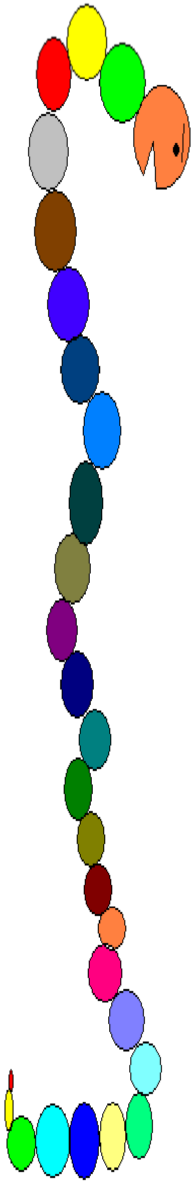
TEAM

ANTI-VIRUS

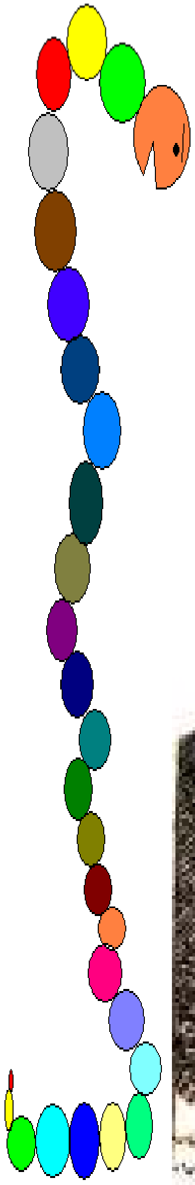


A Look at Defense in Depth

The re-evaluation

Kenneth L. Bechtel, II

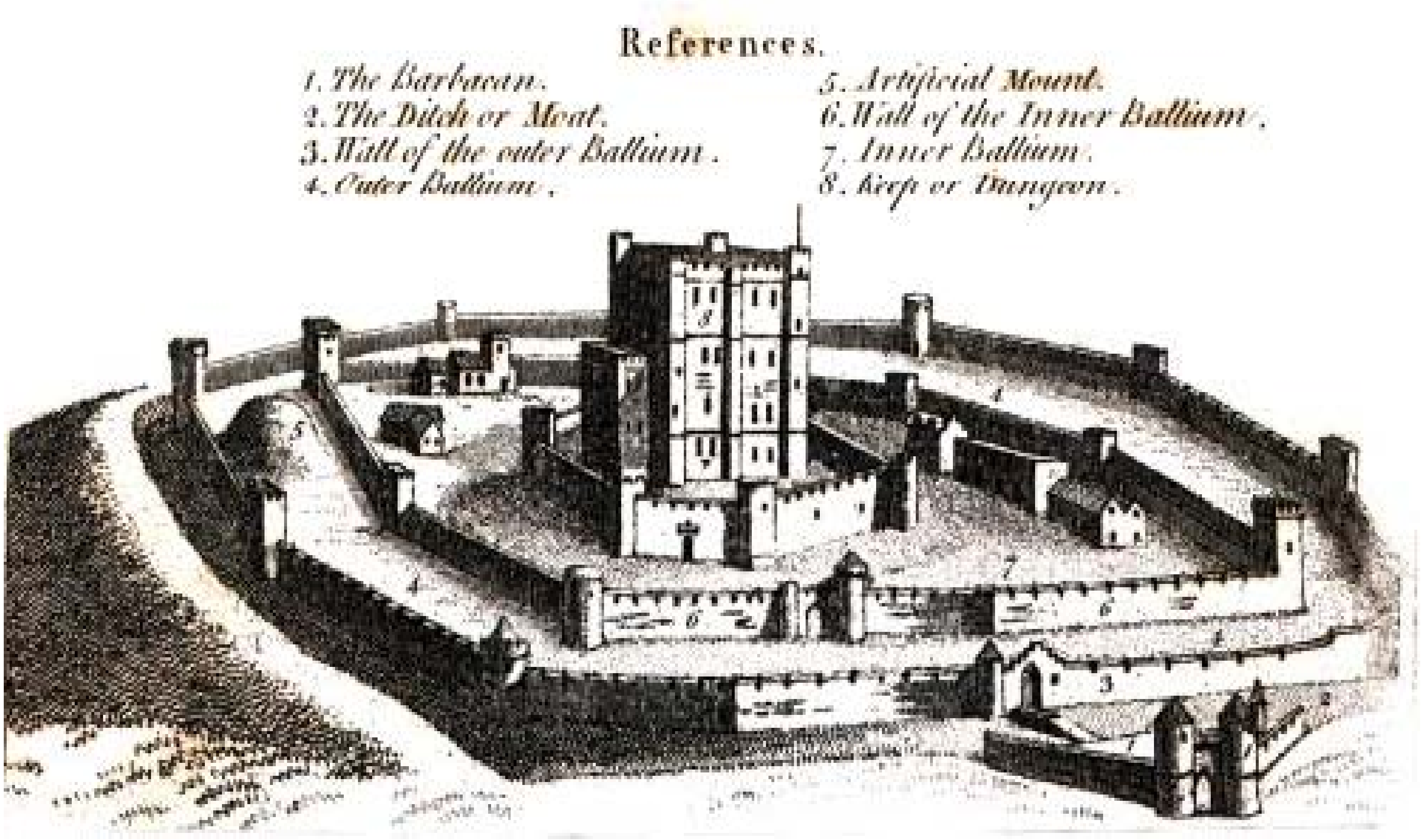
kbechtel@teamanti-virus.org



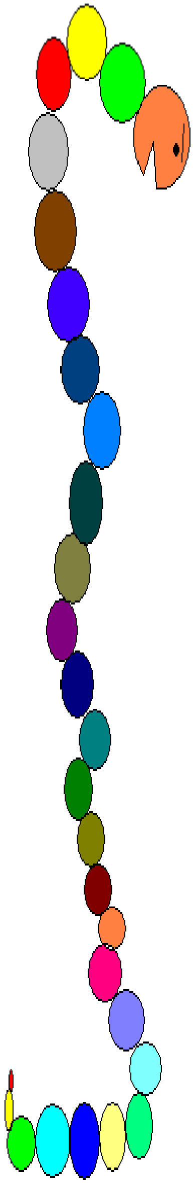
The original Defense

TEAM

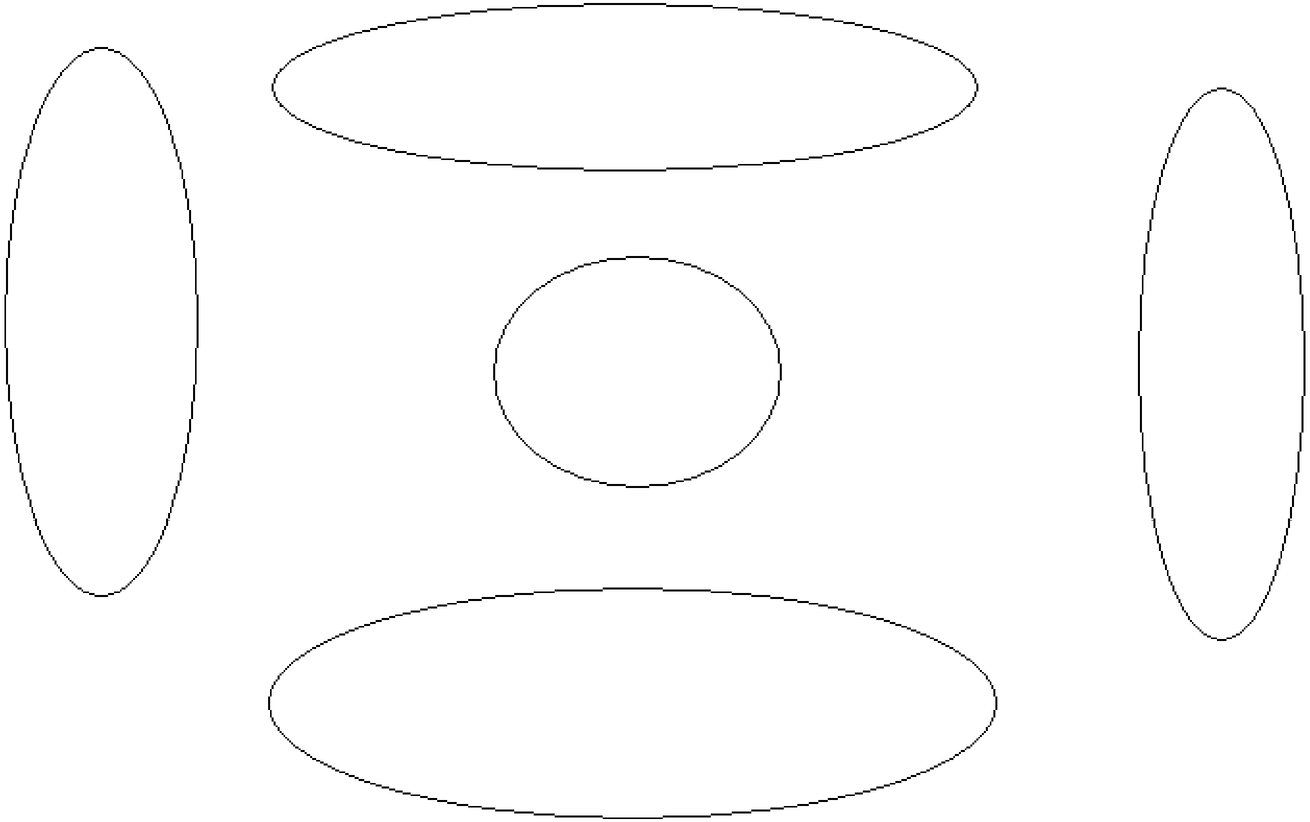
ANTI-VIRUS



TEAM ANTI-VIRUS



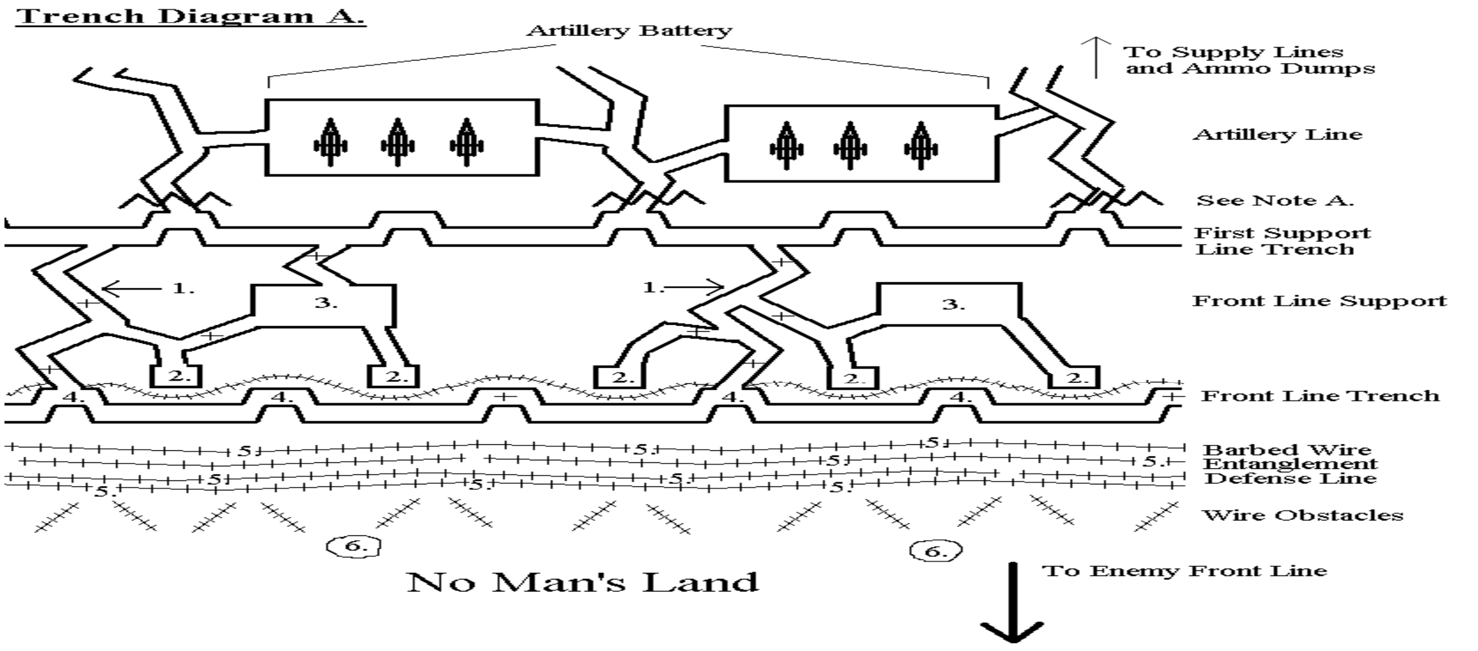
Distributed Defense



TEAM

ANTI-VIRUS

Closer look



Key

Note A. Ususally in between the first support line trench and the artillery line there would be two or three more support trench lines. This diagram has been condensed.

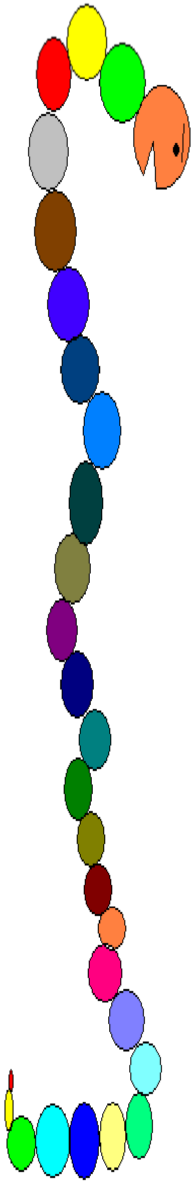
1. Communication Trench
2. Machine Gun Nest
3. Underground Bunker
4. Traverse
5. Wire Break
6. Listening Post

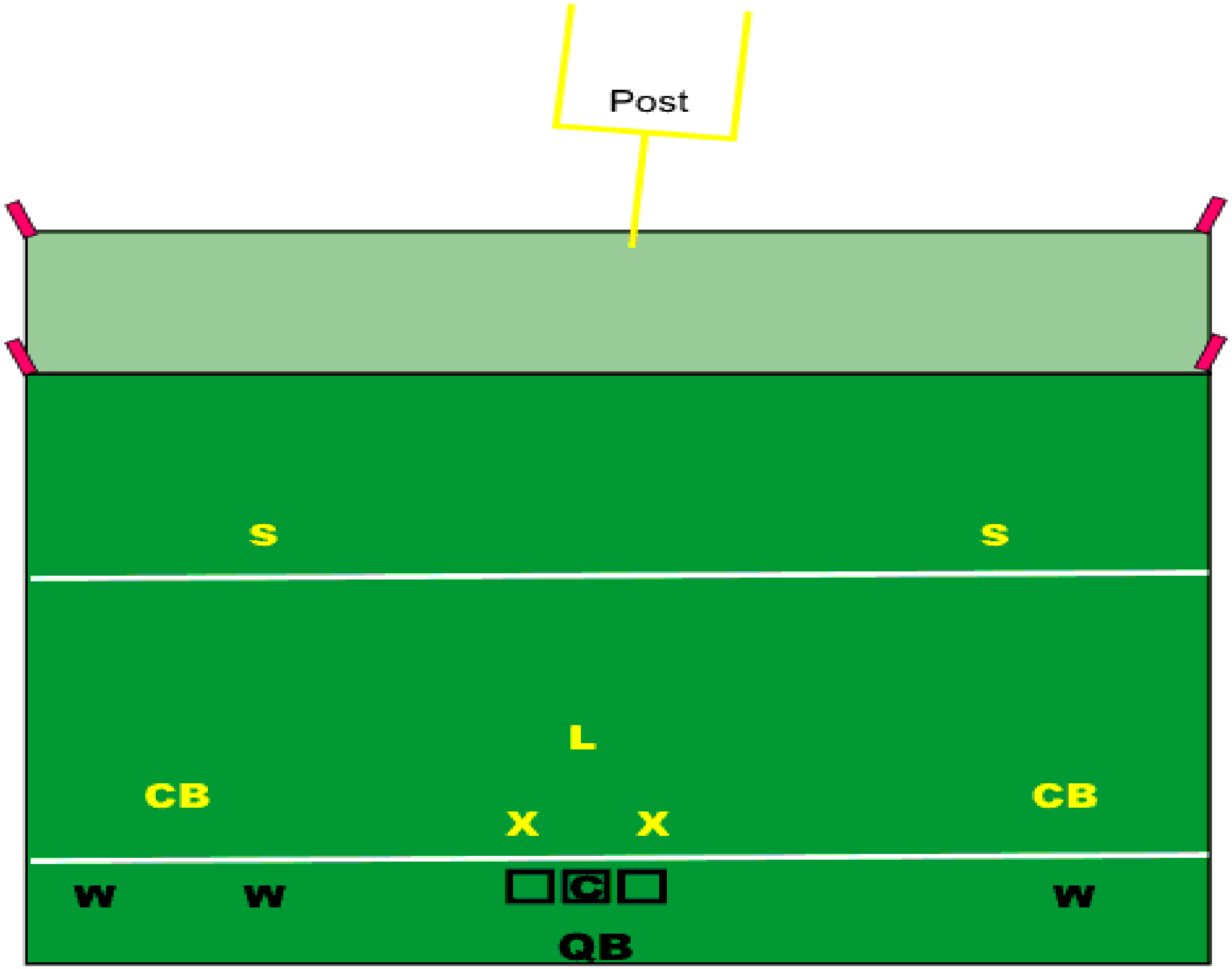
+ Trench Block

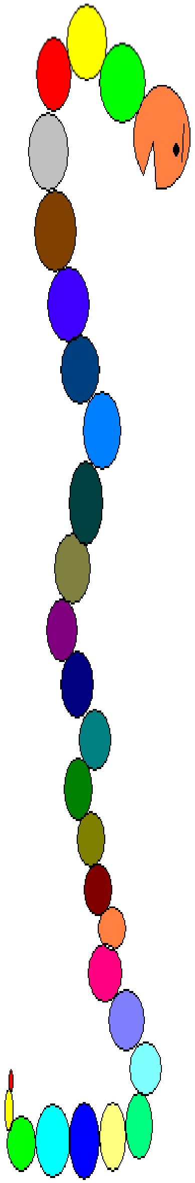
Not just Military

TEAM

ANTI-VIRUS







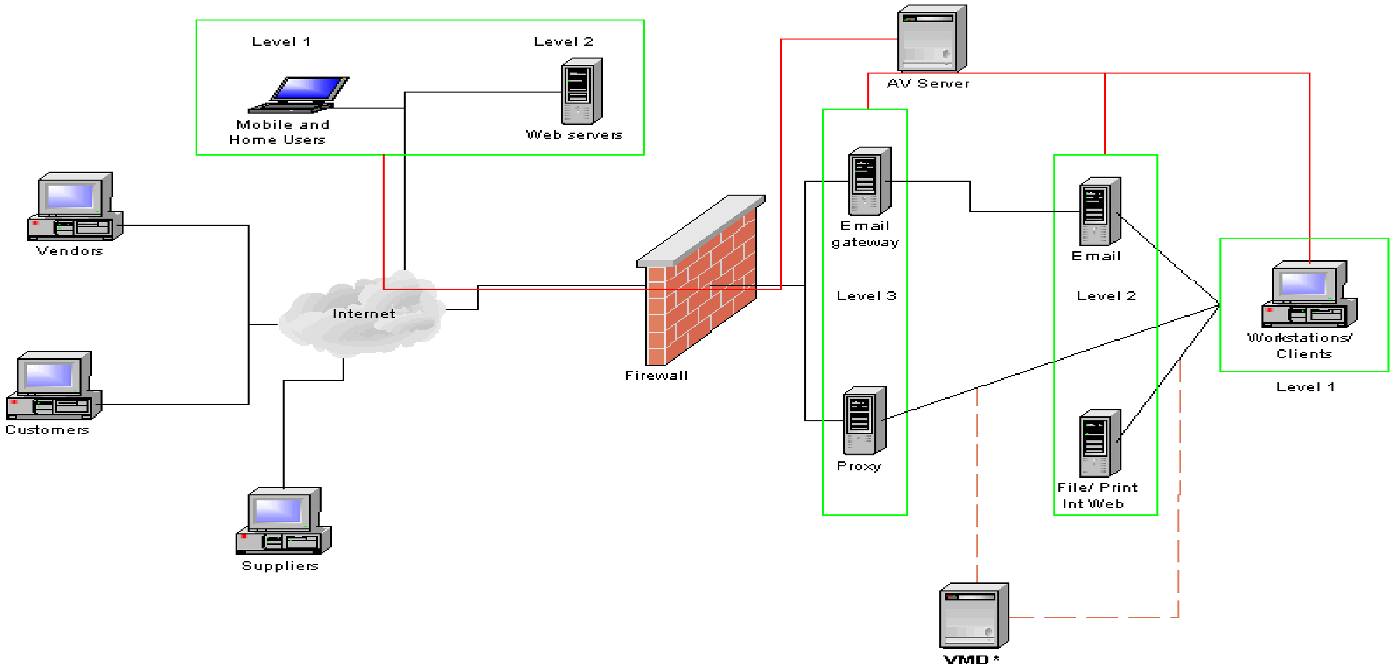
Our Initial premise

TEAM

ANTI-VIRUS

Fig. 1

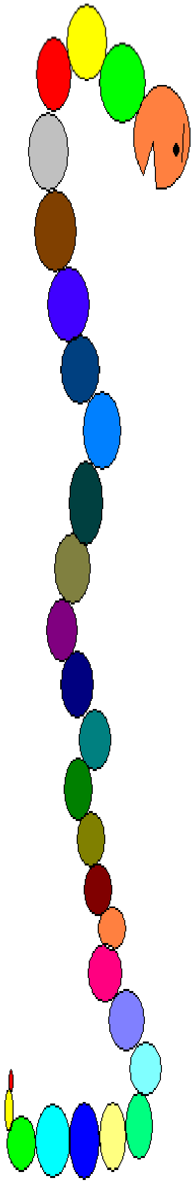
Malware protection infrastructure



Level 1 = Protect Workstations, Remote Users, and home users with Standard Anti-Virus product
Level 2 = Protect File and print, Application and web servers with Standard Anti-Virus Product
Level 2.5 = Protect Mail Servers with Standard Anti=Virus Product, Preferred use of alternate from Servers and Workstations
Level 3 = Protect Gateways (SMTP, FTP, Proxy, Firewalls and other outside connections with Anti-Virus. MUST be different from other products used.

Anti-Virus Management:
AV Management console, ties existing infrastructure together, providing centralized reporting, and product management., depicted with red line.
*VMD = Virus Monitoring Devices, These include SMB Lure, honeypot mailboxes and SNORT with virus rules.

Last Updated 25 Nov 2002



Today’s threats

“a year or two ago, most malware was spread via e-mail attachments, which resulted in mass outbreaks like Bagle, Mydoom, and Warezov. Nowadays sending .EXE attachments in e-mail doesn’t work so well for the criminals because almost every company and organization is filtering out such risky attachments from their e-mail traffic.” The same press release goes on to say “New preferred way of spreading malware is by drive-by downloads … so instead of getting infected over SMTP, you get infected over HTTP.”

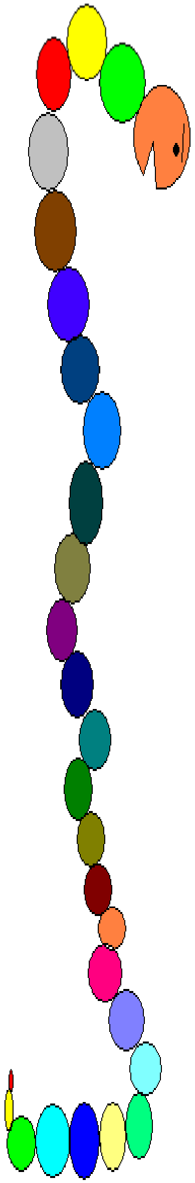
F-Secure Press Release: F-Secure predicts: a million viruses by the end of the year 31 March 2008

“Cybercriminals of today seem to have abandoned the attachments tactic that was so innovative in late 2007 and are now focused on exploiting free hosted applications”

MessageLabs Intelligence Summary dated May 2008

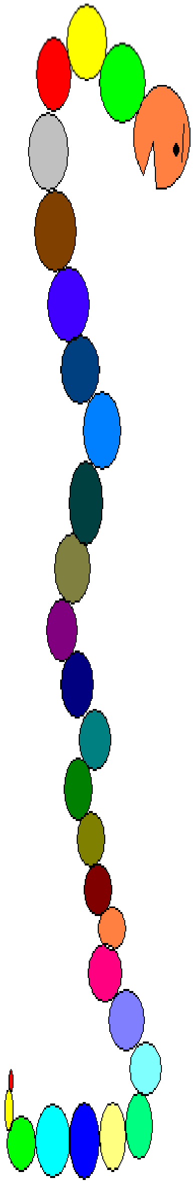
“Over the last year malware authors have moved away from direct attacks – attacks in which they directly interact with victims, via social engineering for example – to indirect attacks accomplished through compromised websites”.

Mary Landesman



Conclusions of Risk

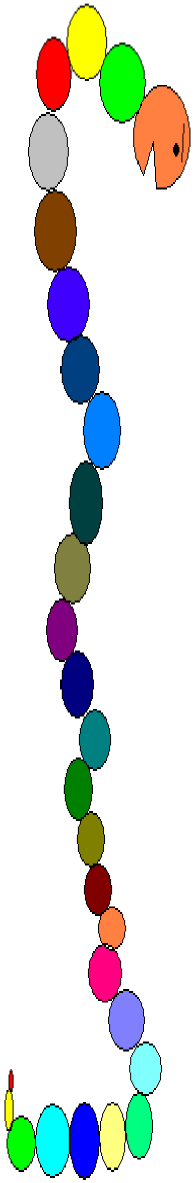
- Malware distribution has migrated from primarily self-replicating SMTP and Network aware threats to delivery by some type of download component.
- While not specifically addressed above, malware authorship has changed from hobbyist at the time of the initial paper, to organized crime and state or corporate backed professional coders.
- A majority of malware is performing network communications, be it exfiltrating data from cookies to files and directories to databases; or even responding to commands from remote control ‘hubs’.



Examples of threats

- W32/Nuwar aka Storm Worm (port 80)
- Thumb Drives and autorun.
- Mobile devices acting as storage devices.
- Root Kits
- ‘0 Day’ exploits in applications

Conclusions



- Are our original assumptions correct?
  - Yes
- What modifications need be made?
  - Secondary controls (HIPS, IDS, etc) more critical.
  - Closer cooperation with CIRTs, IDS, vuln/ patching teams
  - Closer concentration on Group policy rules.
  - Cover all choke points.

TEAM

ANTI-VIRUS

Questions