A White Hat Perspective on Cyber Security and Other Internet Issues

A presentation to the Internet Society, Washington, DC

HacDC, 16 October 2012

By: The Doctor [412/724/301/703] [ZS]

Disclaimer

- I do not speak for my employers or clients, past or present
- I do not speak for HacDC
- I am receiving no compensation for this presentation
- All observations and opinions are mine and mine alone

What is HacDC?

- A hackerspace in northwestern Washington, DC
- A 501(c)(3) nonprofit organization
- A place where people of all ages gather to
  - Teach one another
  - Learn new things
  - Experiment with new technologies
  - Use tools and apparatus that they might not have access to at home
  - Do interesting things because we can

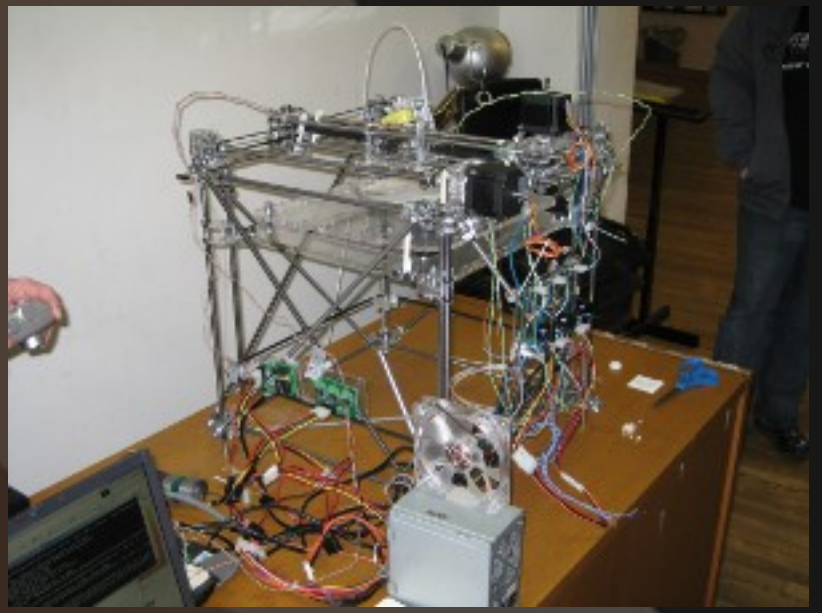
What is hacking?

Source: http://catb.org/jargon/html/H/hacker.html

- A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary. (sense 1)
- One who programs enthusiastically (even obsessively) or who enjoys programming rather than just theorizing about programming. (sense 2)
- A person capable of appreciating hack value. (sense 3)
- A person who is good at programming quickly. (sense 4)
- An expert at a particular program, or one who frequently does work using it or on it; as in ‘a Unix hacker’. (sense 5)
- An expert or enthusiast of any kind. One might be an astronomy hacker, for example. (sense 6)
- One who enjoys the intellectual challenge of creatively overcoming or circumventing limitations. (sense 7)
- A malicious meddler who tries to discover sensitive information by poking around. Hence password hacker, network hacker. The correct term for this sense is cracker. (sense 8) (deprecated)

Hack all the things!

- High altitude balloon launches
- 3D printing
- Metalworking
- Electronics
- Robotics
- Amateur radio (W3HAC)
- Software development
  - Classes
  - Working groups



Who am I?

- The Doctor [412/724/301/703] (http://about.me/drwho)
- Member of HacDC (http://hacdc.org/)
- A core developer of Project Byzantium (http://byz.im/)
- Zero State project manager (http://zerostate.net/)
- Security consultant, system administrator, system architect, penetration tester
- Privacy and anonymity advocate
- Consulting agent of Telecomix (http://telecomix.org/)

State of Infosec in 2012

- Great advances have been made since people started taking infosec seriously
- They haven't done much good
- The two sides are playing different games
  - White hats are entirely defensive, play by arbitrary rules, and aren't doing due dilligence
  - Black hats have no rules other than “Pwn 'em.”

Attacks and Vulnerabilities

- Code vulnerabilities are more difficult to exploit
- Vulnerabilities are now architectural
- IOW, not inherent in languages but how languages are used
- Too numerous to mention
  - SANS Top 25
  - OWASP Top 10
- Uppermost OSI level – the user – most often exploited vulnerability

Economics of Software Development

- Secure code development still not taught
- First to market, first to recoup costs, first to patch... maybe.
  - Not coding securely means being first to market
- Developers have little investment in end users
  - “Why should I care?”
  - “Users should know better.”

End users

- Attempts to get users to take a more proactive role have failed
- Trying to make them consider their actions inadvertantly trained them to click on whatever it takes to make the warning message go away
  - Sometimes it's scared users away from patching
- Don't care about assessing risks or threat models, they want their shiny thing to play with
- Users are trusting, so spear phishing is like... shooting fish in a barrel
- “I don't have anything black hats would want!”

Blackhats have more uses for your PC than you do.

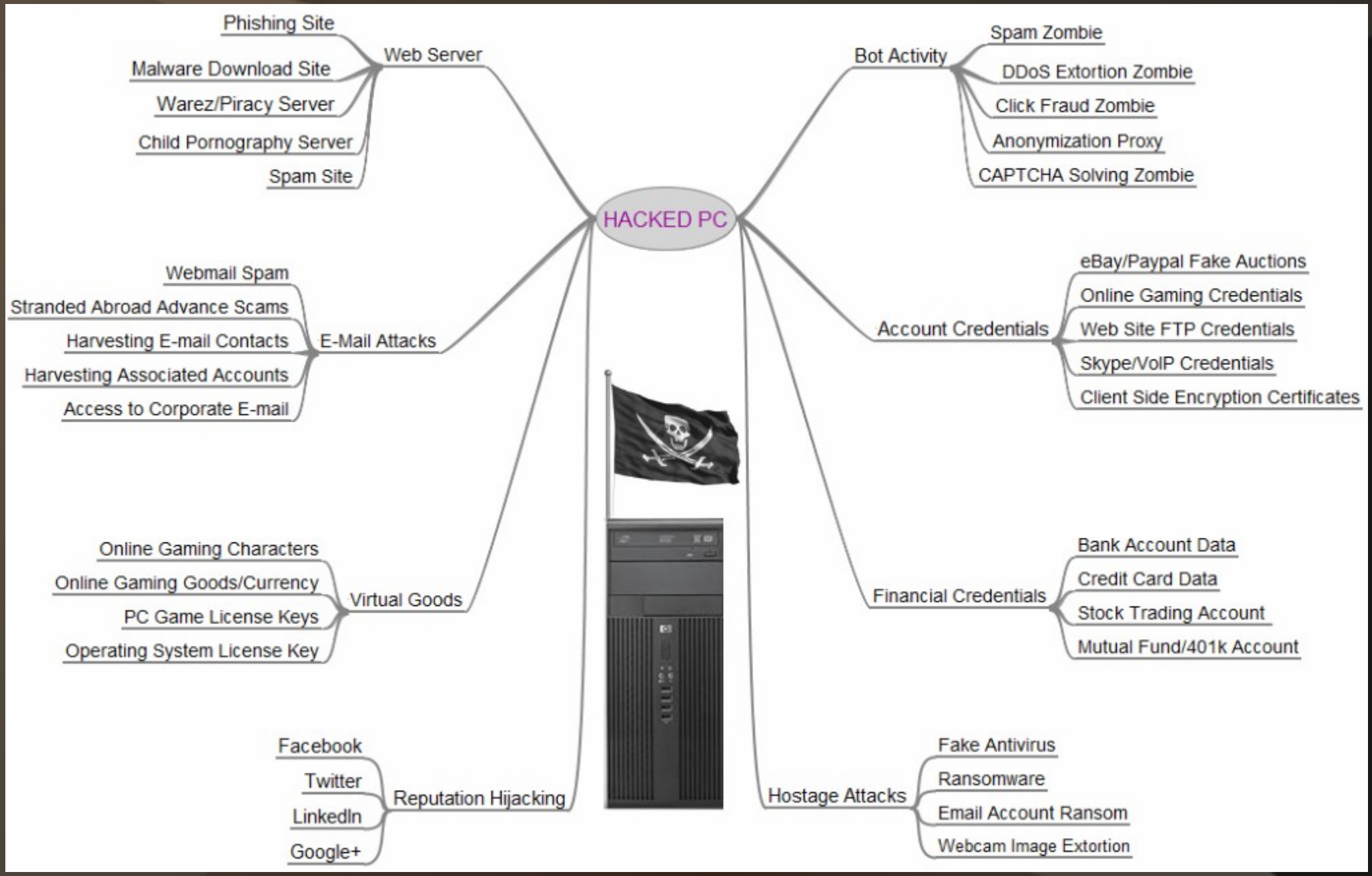


Image credit: krebsonsecurity.com (2012)

Magickal Crypto Pixie Dust

- Code signing was said to make malware harder to install
- Users have been trained to ignore warning windows
- Vendors have been compromised and their code signing certs abused to sign malware
- Code signing doesn't prevent exploitation
- Exploitation means silent installation of malware

Image credit: goth_macros Livejournal community (RIP)

“Trust ME, Bo. Trust ME...”

- Automatic updates are now abused to install malware
- Malware pretends to be updates to Windows, Skype, iTunes and prompts user to install them
- Malware written and sold by commercial entities is packaged this way
- Updates are signed with the right certs, so auto-update installs them without a second thought.
- Surveillance software that bypasses crypto, accesses camera and microphone, records traffic
- Spotted in Middle East, Germany, United States of America...

Some Companies Who Sell Malware

- Gamma International - FinFisher/FinSpy
- Digitask - Bundestrojaner
- Carrier IQ – CarrierIQ (Apple iOS and Android)
- Vupen
- Elaman
- Hacking Team – Remote Control System

Messengers Get Shot

- Professionally hazardous to do security research
  - Jobs can be lost - “Only black hats look for vulns!”
- DMCA takedowns
- Cease and desist orders
- Lawsuits against people who report vulnerabilities
  - More rare in second decade but still a risk

0-days.. get'cher white-hot 0-days!

- Markets where 0-day exploits are sold
- Discoverers don't have to be disclosed, so it's legally safer to find bugs
- Getting paid for doing something fun
- 0-days bought aren't necessarily reported to vendors
- More money made reselling vulnerabilities
- Not many consider what the vulns they sell might be used for

“You know that thing I told you about that one time...?”

- Purchased 0-days used tactically against targets
  - Sensitive government systems
  - Multinational corporations
  - Activists and dissidents
- Flame, Stuxnet, Elderwood, et al first generation of true net.warfare weapons
  - Specific target
  - Tactical and strategic goals
  - Planning and execution of attacks
  - Visible effects have other desirable outcomes

Security Apathy

- Why investigate when you can re-image?
- DevOps and security-by-default are still in beta
  - “I don't care. Get it on line NOW.”
- Some security measures are inherently user-hostile, engendering anti-security attitudes in users
  - Syscall auditing on database servers
  - Requiring debug logging in web apps
- Cost of cleanup, fines <<< cost of proactive security
- RoI of infosec is uncertain
- RoI of cleanup is well understood

Subcritical Mass

- Opportunistic IPsec is too difficult to configure, so most don't bother
- SElinux has a reputation for causing problems, so most people turn it off rather than spend time configuring it
- Hardening is seen as a waste of time
  - “Don't bother, we have a firewall,” syndrome
  - “Security breaks our apps.”
- Antivirus software is better than nothing, but not as effective as is commonly believed
  - Not detected < 10 days, probably won't ever be
- Disk encryption doesn't protect live systems

"PKI Is A Joke In Your Town!"

- CA system doesn't do what it was thought to
- That a cert was signed matters. Who signed it doesn't so long as the browser thinks it trusts the signer.
- Several CAs are known to have been compromised
  - Signing certs copied so arbitrary certs can be made to appear legitimate
  - Fake certs for Google, Facebook, Microsoft, Yahoo, ...
  - Wildcard certs – *.*, *.com, ...
- Some CAs sell wildcart certs for DPI and DLP products to MITM all encrypted services
  - Private companies
  - Governments at the national level

Pwned CAs

- Comodo
- Diginotar
- GlobalSign
- Koninklijke Notariele Beroepsorganisatie
- Stichting TTP Infos

Network Neutrality

- All Internet traffic should be treated equally
- So long as you're not hurting the infrastructure or breaking any laws, you should be able to run whatever apps you want
- Some say QoS counts, some say it doesn't
- Some say that enforcing scarcity of bandwidth and/or tiered bandwidth encourages innovation
  - Make more money, buy more bandwidth
- Some say that this prices innovation out of the hands of many
- Verdict: Sticky wicket. Watch this space.

Twenty-first Century Panopticon

- Data retention required by some governments
  - Australia passed such a bill
  - UK Clean IT Act (pending)
- Happening in the US for over a decade
- Collection of all traffic metadata, sometimes all traffic without prior cause - “Just in case.”
- Captured data has to be kept online so it can be updated
- Vulnerable to compromise and abuse
  - Misuse of CALEA functionality in telco hardware
  - net.filtering infrastructure logging servers
- Never quite sure who's doing the work

- Misuse of data can take many forms
  - Sold to data mining companies
    - Loss of health coverage
    - Loss of jobs
      - Outing people
  - Leaked online
    - Identities of federal agents, their duty posts, financial information
  - Data stewards can misuse their positions
    - Stalking
    - Murder

Intellectual Property Showdown

- Overbroad IP laws make it possible to get most anything taken down
  - Materials specifically in the public domain
  - Internet domains
  - Comments and reviews posted to websites
  - Websites of copyright lawyers
- Memetic attacks against Open Source/Free Culture/Creative Commons
  - Microsoft equated F/OSS with software piracy
  - RIAA, MPAA says Creative Commons == piracy
  - Organizers of a Creative Commons music festival in Leipzig had to pay royalties to GEMA (German RIAA equivalent) for the music played there

What do we do about it?

- Train users more often, not more harshly
  - Positive and negative reinforcement don't work
- Your sysadmins want to lock stuff down. Let them.
  - Put in the time up front to get apps working
  - Script the fixes so it won't take as long later
  - Apply everywhere
- Push back
  - Fight for your right to harden servers
  - Work with whomever you need to get the job done
- Don't punish technicians for being proactive
- Review your code. No, really. Playing Call of Duty at lunchtime doesn't count.

What else can we do?

- Test environments are just that. Build and use them.
  - Would you rather spend that money fixing production servers?
- When someone tells you your idea is insecure, listen to them
  - Security models do not exist to prevent you from doing what you need to do
  - Security models exist to help prevent intruders from abusing your systems
  - If the first thing you do when designing a production app circumvent security protocols to make it run, maybe you're playing on the wrong team
    - Think about that a little.

Comments?

Questions?

That's all, folks!

Thanks for coming!

Let's see the rest of HacDC!