Scan Activity Seen At LBL
The Worm Era Begins

Scan Activity Seen At LBL

# Hosts Scanning / Day

Year

Scanning Activity Seen @ LBNL

Incoming Connections

Year


100 1K 10K 100K 1M 10M 100M

All
Scanners
Non-Scanners
Services Scanned Over Time
Daily Patterns Seen in 1023/TCP Scans

/16 at LBL, sampled 1-in-1K
(a) Agobot Sources: UW I
(b) Agobot Sources: UW II
Blocking Scans at LBNL

Scan Drops / Day

Year

2007 2008 2009 2010 2011 2012
User Populations

Characteristics overlap of legitimate users and bruteforceRs

Forgotten usernames/passwords

Have past history of successful logins

LOW-RATE DISTRIBUTED BRUTEFORCERS

Distributed across networks; the network being monitored sees only a few hits

Have a high rate of logins compared to distributed
Dataset

• **SSH syslog** login records collected at Lawrence Berkeley National Laboratory (LBNL)
  
  – LBNL has two /16 address blocks

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>SSH servers</td>
<td>2,243</td>
</tr>
<tr>
<td>Valid users</td>
<td>4,364</td>
</tr>
<tr>
<td>Mean daily password login attempts</td>
<td>486 (σ ≈ 183)</td>
</tr>
<tr>
<td>Mean daily users</td>
<td>116 (σ ≈ 32)</td>
</tr>
<tr>
<td>Total attempts using passwords</td>
<td>5.3M (1/4 successes)</td>
</tr>
</tbody>
</table>

*Excludes: Key-based logins and readily detectable high-rate brute-forcers.*

• Complemented by SSH flow data
Figure 1: Empirical CDF of the number of failed login attempts per hour until a success for legitimate user login efforts with forgotten or mistyped usernames/passwords.
Aggregate Site Analyzer

Site-wide parameter: **Global Failure Indicator (GFI)**

– Site-wide # of failed logins per batch of x logins