Worms and network malice

What are worms:

Self propagating malicious programs:

The key is self-propagating, lack of user interaction
(Most mail viruses don't self propagate)
As a result, worms outrace human-based defenses

Worms are propagation:

The payload is the attacker's intent, the worm just gets it outh there.

Other portions of malcode:

Rootkit: Stealthing technology
Payload: ATtacker's intent
C2 networks as payload
Other propagation techniques:
Viral
Mail virus/mail worm
Single step (trojans, downloaders)

Taxonomy of worms:

Scanning ->	Latency Limited	(code-red)
	\-> Bandwidth Limited	(Slammer)
Target lists ->	Hitlist	(witty)
	\-> Topological	(morris)
	\-> Metaserver	(misc googlestuff)
Passive		(part of Nimda)

Properties of note:
Note disruptive is NETWORK layer disruptive.

	Speed	Disruptive	Stealth
LL	(hours)	(mild)	(none)
BW-L	(minutes)	(extreme)	(none)
Hlist	(seconds)	(nil)	(moderate)
Topo	(seconds-hrs)	(nil)	(none to extreme)
Meta	(seconds)	(nil-moderate)	(moderate?)
Passive	(seconds-days)	(nil)	(high to extreme)

The worst-case disruptive has been bandwidth-limited scanning worms (Slammer, Witty):

OUTBOUND link saturation
Tickling multicast/other bugs:
Multicast addresses caused work for switches/routers
Causing crashes:
Guarenteed way to crash most switches/routers:
Peg the CPU at 100
Easy to test for
OK to mitigate:
Solve bandwidth fairness problems

Other far less.

Test vs latency & bw limited scannign worms and don't worry about it!

More interesting question: malicious network disruption:

Malicious effects in general -> Harder

What is attacker's objectives, resources, and skills?

Network disruption is only mildly interesting: Can already DDoS any particular target out of existance. And tends to be transient.

The value is on the end hosts...

Techniques:

Disruption vs Damage: Transitory vs longer lasting.

But why bother?

DDoS (self evident). Worms very useful for gaining zombies

Corrup all routers of a given class. Worms very useful: They are a class break: "All of Type X", if Type X is Cisco IOS, teh results are nasty.

Avi Freedman Routing Attack: Root on one router: BGP -> OSPF, all routers in domain now have 0(^2) updates, cpu pegs, crash, bye-bye.

Terrorist Backhoe Brigade:

But more interesting network: WHere to place defenses?

End host: Brittle containment

Big Bad Firewall: Bad position (easily bypassed)

Internet: Tragedy of the commons

Lan! high speed AND cheap!

This is an interesting problem in dependanble networks.