The Future of Malware

Workshop on advanced and intelligent malicious software

Tom Vogt
<tom@lemuria.org>

Preface

What this is not

No actual malware will be demonstrated

No new exploits will be announced

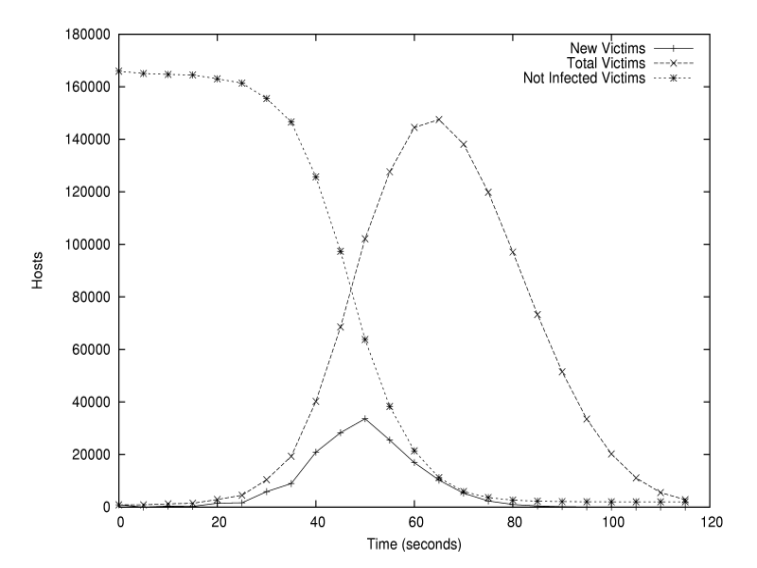
What this is

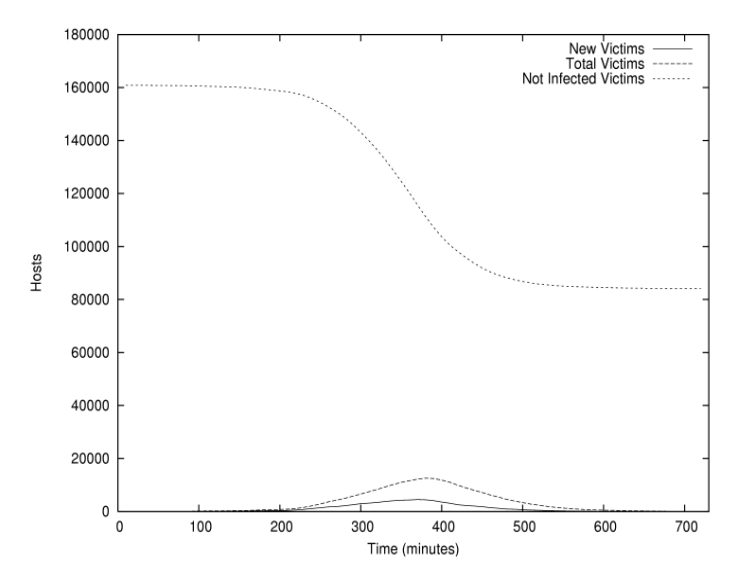
A collaboration, a workshop, a gathering of minds

Kickstarted with some collected thoughts

A glimpse of a possible future

Last Year





Advanced worm propagation algorithms

proof that very fast worms are possible

concepts for countermeasures

Since Then

Strikeback

Generic strikeback program unfeasable

Useful for known threats only

Real World

Witty employed many of the concepts I had suggested in my work

Few other major worms have appeared

The focus has shifted…

New Malware

…is written for financial gain

Zombie networks, to sell to spammers/phishers

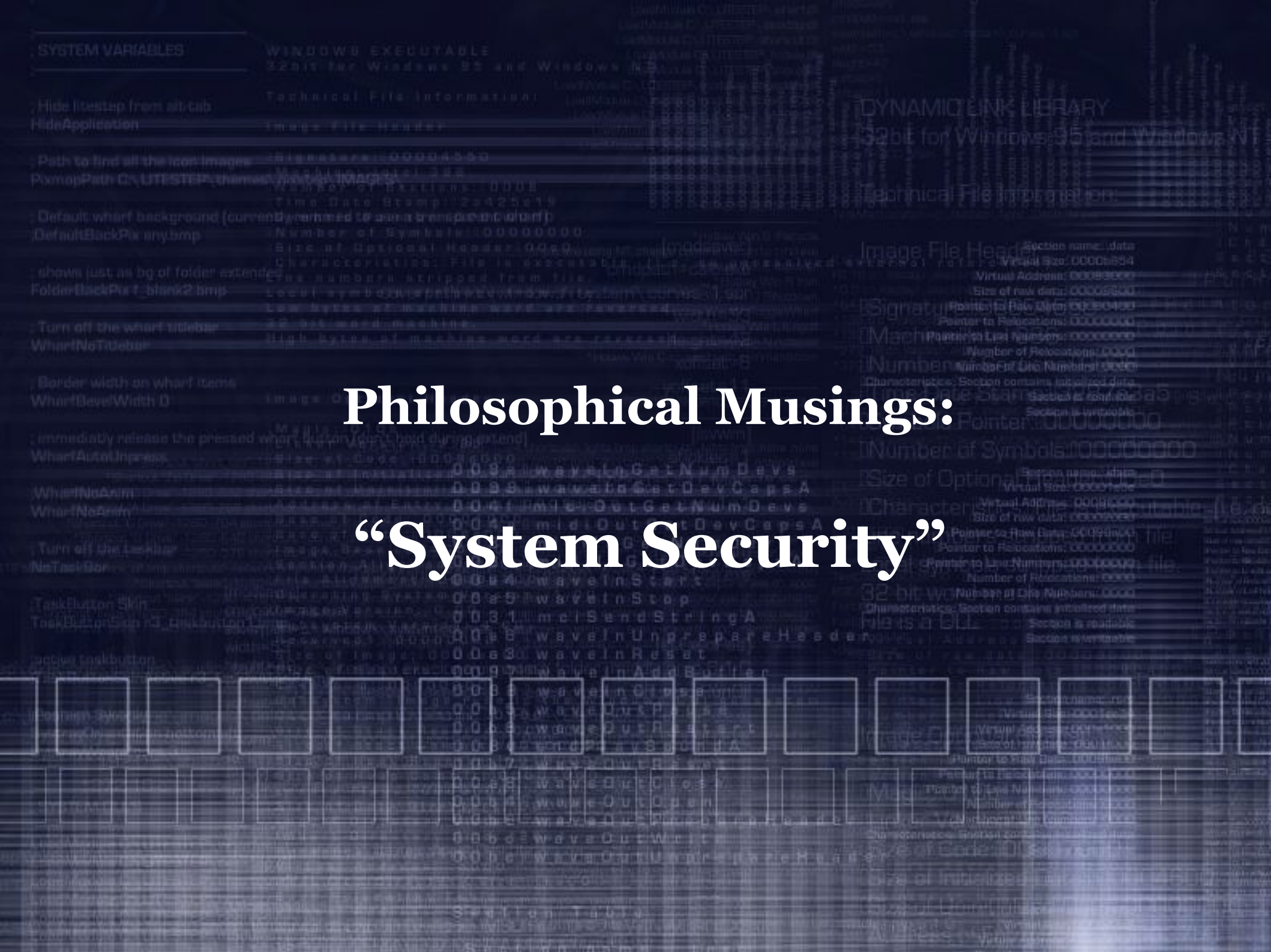
“Hostage taking” worms make first appearance

Cases of malware “fighting over” victims (Netsky)

…are still using the same old tricks

E-Mail attachments are still #1 malware source

No significant technological advances


Philosophical Musings:
“System Security”

Philosophy

Holistic Approach

Security of the whole, instead of the parts

Useful for high-level concepts

The philosophy behind stuff like RBAC, MLS, etc.

Why?

It's useful to evaluate some trends

Nobody in the security industry does it (even though many preach it)

Musings

System security does not automatically increase if OS or application security improve.

Only if security improves faster than malware

Think health care: If the virus evolves faster than the pharma industry can develop vaccinations, the illness it causes stays, no matter how rapid the medical progress.

Failings

Numbers suggest that system security is **not** improving, and hasn't for years.

For all it's work and money, the security industry barely manages to hold the status quo.

One thing in common with malware:
No significant technological advances.

Successes

Malware will continue to target the weakest link, which will often be the human user.

Anti-Malware products have partial success in containing known threats.

Both sides have thus far avoided entering a technology arms race, and are instead fighting the easier war of attrition.

Security products sell a lot.

Malware apparently sells quite good, too.


Future
Malware
let slip the dogs of war
(slide 11, I'm sure slow in coming to the topic)

Terror Cell Networks

Essentially, a decentralized zombie network

Every node knows a small number (~10) others.

Commands are inserted anywhere, encrypted with public-key encryption.

If the command verifies, it is executed and propagated.

Thanks to combinatorial explosion, commands will propagate through even huge networks (millions of zombies) in 7-10 steps.

Terror Cell Networks

Essentially, a decentralized zombie network

Every node knows a small number (~10) others.

Commands are inserted anywhere, encrypted with public-key encryption.

If the command verifies, it is executed and propagated.

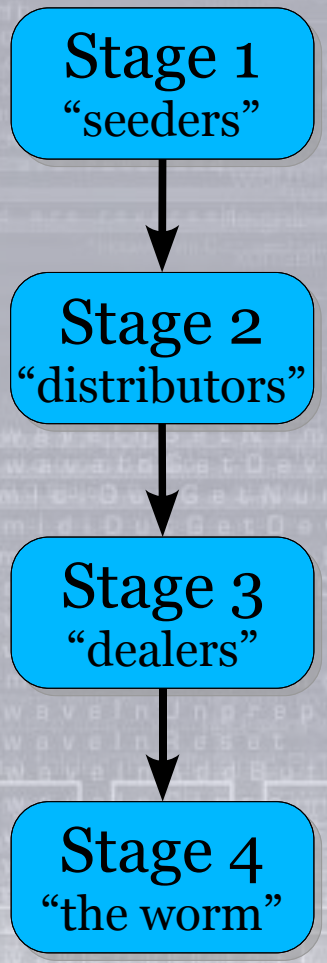
Thanks to combinatorial explosion, commands will propagate through even huge networks (millions of zombies) in 7-10 steps.

Multistage Worms

"This is not the worm your are looking for."

Purpose: Rapid re-infection after AV cleanup

Potentially very hard to clean out



Manually infected
sends stage 2 to pre-scanned, known-vulnerable hosts

low activity level
keeps list of victims
no scanning activity after initial round of infections

Distribute final stage
dormant until triggered
easily replaced

The actual worm
Contains the payload
if wiped out, stage 3 will send out a new strain

Symbiotic Trojans

People give up their passwords for a chocolate.

People install spyware, knowing that it is spyware.

People install trojans and other crap downloaded from some random Internet site.

People execute programs they were sent by mail.

In Summary:

It takes very little to bypass all technology and get the actual user to install a trojan.

Symbiotic Trojans

We already knew that! So what?

Think it through – can we get people to **knowingly** install malware? (no longer a real trojan)

Conditions

Considerable use for the user.

Minor (for him!) malicious side effect.

Example: A browser toolbar that hits a webserver once a second. Now multiply by 10 million…

Symbiotic Trojans

Alternatives

Mask the malware function as a programmer bug. (e.g. the search option loops, oops how stupid of us)

Hidden agendas – what if the next seti@home actually is passwordcracking@home and the colourful statistics are all fake?

Disinformation – your cute browser toolbar rewrites the news you are reading…

Polymorph Worms

Learning from History

Why do virii not use 15 year old technology?