Zero Day: The Business Plan

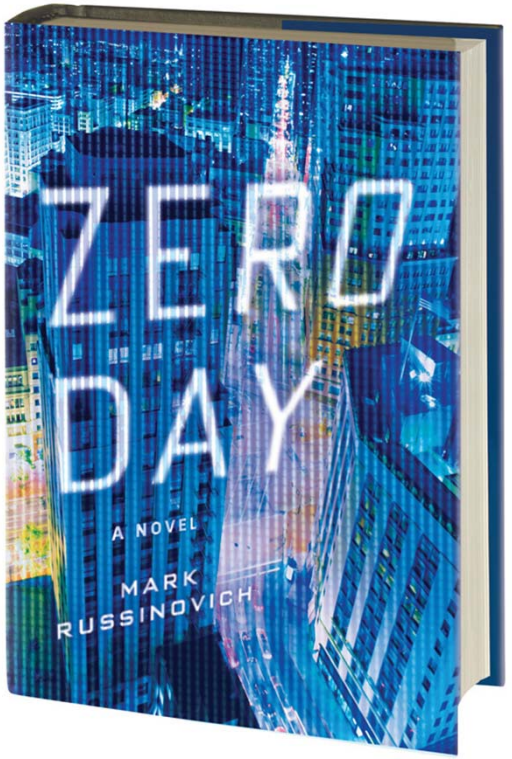
Mark Russinovich
Technical Fellow
Microsoft

Session ID: EXP-402
Session Classification: Intermediate

Zero Day: A Novel
The Idea

- Central idea evolved in the early 2000's from wave of network worms
  - Most written for the hell of it
  - Caused havoc because of side effects
- What if terrorists created a worm?
  - 9/11 attack was about creating fear
  - Could a worm intent on destruction cause major disruption?

Zero Day: A Novel

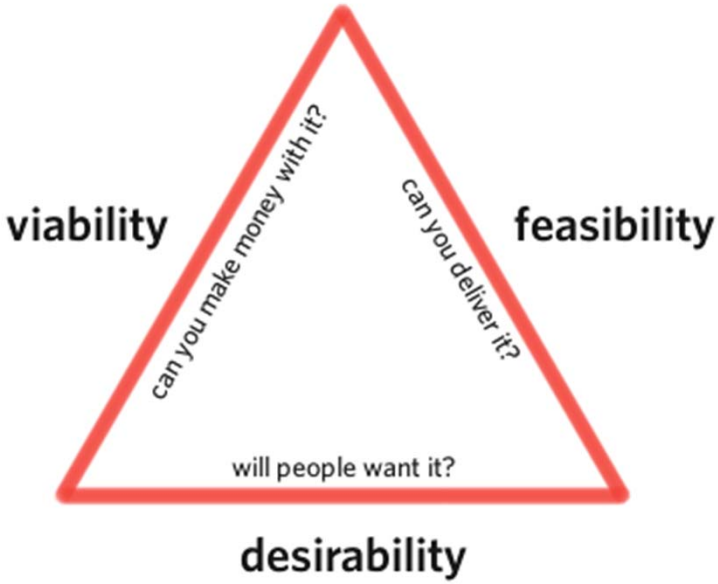


- Finished draft in 2005
  - Found agent
  - Found publisher
  - Iterated on drafts
  - Got blurbs
- Published in March of 2011
  - Considered very successful by publisher
  - Well received by security community
- But does it portray a realistic threat?

The Zero Day Business Plan: Destroy the World (or as much of it as we can)

- Infect lots of systems
- On a trigger date, delete everything

The Zero Day Business Plan: Destroy the World (or as much of it as we can)



- Is it technically feasible?
- Is there means?
- Are there people interested in our plan?
- What do we do about it?

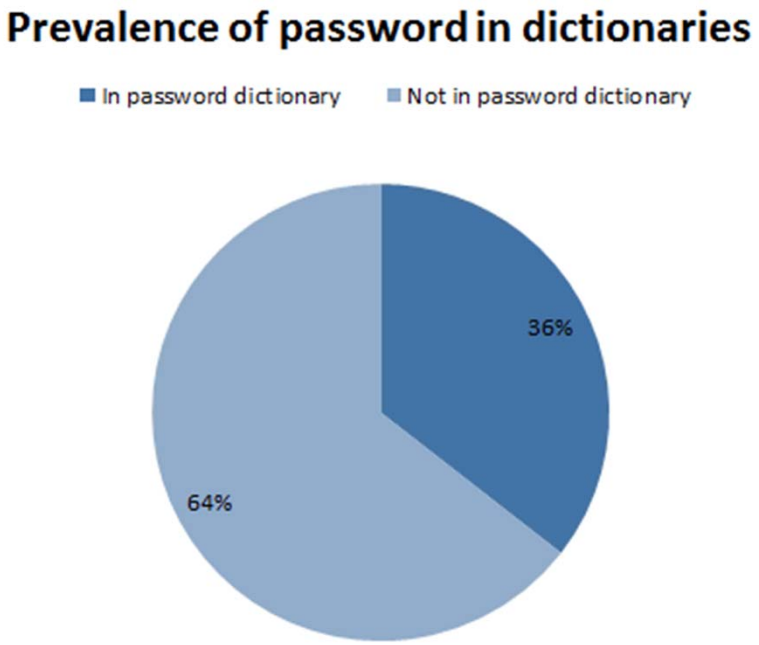
IS IT TECHNICALLY FEASIBLE?

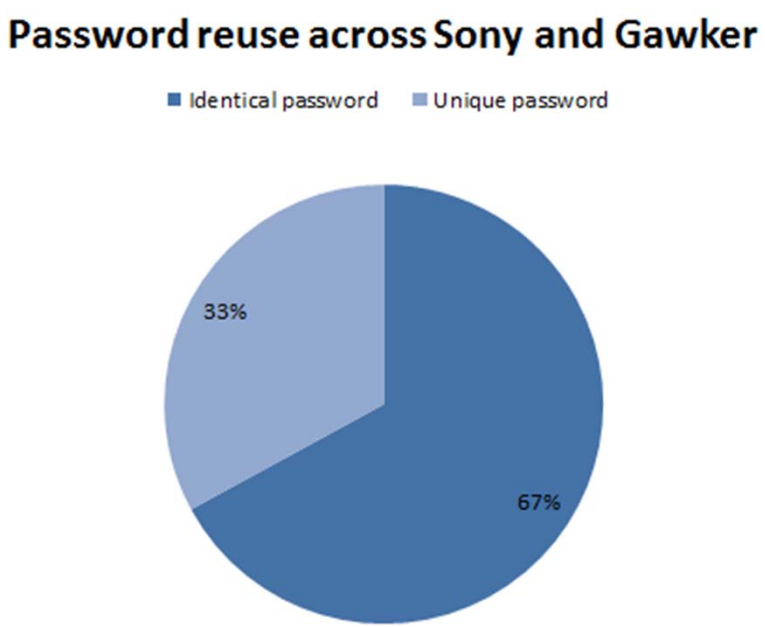
Infecting Lots of Systems

- Zero Days are ideal
  - Can buy them for $2K-125K
  - Hire the right guys to find them for you
- Known vulns are also effective
  - 8% of systems go unpatched
  - 60% of Adobe software is unpatched (getting better)
  - Corporate patch windows are typically 15-60 days

Getting in with Passwords

- Passwords are still notoriously weak
- Sony breach of 1M passwords reveal common usage





Spreading

- Once on a system, relatively easy to spread to others:
  - Keystroke log to obtain passwords
  - “Pass the hash” to spread without actual password
- How far can you spread?
  - Conficker: 8M
  - Mariposa: 12M
  - Shady Rat: infestations at 70 major military, corporate and government organizations

Critical Infrastructure

- Zero Day had examples of infrastructure infections:
  - Plane, factory, nuclear plant

The Epoch Times

Feds Prepare for Cyberterrorism as Old Threats Fade

Stealthy, unannounced infiltrations pose the largest threat

By Joshua Philipp
Epoch Times Staff

Created: February 8, 2012
Last Updated: February 20, 2012

"Ultimately, what we found is the state of ICS security is kind of laughable," McCorkle said.

- Infrastructure is very vulnerable
  - Stuxnet is the canonical example
  - May 2011 pentest breached LA water system in 12 hours
  - Hospital system infections are "routine"
  - DHS, White House, DoD, say US is at risk

Remaining Undetected

- Most effective damage is all at once
  - Minimal symptoms and side effects
  - No chance to react
- Have to spread and stay hidden until attack date
  - Hide in plain site
  - Rootkits
  - Memory-resident-only malware

Damage

- Deleting all accessible data is easy
  - Deletes all files user can access
  - With administrator rights, makes system unbootable
- What about other data stores?
  - Deleting SQL databases
  - Deleting email
- Flashing BIOS truly bricks a system
  - Open source flashing kit available
  - Malware already in the wild: Trojan.Mebromi

IS IT VIABLE?

How Much will this Cost?

- What does a hacker cost?
  - Professional software developer makes $100K/year
  - Russian hackers make $20-70K/year
  - Developers don't need to know what they're working on
- Reasonable to expect attackers to be able to fund several man-years of decent hacking
  - al Qaeda made $30M/yr before 9/11

Malware Kits Lower the Bar

- Plenty of kits for constructing malware available for pay and free

- Recently, virulent Ramnit virus combined Zeus Trojan with other off-the-shelf malware

IS THERE DESIRABILITY?

What about “For the Hell of It”?

- Many viruses delete various types of files
- Many people have asked where they can get a destructive virus:

Hacktivists

- Have already shown willingness to go after government
- Leaked DHS memo says fear of Anonymous going after infrastructure:

The Washington Times

NEWS | OPINION | CAMPAIGN 2012 | SPORTS | BOOKS | LIFE | BLOGS | COMMUNITIES | MULT

POLITICS | NATIONAL | WORLD | SECURITY | ECONOMY | D.C. LOCAL | NEWSMAKERS | Inside the

HOME ▸ NEWS ▸ SECURITY LOG IN | E-MAIL ALERTS

Hacker group threatens industrial computer systems

By Shaun Waterman - The Washington Times Monday, October 17, 2011

Traditional Terrorists

- Al Qaeda has been using Internet for training since before 2004
  - In addition to propaganda
- Al Qaeda Internet usage guidelines include:
  - Changing Internet cafés
  - Pasting messages to avoid long Internet connections
  - Exchanging messages in files on compromised systems

Al Qaeda and Cyberterrorism

- After Bin Laden's death, al Qaeda called for cyber-jihad

- US Administration, British Intelligence, and FBI all believe al Qaeda will use cyberterrorism

“Pig in Boots” Attack

- In fact, al Qaeda has already attacked:

WHAT DO WE DO ABOUT IT?

Impact of a Zero Day Attack

- Hard to gauge costs
  - Effectiveness of spreading
  - Secondary-impacted systems
  - Critical infrastructure
- Much milder attacks than Zero Day's have cost billions
  - Conficker: $9.7B
  - SoBig: $37.1B

Zero Day: We're Living the Non-Fiction

- All aspects of Zero Day are in operation today
- Someone with motivation just has to put it all together
- Even on small scale, damage would greatly exceed all previous viruses

How do We Prevent the Zero Day Business Plan?

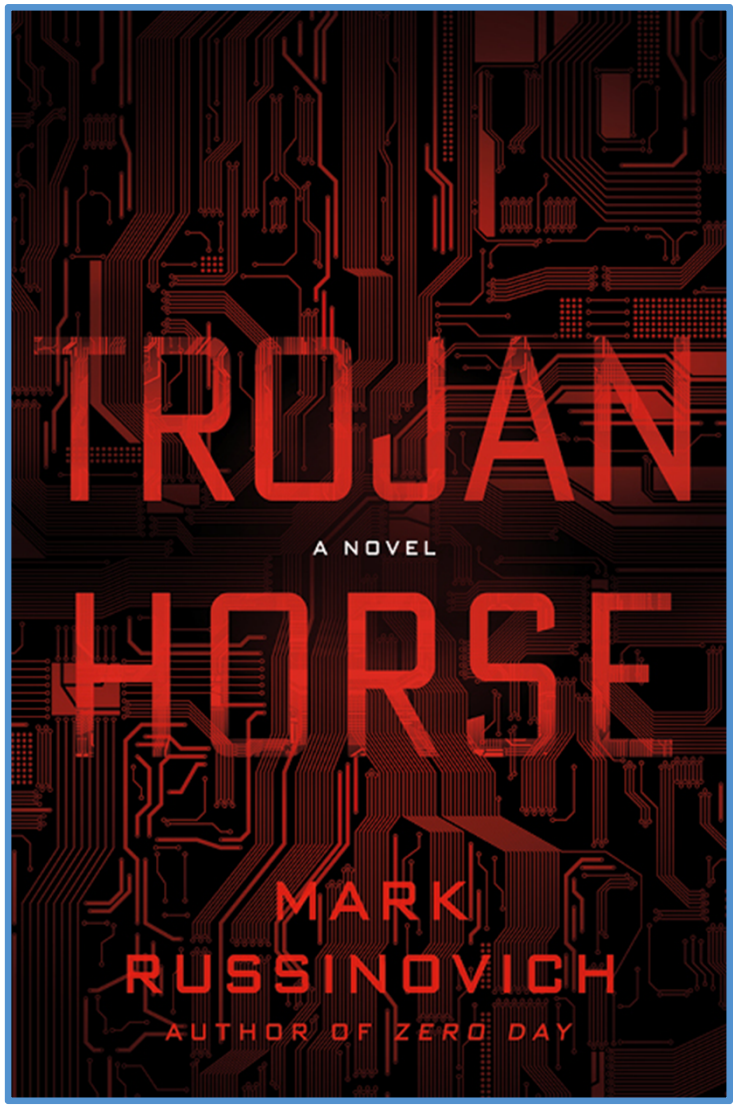
- Good news: the world is waking up to cyber threats
  - NERC has become more vigilant
  - Congress is starting to pass more legislation
  - Focus on securing power grid
  - Mobile devices and printers adopting firmware flash protection
- Bad news: daily headlines show there's a lot of work to do

Everyone Has a Role

- Home users:
  - A/V
  - Unique and strong passwords
  - Patching
  - Latest software releases
  - Backup
  - Least privilege
- IT - all the above plus:
  - Whitelisting
  - Network segmentation
  - Monitoring and auditing with analysis
- This community:
  - Lobby for cybersecurity incentives and regulation

Trojan Horse: A Novel

- Sequel to Zero Day
- State-sponsored cyber-espionage
- Available in September
- Forward by Kevin Mitnick



To me it feels like it is Sept. 10, 2001. The system is blinking red — again. Yet, we are failing to connect the dots — again."

Senator Joe Lieberman
Testimony to Congress
2/17/2012