Worms & Botnets

CS 161: Computer Security
Prof. Vern Paxson

TAs: Devdatta Akhawe, Mobin Javed & Matthias Vallentin

http://inst.eecs.berkeley.edu/~cs161/

April 21, 2011
Announcements

• HKN reviewing today, 12:15PM

• Final exam will be in F295 Haas
  – This is not Haas Pavilion!
  – Haas School of Business, east side of campus near Gayley

• Course Summary lecture
  – For sure works best if you take advantage of the opportunity to ask questions …
    • … including sending them in advance
Large-Scale Malware

- **Worm** = code that self-propagates/replicates across systems by arranging to have itself immediately executed
  - Generally infects by altering *running* code
  - No user intervention required

- **Botnet** = set of compromised machines (“bots”) under a common command-and-control (C&C)
  - Attacker might use a worm to get the bots, or other techniques; orthogonal to bot’s use in botnet
The worm dies off globally!

Measurement artifacts

Number of new hosts probing 80/tcp as seen at LBNL monitor of 130K Internet addresses
Modeling Worm Spread

• Worm-spread often well described as *infectious epidemic*
  – Classic SI model: homogeneous random contacts
  • SI = Susceptible-Infectible

• Model parameters:
  – $N$: population size
  – $S(t)$: susceptible hosts at time $t$.
  – $I(t)$: infected hosts at time $t$.
  – $\beta$: contact rate
    • How many population members each infected host communicates with per unit time
    • E.g., if host scans 10 Internet addresses per unit time, and 2% of Internet addresses run a vulnerable server, then $\beta = 0.2$

• Auxiliary parameters reflecting the relative proportion of infected/susceptible hosts
  – $s(t) = S(t)/N$ \quad $i(t) = I(t)/N$ \quad $s(t) + i(t) = 1$
Computing How An Epidemic Progresses

• In continuous time:

\[
\frac{dI}{dt} = \beta \cdot I \cdot \frac{S}{N}
\]

Increase in # infectibles per unit time

Total attempted contacts per unit time

Proportion of contacts expected to succeed

• Rewriting by using \( i(t) = \frac{I(t)}{N}, S = N - I \):

\[
\frac{di}{dt} = \beta i(1 - i) \quad \Rightarrow \quad i(t) = \frac{e^{\beta t}}{1 + e^{\beta t}}
\]

Fraction infected grows as a logistic
Fitting the Model to Code Red

Exponential initial growth

Growth slows as it becomes harder to find new victims!
Spread of Code Red, con’t

- Recall that # of new infections scales with contact rate $\beta$
  \[ \frac{dI}{dt} = \beta \cdot I \cdot \frac{S}{N} \]
- For a scanning worm, $\beta$ **increases** with $N$
  - Larger populations infected more quickly!
    o More likely that a given scan finds a population member
- Large-scale monitoring finds 359,104 systems infected with Code Red on July 19
  - Worm got them in 13 hours
- That night ($\Rightarrow 20^{th}$), worm dies due to DoS bug
- What happens on August 1st?
Activity starts a bit *early* due to systems with inaccurate clocks!
This is what seeded the *reinfection*!

Secondary peak due to home systems coming on in the evening

Reinfection about 1/2 as big as original

(Again from LBNL monitoring)
Code Red 2

• Released August 4, 2001 (3 days later!)
• Exploits same IIS vulnerability
• String inside the code: “Code Red 2”
  – But in fact completely different code base.
• Payload: a root backdoor, resilient to reboots.
• Bug: crashes NT, only works on Win2K.
• Kills original Code Red.
• *Localized scanning*: prefers nearby addresses.
• *Safety valve*: programmed to die Oct 1, 2001.
Striving for Greater Virulence: *Nimda*

- **Multi-mode spreading:**
  - attack IIS servers like Code Red & Code Red 2
  - email itself to address book as a virus
  - copy itself across open network shares
  - modify Web pages on infected servers with browser exploit
  - scan for Code Red 2 backdoors (!)
    \[ \Rightarrow \text{Worms form an ecosystem!} \]
- **Leaped across firewalls**
  - Ravaged sites that lacked “institutional antibodies”

**Note:** in some ways a virus, in some ways a worm.
Code Red 2 kills off Code Red 1

Code Red 2 settles into weekly pattern

Nimda enters the ecosystem

Code Red 2 dies off as programmed

CR 1 returns thanks to bad clocks
Code Red 2 dies off as programmed. Nimda hums along, slowly cleaned up.
With its predator gone, Code Red 1 comes back!, still exhibiting monthly pattern
Life Just Before Slammer

Sat Jan 25 05:29:00 2003 (UTC)
Number of hosts infected with Sapphire: 0
Life Just After Slammer
Going Fast: **Slammer**

- Slammer exploited **connectionless** UDP service, rather than connection-oriented TCP

  - *Entire worm* fit in a single packet!
    - When scanning, worm could “fire and forget” *Stateless!*

- Worm infected 75,000+ hosts in **10 minutes** (despite broken random number generator).
  - At its peak, **doubled every 8.5 seconds**
The Usual Logistic Growth

Probes Recorded During Code Red's Reoutbreak

Number Seen in an hour

Hour of the day

# of scans  Predicted # of scans
Slammer’s Growth

DShield Probe Data

What could have caused growth to deviate from the model?

Hint: at this point the worm is generating 55,000,000 scans/sec

Answer: the Internet ran out of carrying capacity! (Thus, β decreased.) Access links used by worm completely clogged. Caused major collateral damage.
Further Worm Developments

• Malicious payloads (disk-trashing)
• Global outbreaks within 24 hours of vulnerability disclosure
• “Server” exploited for infection is a NIDS
• Single outbreak of > 15 million infectees
• “Counterworm” released to clean up original worm …
  – … oh and install a root backdoor
• DoS’ing *Windows Update* as a worm spreads
• Worms that use Google to search for victims
Step-By-Step Guide: Embedded Windows Media in Firefox... Jan 26, 2005... For pre-1.0 versions of Firefox (also under Windows), see this earlier version of this guide: http://forums.mozillazine.org/viewtopic.php?t=140828.

forums.mozillazine.org/viewtopic.php?t=206213 - Cached - Similar
[Ext] Fission 0.8.9 [Sep 25] • mozillaZine Forums - 15 posts - Jan 19, 2006
[Ext] Console² 0.1 to 0.3.6.2 • mozillaZine Forums - 15 posts - Sep 17, 2005
Quicktime/Real/Windows Media Player Issues... - 3 posts - Jan 25, 2005
keyconfig 20080929 • mozillaZine Forums - 15 posts - Jul 29, 2004
More results from forums.mozillazine.org »

phpBB • View topic - howdark.com exploits - follow up
1 post - 1 author - Last post: Nov 18, 2004
In the mean time we strongly, and I mean strongly! urge all our users to make the following change to viewtopic.php as a matter of urgency...

www.phpbb.com/community/viewtopic.php?t=240513 - Cached - Similar
phpbb • View topic - Preventing SPAM - Bots... - Mar 19, 2007
phpBB • View topic - phpBB 2.0.16 released - Jun 26, 2005
More results from phpbb.com »

GREYSCALE & COLOUR CALIBRATION FOR DUMMIES
Written by Kal, Editor/Webmaster www.CurtPalme.com Home Theater Last updated on June 6, 2009 (fixed some minor typo's)...

Stuxnet

• Discovered July 2010. (Released: Mar 2010?)

• **Multi-mode spreading:**
  – Initially spreads via USB (virus-like)
  – Once inside a network, quickly spreads internally using Windows RPC

• **Kill switch:** programmed to die June 24, 2012

• **Targeted** SCADA systems
  – Used for industrial control systems, like manufacturing, power plants

• Symantec: infections **geographically clustered**
  – Iran: 59%; Indonesia: 18%; India: 8%
Stuxnet, con’t

• Used four Zero Days
  – Unprecedented expense on the part of the author

• “Rootkit” for hiding infection based on installing Windows drivers with valid digital signatures
  – Attacker stole private keys for certificates from two companies in Taiwan

• Payload: do nothing …
  – … unless attached to particular models of frequency converter drives operating at 807-1210Hz
  – … like those made in Iran (and Finland) …
  – … and used to operate centrifuges for producing enriched Uranium for nuclear weapons
Stuxnet, con’t

• Payload: do nothing …
  – … unless attached to particular models of frequency converter drives operating at 807-1210Hz
  – … like those made in Iran (and Finland) …
  – … and used to operate centrifuges for producing enriched Uranium for nuclear weapons

• For these, worm would **slowly increase** drive frequency to 1410Hz …
  – … enough to cause centrifuge to **fly apart** …
  – … while sending out fake readings from control system indicating everything was okay …

• … and then **drop it back to normal range**
Israel Tests on Worm Called Crucial in Iran Nuclear Delay

By WILLIAM J. BROAD, JOHN MARKOFF and DAVID E. SANGER
Published: January 15, 2011

This article is by William J. Broad, John Markoff and David E. Sanger.

The Dimona complex in the Negev desert is famous as the heavily guarded heart of Israel’s never-acknowledged nuclear arms program, where neat rows of factories make atomic fuel for the arsenal.

Over the past two years, according to intelligence and military experts familiar with its operations, Dimona has taken on a new, equally secret role — as a critical testing ground in a joint American and Israeli effort to undermine Iran’s efforts to make a bomb of its own.

Behind Dimona’s barbed wire, the experts say, Israel has spun nuclear centrifuges virtually identical to Iran’s at Natanz, where Iranian scientists are struggling to enrich uranium. They say Dimona tested the effectiveness of the Stuxnet computer worm, a destructive program that appears to have wiped out roughly a fifth of Iran’s nuclear
Worm Take-Aways

• Potentially enormous reach/damage ⇒ *Weapon*
• Hard to get right
• Emergent behavior / surprising dynamics
• Institutional antibodies
• **Remanence**: worms stick around
  – E.g. Nimda & Slammer still seen in 2011!
• *Propagation faster than human response*
• What about fighting a worm using a worm?
  – “White worm” spreads to disinfect/patch
  – Experience shows: likely not to behave predictably!
  – Additional issues: legality, collateral damage, target worm having already patched so white worm can’t access victim
Botnets
Botnets

• Collection of compromised machines (bots) under (unified) control of an attacker (botmaster)
  – Launch a worm / virus / drive-by infection / etc.

• Method of compromise decoupled from method of control

  • Upon infection, new bot “phones home” to rendezvous w/ botnet command-and-control (C&C)

• Lots of ways to architect C&C:
  – Star topology; hierarchical; peer-to-peer
  – Encrypted/stealthy communication

• Botmaster uses C&C to push out commands and updates
Fighting Bots / Botnets

• How can we defend against bots / botnets?
  • Approach #1: prevent the initial bot infection
    – Because the infection is decoupled from bot’s participation in the botnet, this is equivalent to preventing malware infections in general … HARD

• Take down the C&C master server
  – Find its IP address, get associated ISP to pull plug

• Botmaster countermeasures?
  – Counter #1: keep moving around the master server
    • Bots resolve a domain name to find it
    • Rapidly alter address associated w/ name ("fast flux")
  – Counter #2: buy off the ISP …
Termed \textit{Bullet-proof hosting}

\textbf{Hosting Plans}

We offer a complaint-resistant hosting to host your sites, which are specified in mass mailings.

We decided to bring visitors to your web site through unsolicited mass emails? Wonderful idea! You certainly expect a boom visits. But! As in any ointment and then not pass without a spoon of tar ... Alas, but your wonderful site, shortly after the start of spam mail, will be closed due to flood of complaints from postal services. Is there a way to avoid these problems? Of course! Our complaint-resistant hosting simply ignores any complaints, all postal services, and you can be rest assured about the performance of their sites - they will not be closed. And you get new customers, expand their business and increase their sales and revenue, thanks to spam mailing lists.
Obuzoustoychivy hosting is more expensive than usual, but you will have the full guarantee that your site no one ever closes, it will always be available to your customers!

<table>
<thead>
<tr>
<th>MINI PLAN</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume disc</td>
<td>400 MB</td>
<td></td>
</tr>
<tr>
<td>Domains</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Traffic *</td>
<td>Unlimited</td>
<td></td>
</tr>
<tr>
<td>FTP-access</td>
<td>there is</td>
<td></td>
</tr>
<tr>
<td>MySQL database</td>
<td>there is</td>
<td></td>
</tr>
<tr>
<td>Control panel</td>
<td>there is</td>
<td></td>
</tr>
<tr>
<td>COST</td>
<td>4 000 rub. / 1 month.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>STARTER PLAN</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume disc</td>
<td>500 mb</td>
<td></td>
</tr>
<tr>
<td>Domains</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Traffic *</td>
<td>Unlimited</td>
<td></td>
</tr>
<tr>
<td>FTP-access</td>
<td>there is</td>
<td></td>
</tr>
<tr>
<td>MySQL database</td>
<td>there is</td>
<td></td>
</tr>
<tr>
<td>Control panel</td>
<td>there is</td>
<td></td>
</tr>
<tr>
<td>COST</td>
<td>5 000 rub. / 1 month.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>BUSINESS PLAN</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume disc</td>
<td>1000 mb</td>
<td></td>
</tr>
<tr>
<td>Domains</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>Traffic *</td>
<td>Unlimited</td>
<td></td>
</tr>
<tr>
<td>FTP-access</td>
<td>there is</td>
<td></td>
</tr>
<tr>
<td>MySQL database</td>
<td>there is</td>
<td></td>
</tr>
<tr>
<td>Control panel</td>
<td>there is</td>
<td></td>
</tr>
<tr>
<td>COST</td>
<td>7 000 rub. / 1 month.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PREMIUM PLAN</th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Volume disc</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Domains</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Traffic *</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FTP-access</td>
<td></td>
<td></td>
</tr>
<tr>
<td>MySQL database</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Control panel</td>
<td></td>
<td></td>
</tr>
<tr>
<td>COST</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>