control
- Wider deployment of kernel level policy enforcement (HIPS)

Questions?

chris@chrisbrenton.org
www.chrisbrenton.org