Agenda

• Introduction
• Think Evil…
• Observations
• Recommendations
• Questions
Speaker

Tom Brennan CISSP, is the Founder and CEO of ProactiveRISK known for CATScan℠ (Comprehensive Accurate Testing & Scanning) and his volunteer service to the OWASP Foundation since 2004 most recently as the Global Vice Chairman. He is also a member of the (ISC)2 Application Security Advisory Committee (ASAC) with a focus on the CSSLP (Certified Secure Software Lifecycle Professional)

Tom is a veteran of the United States Marine Corps and resides in the Rockaway Township, New Jersey with his wife and children. He enjoys building both open source and commercial software solutions, off-roading in his Jeep and flying FPV Drones in his spare time.
Hackers Can Turn Your Home Computer Into a Bomb... & Blow Your Family to Smithereens!

By RANDY JEFFRIES / Weekly World News

WASHINGTON — Right now, computer hackers have the ability to turn your home computer into a bomb and blow you to Kingdom Come — and they can do it anonymously from thousands of miles away!

Experts say the recent “break-ins” that paralyzed the Amazon.com, Buy.com and eBay websites are tame compared to what will happen in the near future.

Computer expert Arnold Yabenson, president of the Washington-based consumer group National CyberCrime Prevention Foundation (NCPF), says that as far as computer crime is concerned, we’ve only seen the tip of the iceberg.

“The criminals who knocked out those three major online businesses are the least of our worries,” Yabenson told Weekly World News.

“There are brilliant but unscrupulous hackers out there who have developed technologies that the average person can’t even dream of. Even people who are familiar with how computers work have trouble getting their minds around the terrible things that can be done.

“It is already possible for an assassin to send someone an e-mail with an innocent-looking attachment connected to it. When the receiver downloads the attachment, the electrical current and molecular structure of the central processing unit is altered, causing it to blast apart like a large hand grenade.

As shocking as this is, it shouldn’t surprise anyone. It’s just the next step in an ever-escalating progression of horrors conceived and instituted by hackers.”

Yabenson points out that these dangerous sociopaths have already:

- Vandalized FBI and U.S. Army websites.
- Broken into Chinese military networks.
- Come within two digits of cracking an S7-digit Russian security code that would have sent deadly missiles hurtling toward five of America’s major cities.
- As dangerous as this technology is right now, it’s going to get much scarier,” Yabenson said.

“Soon it will be sold to terrorists, cults and fanatical religious-fringe groups.

“Instead of blowing up a single plane, these groups will be able to patch into the central computer of a large airline and blow up hundreds of planes at once.

“Worse, this e-mail bomb program will eventually find its way into the hands of anyone who wants it.

“That means anyone who has a quarrel with you, holds a grudge against you or just plain doesn’t like your looks, can kill you and never be found out.”
Can someone shut off the light?

- 30 Seconds
- (n) Solutions
- End-Game Logic
Answer Key

• Find the switch and flip it
• Throw a object at it
• Wrap your hand and touch it
• Ask someone to do it for you
• Cause a power failure in building
• Don’t pay the electric bill
• Close your eyes
Can someone hack my system?

• Breach perimeter security without detection
• Propagate from system to system undetected
• Arrogate the treasure inside the organization undetected
• Must exfiltrate the treasure out of the organization undetected
Observations
Symptom #1

- Unusual account activity based on known behaviors or the account holders

<table>
<thead>
<tr>
<th>Access Type [? ] (Browser, mobile, POP3, etc.)</th>
<th>Location (IP address) [?]</th>
<th>Date/Time (Displayed in your time zone)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browser</td>
<td>160.196.77.10</td>
<td>Feb 2 (17 hours ago)</td>
</tr>
<tr>
<td>Browser</td>
<td>160.196.77.10</td>
<td>Feb 2 (20 hours ago)</td>
</tr>
<tr>
<td>Mobile</td>
<td>160.196.77.10</td>
<td>Feb 2 (22 hours ago)</td>
</tr>
<tr>
<td>Browser</td>
<td>160.196.77.10</td>
<td>Feb 2 (22 hours ago)</td>
</tr>
<tr>
<td>Browser</td>
<td>160.196.77.10</td>
<td>Feb 2 (1 day ago)</td>
</tr>
<tr>
<td>Browser</td>
<td>160.196.77.10</td>
<td>Feb 2 (1 day ago)</td>
</tr>
<tr>
<td>Browser</td>
<td>160.196.77.10</td>
<td>Feb 1 (2 days ago)</td>
</tr>
<tr>
<td>Browser</td>
<td>160.196.77.10</td>
<td>Feb 1 (2 days ago)</td>
</tr>
</tbody>
</table>

Alert preference: Show an alert for unusual activity. change
Symptom #2

- Unexplained outbound activity from systems
Symptom #3

• Newly created files on systems in system directories
Symptom #4

- Login geographic origin anomalies
Symptom #5

• Unexplained changes to the windows registry
Symptom #6

• Attempts to tamper log archives
Symptom #7

- Anti-virus/Anti-malware control tampering
Symptom #8

- Service activity (added/stopped/paused)
Symptom #9

• Unexplained downtime
Symptom #10

- Unauthorized administrative console access
If someone punched you in the face what would you do?
PRACTICAL SOLUTIONS YOU CAN DO FOR FREE!

YOU CAN DO IT!!
Center for Internet Security

- Council on CyberSecurity
  - Top 20 Security Controls
  - Workforce Development
- Information about the Benchmarks, Metrics, and Assessment Tools
- 101 Benchmark documents in PDF
- 28 Security Metric Definitions in PDF
- Configuration Assessment Tools
Web Application Security

OWASP (Open Web Application Security Project)
- ASVS (Application Security Verification Standard)
- Top 10 Risks
- Developer Guide
- Web Application Testing Guide
- Developer Cheat Sheets
- Honeypot Project
- Zed Attack Proxy (ZAP)
- RFQ Criteria
- Incident Response Top 10

+100+ projects visit http://www.owasp.org
• Make sure it runs under its own user (apache or www-data), definitely NOT root!
  • `grep -ir 'APACHE_RUN_USER' /etc/apache2`

• Check permissions in web root. Web files shouldn’t be writable by apache, unless by design (logs, file upload feature..etc) `chmod` & `chown` the rest to root.

• Apache doesn’t need shell access, remove its shell:
  • `chsh -s /dev/null www-data [or apache]`

• Update Apache if possible 2.4.7
• Disable Server Side Includes (if not used) with Options –Includes

• Disable CGI scripts (if not used) with Options –ExecCGI

• Disable directory browsing with Options –Indexes (They always forget that!)

• Disable Apache mod_status, mod_userdir, mod_info, mod_autoindex.
  • a2dismod autoindex
  • a2dismod status
• Check it doesn’t have a UID of 0:
  • `grep www-data <or apache> /etc/passwd`

• Lock the Apache user, it doesn’t need to login:
  • `passwd -l www-data (or apache)`

• Install the **Sohusin** and **PHPIDS** security plugins.

• Prevent `.htaccess` modification with:
  ```
  <Directory />
  AllowOverride None
  </Directory>
  ```
- PHP hardening options in php.ini file:
  - display_errors = Off
  - disable_functions = system, exec, passthru, shell_exec, show_source, dl...etc
  - open_base_dir = ‘/var/www/html’ #web root
  - allow_url_fopen = Off
  - allow_url_include = Off
  - file_uploads = Off (if not used!)
• Install ModSecurity for IIS.

• Remove unneeded ISAPI filters.

• In machine.config, disable tracing debug:
  • <trace enable="false" />
  • <compilation debug="false" explicit="true"/>
  • <deployment retail="true"/>

• Use IISLockdown, IIS URLScan, or its easier open source equivalent: AQTRONIX WebKnight
Verify Directory browsing is disabled with:

- `%systemroot%\system32\inetsrv\appcmd list config /section:directoryBrowse /enabled:false`
- Output: `<directoryBrowse enabled="false" />`

ApplicationPool Identities are the real users running the web applications. The best security practice is to use ApplicationPoolIdentity.

- Set DefaultAppPool’s type = ApplicationPoolIdentity

Stop double-encoding attacks by editing `web.config`:

- `<security><requestFiltering allowDoubleEscaping="false"/></requestFiltering></security>`
• Check that no users with empty passwords exist:
  • Select user, password from mysql.user where length(password) = 0 or password is null;

• Check that no anonymous user exists:
  • select user from mysql.user where user = ";

• Check FILE permissions, only admins need it:
  • select user, host from mysql.user where File_priv = 'Y';

• Disable LOCAL INFILE, in my.cnf file:
  • set-variable=local-infile=0

• Drop ‘test’ database.
• Change the default passwords for many users: apex_040000, system, dbsnmp, mdsys, appqossys … and many others!

• Remove Oracle test users:
  • DROP USER BI CASCADE;
  • The same for HR,OE,PM,IX,SH, SCOTT

• Check for updates: select * from DBA_REGISTRY_HISTORY;
  • ^ If this returns nothing, you have no security patches!
• Verify only the root user has UID 0:
  • `sudo awk -F: '($3 == "0") {print $1 }' /etc/passwd`

• Verify no user has an empty password:
  • `sudo awk -F: '($2 == "") {print $1 }' /etc/shadow`

• Use Bastille Linux: Bastille Linux is a hardening patch for Linux through an easy and interactive interface. Excellent for experts and beginners!
  • `apt-get install perl-Tk`
  • `apt-get install bastille`
  • `bastille -c`
Bastille Linux is the ultimate Linux hardening tool. It explains everything before it does it, allows you to undo, and gives full flexibility.
• Check the processes under a user, verify only verified ones are running:
  • `top -u apache` / `top -U www-data`

• Check user login activity with `w`, `who`, `last`, `lastlog`

• Check bash history with `cat .bash_history`

• Check active cron jobs with `ls /etc/cron.*`

• Check active processes with `ps aux`, note the ones running under root!
Check your network connections with `netstat -tulpan`
- Entries with 0.0.0.0 are open to all interfaces.

Or use `ls/of -i`, it might be clearer for you:
- root starts just one apache process to bind on port 80, don’t be scared by that. It is okay.
- You might see connections with *.1e100.net. Don’t worry, that is not malware. It’s just Google.

Use `tcpdump` to check connections on unusual ports:
- `tcpdump -i <INTERFACE> port not 80 and port not 443 and not host 127.0.0.1 and not arp and not ip6 and port not ntp and port not ssh and port not 53`
• You might want to check out OSSEC Host-based Intrusion Detection System. Free and open source!
• http://www.ossec.net/

• OSSEC performs excellent functions like file integrity/changes check, rootkit checks, CIS (Center for Internet Security) benchmark checks, VMware security checks, email alerts…etc
• The easiest way to start to secure your windows installation is by running Microsoft Baseline Security Analyzer (MBSA).

• Use TCPView to check your network connections.

• Use Filemon to check your file activities. Focus on the inetpub/wwwroot directory activities.

• Use sigverif to verify integrity of system files.
• Check Windows startup folders and registry keys for unauthorized entries:
  • `\Software\Microsoft\Windows\CurrentVersion\Run`
  • `\Software\Microsoft\Windows\CurrentVersion\RunOnce`
  • `\Software\Microsoft\Windows\CurrentVersion\RunOnceEx`
  • … and others.

• Check no guest access or null sessions are allowed.
• The basis of reactive defense is watching errors as they come in. Attackers are very noisy with errors & exceptions. **Watch your error logs!**

• Many tools exist, from simple grep & awk to commercial offerings.

• Make sure you enabled advanced/detailed logging.

• Watch **5xx HTTP** errors, as they usually point to failed attacks or application faults.

• Too many **404, 403, 401 & 400** = **possible attacks**
• Search or grep for keywords such as authentication, error, access, 404, 403, denied, failed, password, exception, NULL, UNION, OR 1=1, --, *

• You will always find interesting results!

• Be careful about handling sensitive/personal data while checking error logs. If you ever need to submit it to somebody for review & help; remove such info!

• Linux compresses older log files. Search with with:
  • zgrep KEYWORD FILENAME
  • zcat FILENAME | grep KEYWORD
• Always survey the internet for any signs of exposure or attacks against your systems.

• Set up Google Alerts for your organization’s keywords.

• Set up Pastebin alerts for any leak on your organization.

• Search Twitter for any targeted links.

• Keep an eye on what Google indexes on you!

• “LOCK DOWN” an operating system, we do so by removing functions, by reducing the choice set of what might be running shrinking the attack surface
Know what you have…
(ROI) Risk of Incarceration

• Breach perimeter security without detection
• Propagate from system to system undetected
• Arrogate the treasure inside the organization undetected
• Must exfiltrate the treasure out of the organization undetected
BoD 2015 FAQ

• Which threats are relevant to our business? Why?
• What’s connected, what are the most critical services… who runs them?
• Is there a formalized response process in the event of a breach?
• What is our companies formal disclosure process?
• What industry and enforcement relationships are in place when needed to ring the fire alarm?
• Have we conducted a mock exercise to identify our strengths and weaknesses – are you ready to fight?
Questions?

tomb@proactive-risk.com
@brennantom