Exploit/Attack Lifecycle

Noid, jerk
Who am I?

- By Day: Security PM for Microsoft
- INFRAGARD Member
- Organizer for DEFCON

- Organizer of LayerOne
What’s This All About?

- As we become more organized in our approach to security, our adversaries are adapting to counter us
- Exploit Development and Attack Lifecycles are speeding up
- They’re learning from us as we learn from them
That Was Then
This is Now

Major Canadian hacker ring cracked
The Mounties always get their man
Written by Robert Jaques
wnnet.com, 21 Feb 2008

Chinese waging online spy war
Jasem Kouloukis
February 10, 2008

CHINESE computer hackers have launched several targeted attacks on highly classified Federal Government computer networks, prompting an internal review of IT security.

Hacker arrested in Greece for stealing, selling weapons data
Jim Carr
January 30, 2008

Authorities have arrested a 58-year-old man in Greece they said hacked into computer systems of France's Dassault Group for more than five years, stole sensitive weapons technology data and sold it to a variety of countries.

20-Year-Old Arrested for Estonian Cyber Attacks
Posted Jan 25th 2008 11:26AM by Tim Stevens
Filed under Computers

Mega-D Botnet Overtakes Storm, Accounts for 32% of Spam
Posted by Cmrd Taco on Sat Feb 02, 2008 02:23 PM

Stony Stevenson writes

"The new Mega-D Botnet has overtaken the notorious Storm worm botnet as the largest single source of the world's spam, according to security vendor Marshal. This botnet currently accounts for 32 percent of all spam, 11 percent more than the Storm botnet which peaked at 21 percent in September 2007. It started about 4 months ago but has been steadily increasing since then. It sends spam headlines to trick victims into opening the spam, a technique Storm worm uses."

Exploit code for Microsoft Works flaw available: US-CERT
Jim Carr
February 19, 2008

The United States Computer Emergency Readiness Team (US-CERT) has warned that exploit code is publicly available for a critical MS08-011 vulnerability that affects the Microsoft Works 6 file converter.
Current Trends

- Increased Collaboration
- Increased Incentive
  - Money
  - State Sponsorship
- Developing Methodologies
- Increased Availability of Tools
Money is the ultimate motivator
More than ever there is financial incentive for the vulnerability researcher and exploit developer
Some of these ‘exploit auction houses’ are legit, but the vast majority are black market
The More Things Change...

- Continuing to see the ‘same old’ exploits
  - Stack/Heap based attacks
  - Race Conditions
  - XSS
  - SQL Injection

For reference, Aleph1 wrote his (in)famous ‘Smashing the Stack For Fun and Profit’ paper in 1996
Attack Life Cycle

Create or Acquire exploitation methods or attack vectors

Collaborate with or train others

Gather or acquire compromised hosts

Attack high value targets

Analyze resulting data and make modifications
Put Them Together And...

- Decreased time between vulnerability identification and exploit
- Time to exploit in 2004 was 5.8 days
- Current time to exploit is half that
Contributing Factors

- ‘Copy Cat’ exploits with different payloads
  - Harder to keep abreast of if what we are looking for keeps changing
- Exploit creators learning from intelligence gathered in prior attacks
- Use of BotNets to propagate exploit code at a record pace
- Attackers know more about their target OS’ than ever before
They’re using the same tools we use and then some

- Fuzzing
- Web Application Fuzzing
- Metasploit
- MSF–XB
Security product vendors including pre-disclosure signatures acquired through vulnerability purchase programs in their products

Attackers can use these signatures to pinpoint vulnerabilities and exploit vectors before full disclosure occurs
OK, I get it. We’re Hosed
We Have A Chance To Learn

- Attacker loses the element of surprise
- Attacker exposes the nature of his exploit
- We can begin to learn about their methodologies, strategies, and development cycles
How Does This Help?

- We can alter Defense in Depth to meet the changing nature of the threats
- We can spend more resources on the areas where the attackers are focusing theirs
How do we Buy More Time?

- Defense in Depth / Layered Security
  - Developers, don’t assume networking is handling your security needs
  - Ops, don’t assume the developers handled security in their code
  - More intensive testing prior to release
  - Be enterprise focused and holistic
Take Away’s

- Attackers know more than ever
- Attackers have more incentive than ever
- Attackers are more organized than ever
- They learn from us, we need to keep learning from them
Thanks For Your Time

Q&A
noid@dc206.org