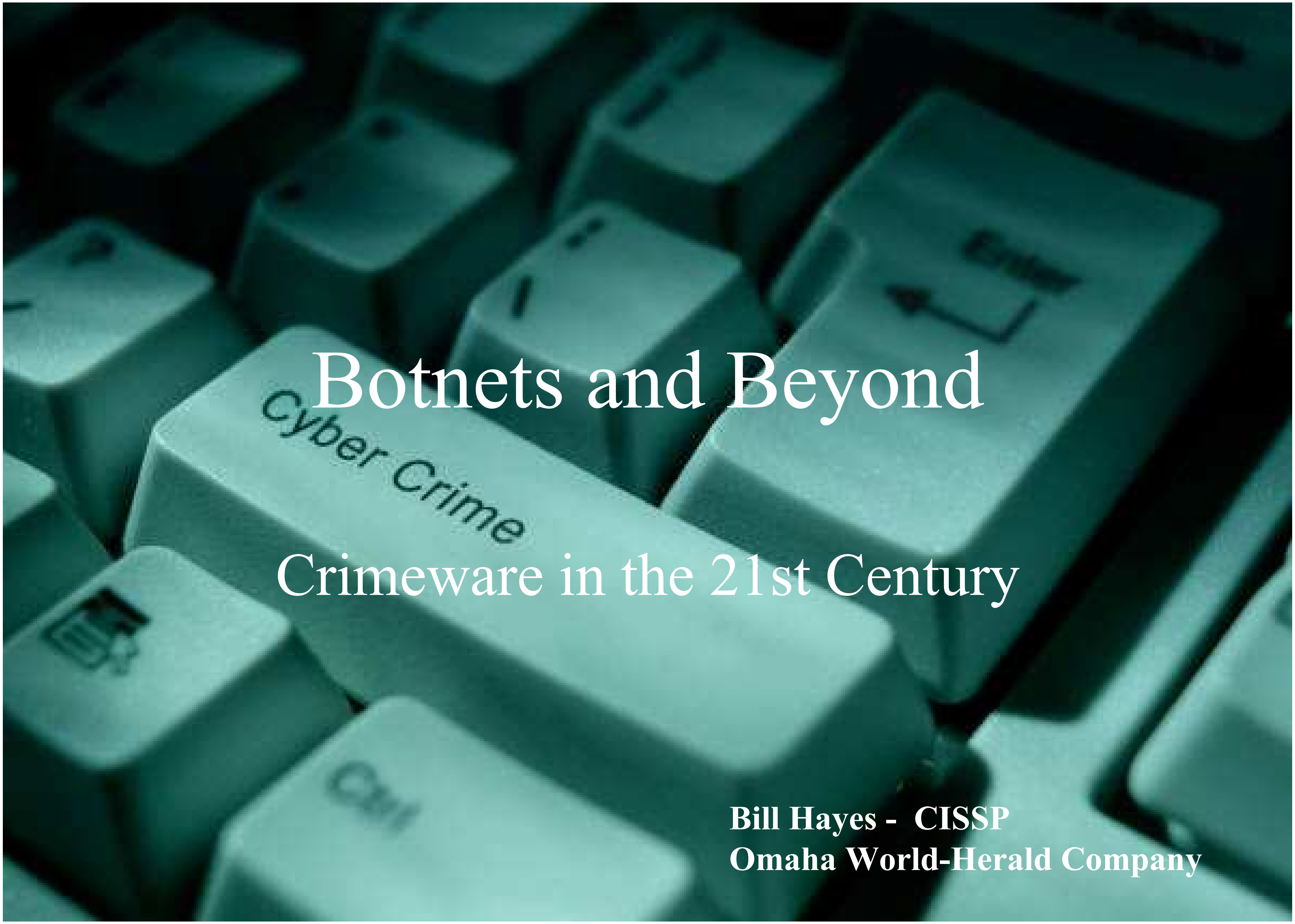
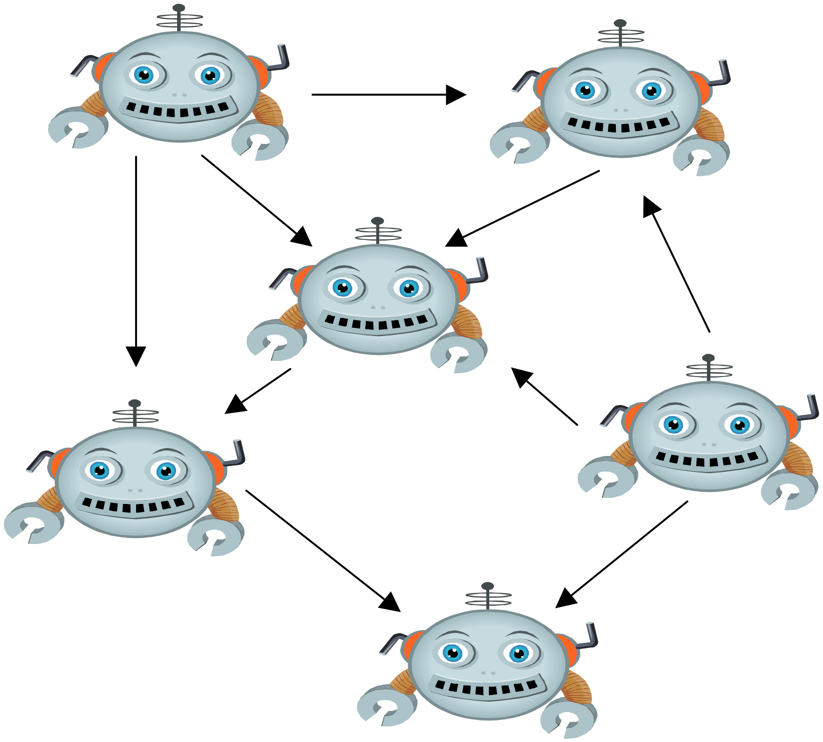


Botnets and Beyond

Crimeware in the 21st Century

Bill Hayes - CISSP
Omaha World-Herald Company

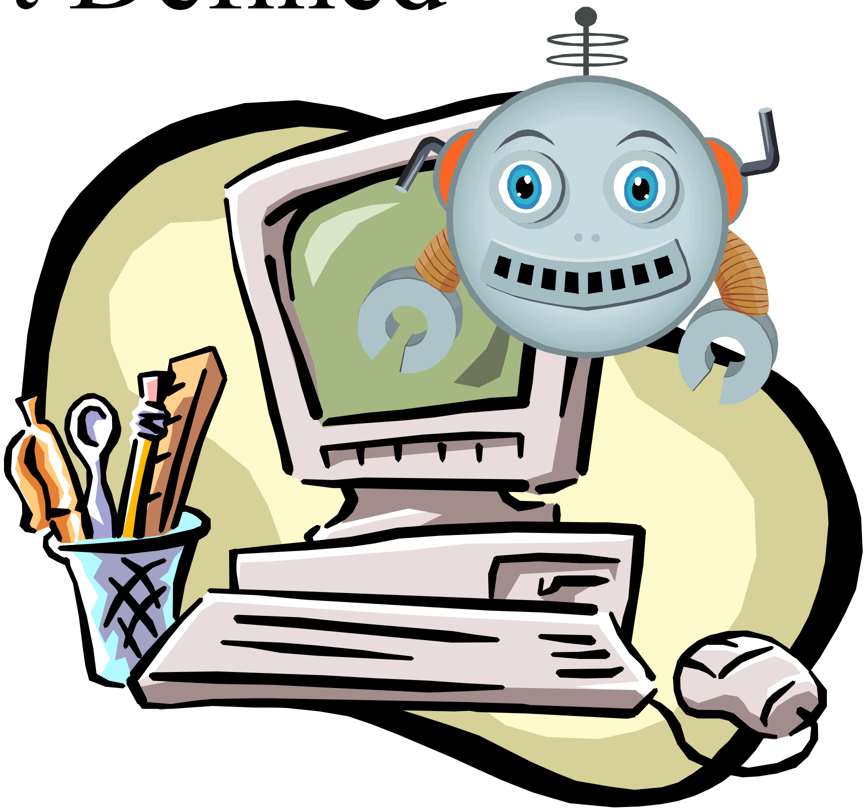
The Botnet Defined



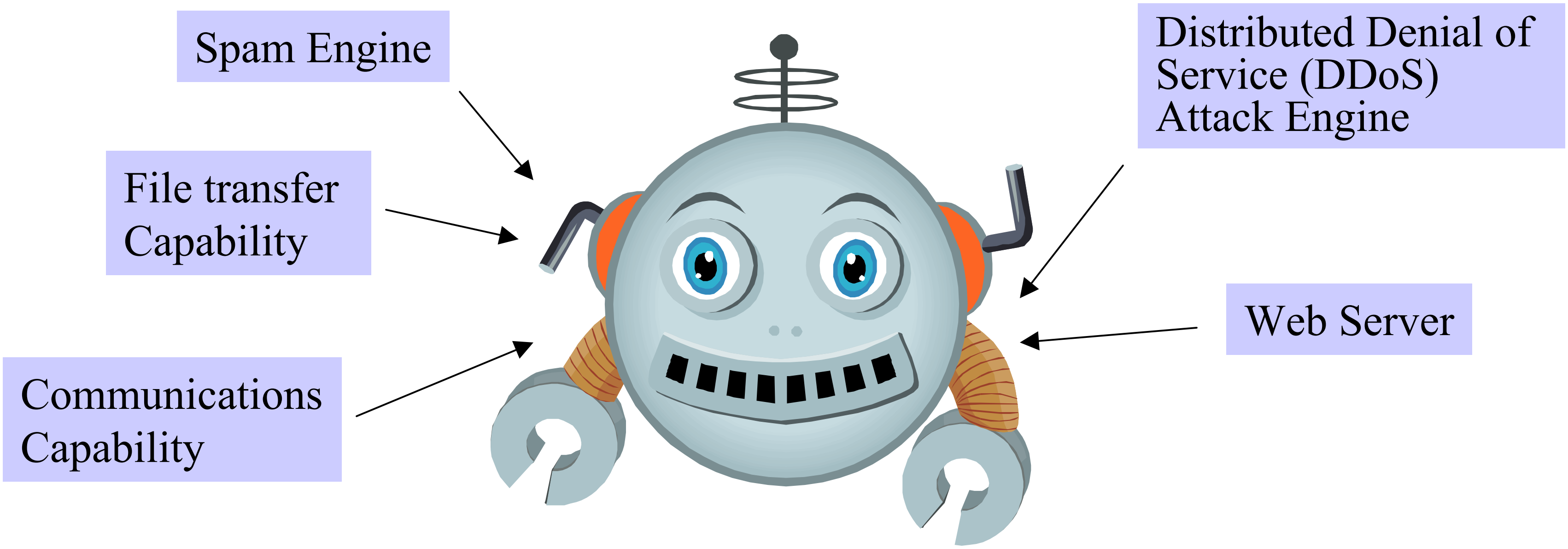
- A group of compromised computers working together for illegal purposes under the control of a human being, usually called a “Bot-herder or “Bot-master”.
- The workhorse of cyber crime.

The Bot Defined

- A compromised computer that conducts illicit actions under the control of a remote operator, usually without the knowledge of the owner.



Bot Functions



Spam Engine

File transfer Capability

Communications Capability

Distributed Denial of Service (DDoS) Attack Engine

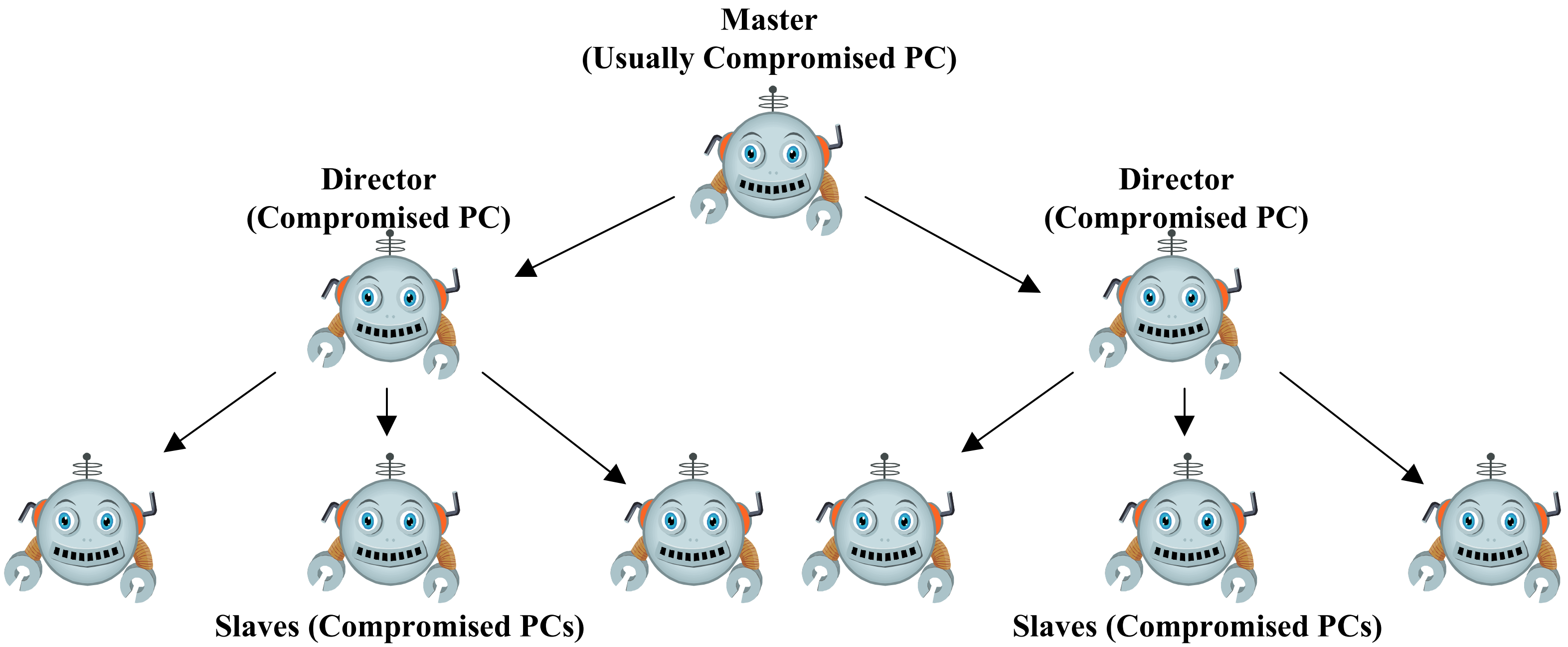
Web Server

Bots are really a combination of separate components gleaned from malware and legitimate software. Common components include Web servers, DDoS engines, file transfer tools, communications tools, and spam engines.

Common Botnet activities

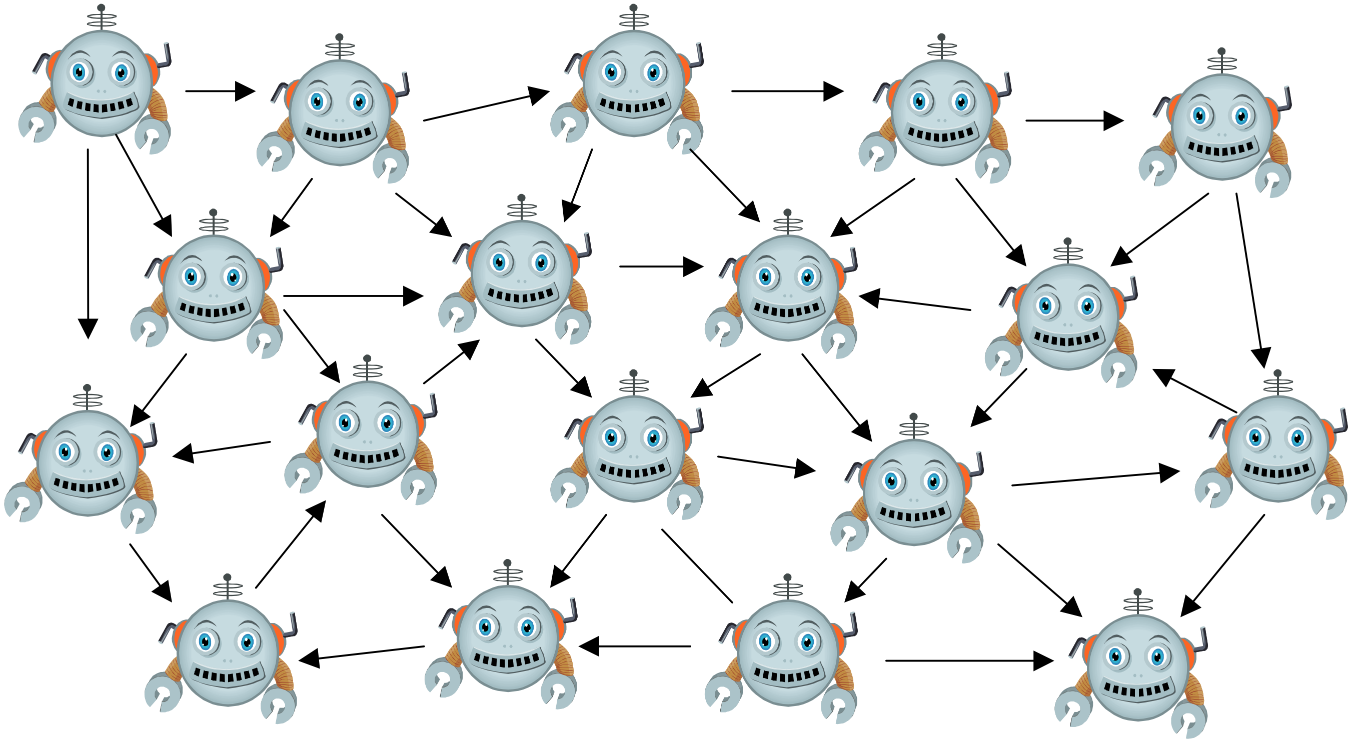
- Dump & Pump Scams - inflating stock prices to sell out before market catches on.
- Click Fraud - creating engines that constantly click online ads to get commissions.
- Phishing - Spam intended for identity theft
- Spam
- DDoS for Hire

Botnet Organization



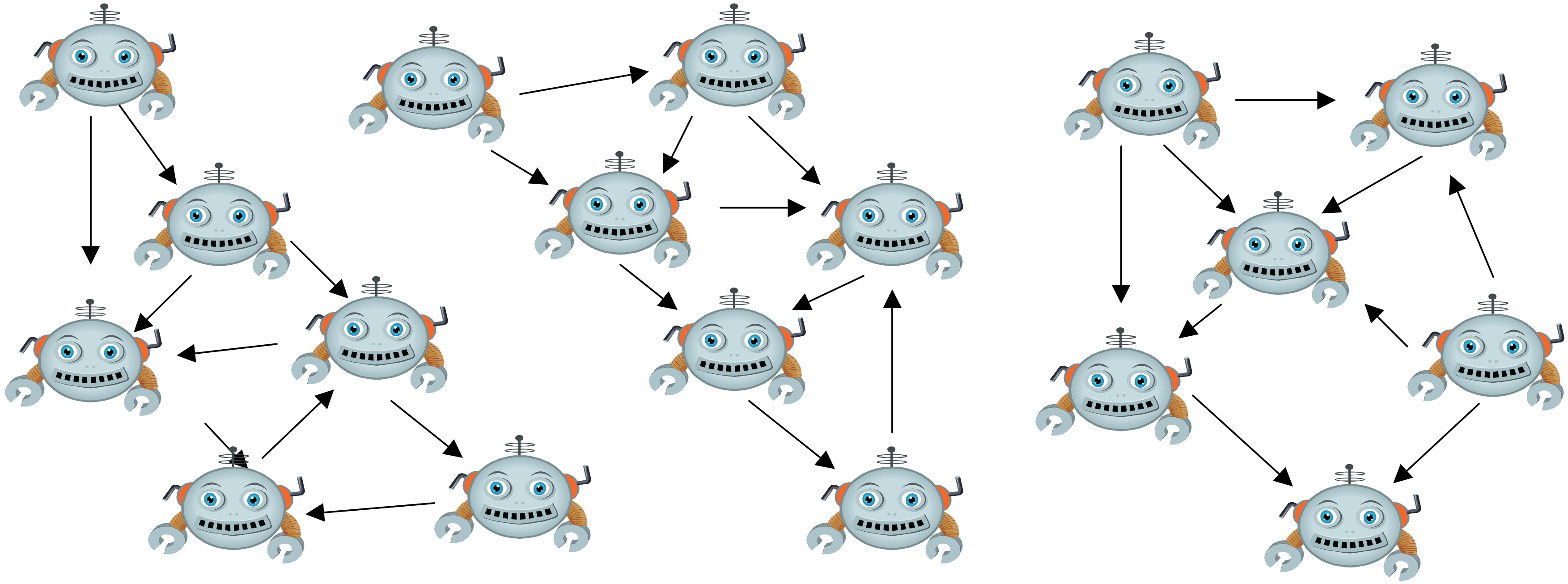
Classic Botnet organization derived from Distributed Denial of Service (DDoS) subnets of the late 1990s such as Stacheldracht Trinoo and TFN/TFN2K. At the same time, script kiddie IRC wars developed eggdrop IRC clients used in DDOS attacks against IRC servers used by rival script kiddies.

Botnet Organization



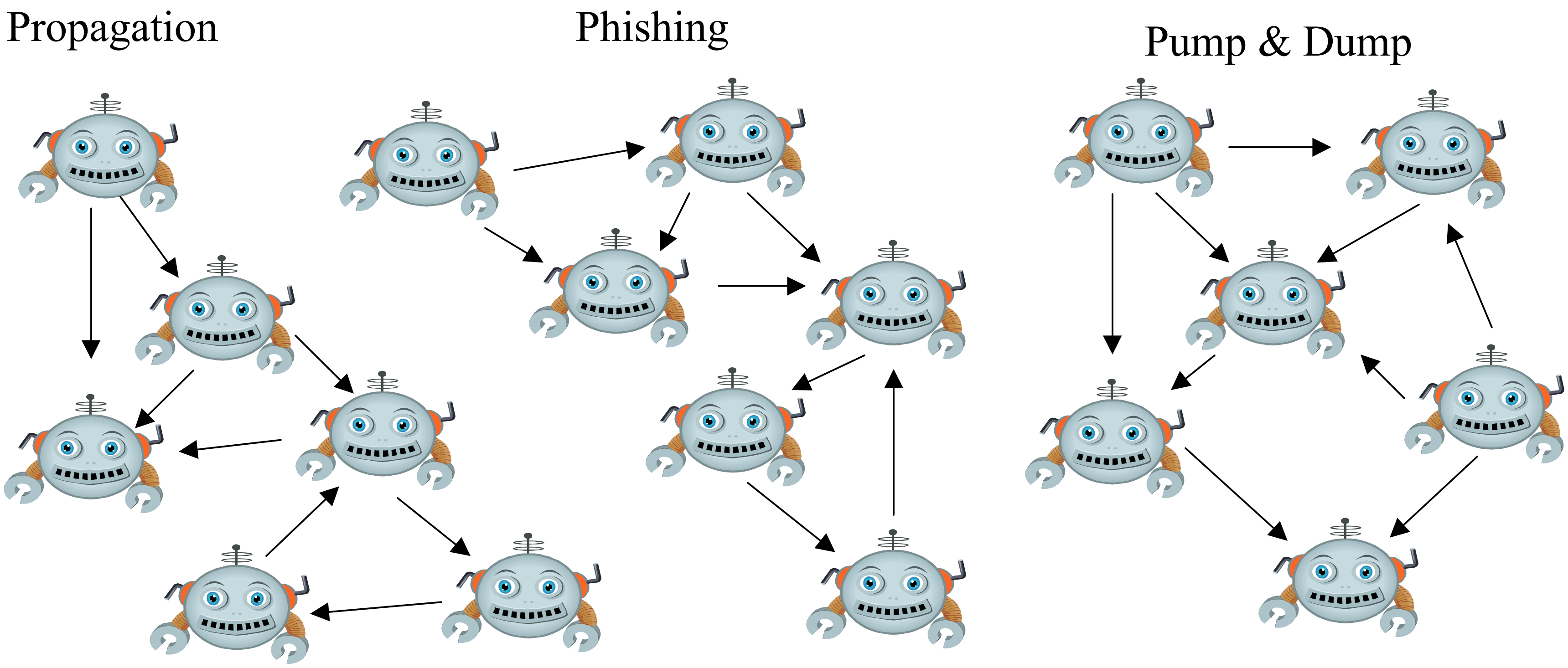
Peer-to-peer botnets are harder to wipe out as any bot can direct any bot. Bots can be configured for a specific attack and then reconfigured. P2P protocols like eDonkey in active use by Botnets.

Botnet Organization



Large botnets are supposed to be difficult to manage so it wasn't too much of a surprise when Storm worm, the largest botnet, reportedly began breaking up into smaller botnets communicating through individual encrypted channels.

Botnet Organization



Propagation

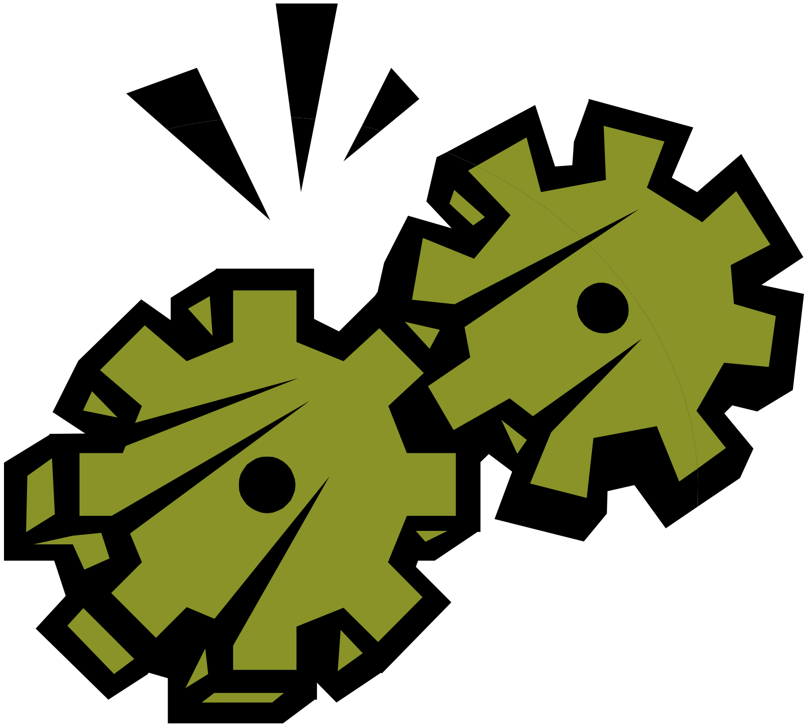
Phishing

Pump & Dump

With a botnet broken up into smaller units, the owners perform more tasks simultaneously. Propagation will always be an overhead task to replace machines cleaned through anti-malware tools such as anti-virus and Microsoft MSRT.

Botnet Installation attempts

Botnet installations can exploit Internet browser flaws in “driveby” installation attempts, often through compromised sites or hidden in banner ads. Users are usually unaware of the installation attempts.



Botnet Installation Attempts

DOWNLOAD THE
Dancing
Skeleton
CLICK HERE FOR A
SPOOKY GOOD TIME
RIP

Social engineering is the installation method of choice. Like the “Polish virus” (a.k.a “Redneck virus”) users willingly install the malware code for a perceived benefit.

Illustration source - http://www.sophos.com/security/blog/2007/10/720.html

Botnet Countermeasures

- Defense in Depth
- Use Anti-virus and anti-spyware
- Log analysis
- Eliminate unnecessary services
- Patching
- Filter SMTP addresses see http://luno.org/project/lred
- Egress policy

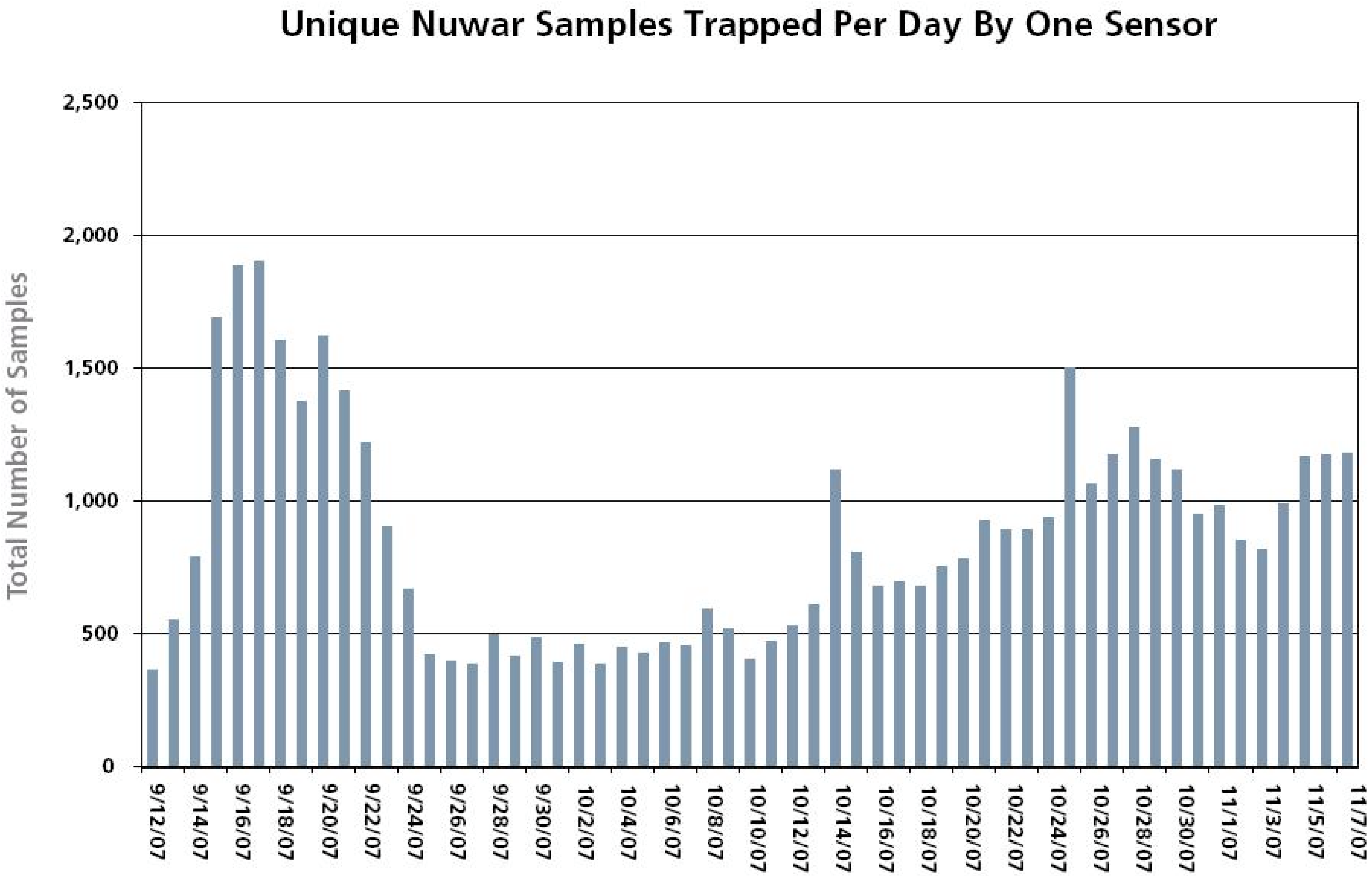
Defense in Depth

- Filter incoming traffic for botnet messages
- Monitor outbound traffic for unexpected destinations and protocols
- Use AV/Anti-spyware/content filtering

Anti-virus and Anti-spyware

- Botnets use downloaders derived from known Trojan horse downloaders.
- Good AV and Anti-Spyware tools will detect components and remove them.

Anti-virus and Anti-spyware continued



Botnets survive by continuing to mutate their code. Choose anti-malware tools able to keep up with these constant changes. Illustration source - ***McAfee Avert Labs Top 10 Predictions for 2008***

Log analysis

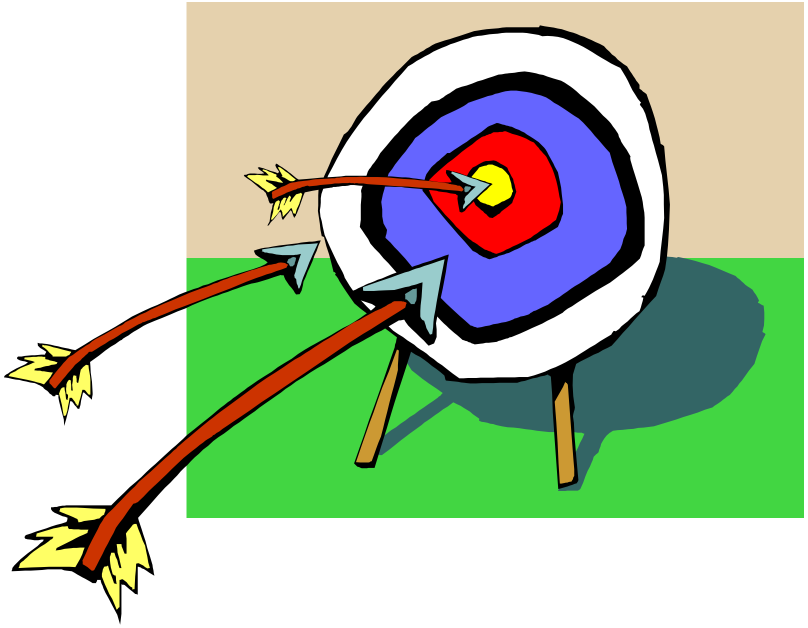
- Use log analysis technology to determine success of existing defenses and detect new attacks

Eliminate Unnecessary Services

- Old/obsolete and unnecessary services are frequently exploited.
- Have a secure, bare-bones configuration with change control measures to prevent software creep

Patching

- Don’t depend on Windows Updates, WSUS, to patch everything.
- Office updates frequently missed.
- Third-party software frequently missed.

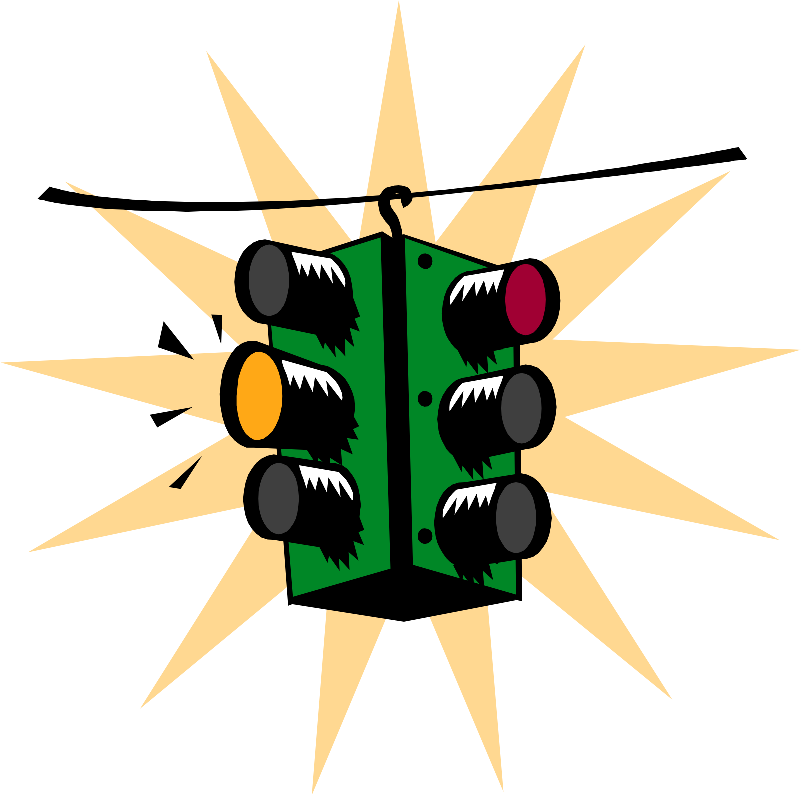


Filter incoming SMTP traffic

- LRED is a regularly-updated list of Perl-Compatible Regular Expressions that match domain name patterns assigned to dynamic addresses.
- Covers cable, dialup or DSL dynamic hosts.
- http://luno.org/project/lred

Egress Policy

- Establish egress policy to monitor/control outbound traffic
- Limit to business needed protocols and destinations.
- Can be challenging in academic/news organizations.



References

Common DDoS tools

Tribe Flood Network - http://staff.washington.edu/dittrich/talks/cert/tfn.html

Stacheldracht - http://staff.washington.edu/dittrich/talks/nanog/stacheldraht.html

Trinoo - http://service1.symantec.com/sarc/sarc.nsf/html/W32.DoS.Trinoo.html

Botnets

http://www.processor.com/editorial/article.asp?article=articles%2Fp2940%2F31p40%2F31p40.asp

Shadowserver - http://www.shadowserver.org/wiki/pmwiki.php?n=Shadowserver.Mission

Fast-Flux service networks - http://www.honeynet.org/papers/ff/fast-flux.html

ISOTF - http://www.isotf.org/?page_value=10

Botnet Activities

DDoS - http://en.wikipedia.org/wiki/DDoS#Distributed_attack

Pump & Dump - http://en.wikipedia.org/wiki/Pump_and_dump

Click Fraud - http://en.wikipedia.org/wiki/Click_fraud

Phishing - http://en.wikipedia.org/wiki/Phishing

Storm worm Botnet

http://en.wikipedia.org/wiki/Storm_botnet

http://www.secureworks.com/research/threats/storm-worm

http://www.cyber-ta.org/pubs/StormWorm/

http://www.sophos/com/security/blog/2007/10/720.html

References continued

Botnet Countermeasures

BotHunter - http://www.cyber-ta.org/BotHunter/

LRED - http://luno.org/project/lred

Law Enforcement

Operation Bot Roast

http://www.fbi.gov/pressrel/pressrel07/botnet061307.htm

Security Consultant is bot-herder

http://www.eweek.com/article2/0,1759,2215469,00.asp

McAfee AVERTLabs predictions

http://www.mcafee.com/us/local_content/white_papers/threat_center/wp_avert_predictions_2008.pdf?bcsi_scan_F25DABAABD7AEBB4=0&bcsi_scan_filename=wp_avert_predictions_2008.pdf

References continued

US-CERT - Trojan Spreading via MSN Messenger
http://www.us-cert.org/current/index.html#msn_messenger_trojan

Microsoft IM Trojan infected 11,000 machines on first day
http://www.techworld.com/security/news/index.cfm?RSS&NewsID=10709
Detected on Sunday, Nov. 18th and by 12:30 pm EST Monday, the botnet had grown to an estimated11,000 machines.

http://www.castlecops.com/p1024499-Another_MSN_Messenger_Trojan_spreading_quickly.html