Open Discussion about Worms

CSC 154

Paper to discuss

- Authors: S.Staniford and V. Paxson and N. Weaver.
- Title: How to 0wn the Internet in Your Spare Time.
- Publication: Proceedings of the 11th USENIX Security Symposium, pages 149-167, San Francisco, CA, August 2002

Questions

- Why do we choose this paper?
  - High quality paper showing you how to write professionally;
  - Attacker's perspective;
- Worm features?
  - Self replication without human intervention;
  - Fast propagation;
- Worm's general working mechanism?
  - Loop(vulnerability scan->exploit vulnerability->scan for other vulnerable hosts);

Questions

- Why do you think worm is dangerous?
  - Especially, the propagation speed is a nightmare for defenders due to limited response capability!
  - Other possible harm may be brought by worms;
- Code Red I vs. Code Red II vs Nimda
  - Code Red I: v1 has a bug; v2 fixed it, added DDoS towards whitehouse.gov, and turned itself on/off;
  - Code Red 2: different code base, same exploit, added local scanning, and killed itself;
  - Nimda: multi-vector approach;
- warhol worm vs. flash worm
  - Hit-list scanning and permutation scanning (warhol worm)
  - Internet-sized hit-lists (flash worm) (internet killed in 30s);

Questions

- How fast can worm propagate?
  - Random Constant Spread model
    - Complex with parameters;
    - Fit well the real data;
  - Simple model: exponential rate
    - s: Search time to find a vulnerable host;
    - i: infection time to take a host;
    - $2^{(t/(s+i))}$

Questions

- What major techniques can worms employ for speed up?
  - Hit-list scanning;
  - Permutation scanning;
  - Topological scanning;

- And their benefits?
  - Pre-knowledge of potential vulnerable hosts, quick division and shrink; “getting-off the ground” earlier;
  - Self co-ordination for minimized duplication of efforts;
  - Take advantage of local host information (like Email contacts and P2P neighbor link information) for more homogeneous victims; firewall bypassed;

Questions

- Stealth worm
  - Slower, but harder to detect
    - Patience is important;
  - Like contagious disease
  - Good candidates: P2P applications with vulnerability
    - Neighbor link information maintained;
    - Tend to transfer large files;
    - Not-mainstreamed, less attention from IDS;
    - User hosts with sensitive information;
    - Grey content

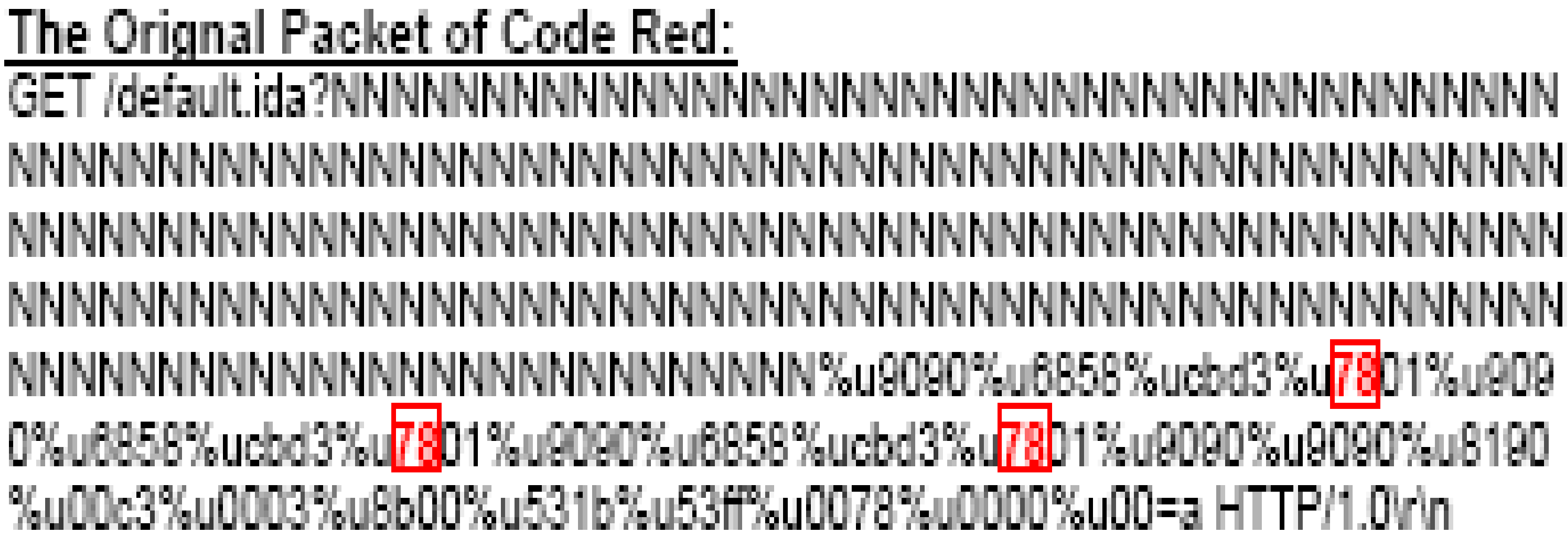
Questions

- What concepts from our lectures are mentioned in this paper?
  - DoS, Virus, worm, buffer overflow, malicious applets;
  - vulnerability, scanner, exploit, backdoor;

- Do you find any interesting points in this paper?
  - Exploit has bug?
  - Different variants of same authored worm compete?
  - Internal working mechanism still unknown?
  - Analogous to epidemics (contagious disease) in natural world?
  - Worm author has comment statement in exploit code?
  - Nimda worm/virus?
  - The internet gets killed in 30s? Impossible?
  - Software with backdoor installed?

Any future solution? Limitation?

- Good behavior: patching systems, using diverse vendors;
- Filtering: look for unusual patterns and drop them;
  - Inside the Bad Packet



The Orignal Packet of Code Red:

```
GET /default.ida?NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN
NNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNNN%u9090%u6858%ucbd3%u7801%u909
0%u6858%ucbd3%u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190
%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=a HTTP/1.0\r\n
```