

How cybercrime, security software and security professionals will evolve



Joe Telafici, VP of McAfee Labs Operations



Some disclaimers



- Speaking largely of host-based products
- Not discussing any particular product
- Everything in here is a forward-looking prognosis of how the security landscape might look in the future
- I hope to prompt some thought and debate

Why this talk – some assertions



- Cybercrime is a societal problem
- The good guys and the bad guys are evolving together
- The bad guy always gets first move
- Things are going to get worse before they get better
- Predictions are annoying, but thinking ahead is a necessity

Flashback - 1995



- Handful of executable and boot sector viruses
- Macro viruses started
- Almost all threats are parasitic in nature
- Almost all threats of the “digital graffiti” variety: written for annoyance or bragging rights

Vendors:

- High effort expended on every new threat (weeks, months, in some cases)
- Even more effort expended when the pimply kids changed vectors (e.g. Office documents)
- Data destruction (and hence very angry customers) or rapid proliferation common
- Sigs released monthly
- Sig size < 1 floppy

Customers

- AV common but not ubiquitous
- Gateway antimalware was just starting
- Firewalls were common
- Vulnerabilities were unheard of
- Dedicated security or risk mgmt function?

Implications of this environment



- Most threats never made it into the wild
- Defense in depth was minimal
- Vendor response was around depth of analysis and elegance of solution
- Repair was of huge importance
- Customers largely concerned with host machine data loss, downtime
- Malware authors largely interested in expanding skills, fame
- New platforms and file types are fascinating to them

Partied like it's 1999



- Boot sectors largely gone
- File infectors still doing their thing (Funlove)
- By 2000, script viruses were getting common (remember Loveletter?)
- Mass-mailers are common
- Spyware and adware starting out
- Vulnerabilities now not uncommon, though seldom used

The vendor world of 2000

- Avoiding legal implications of spyware like the plague
- Higher volume – approaching 100 threats a week
- Wider variety of products under development, use
- Sigs released weekly
- Sig size ~1-2 Mb

Customer environment

- Gateway and server AV now common thanks to Loveletter, et al.
- Host AV largely ubiquitous
- Host management starting to be a concern
-

- Speed of mail-borne attacks has everyone worrying about how to slow spread/keep systems up
- Bad guys focusing as much on new vectors of distribution (e.g. mail, Usenet) as new file types and platforms
- Response to malware attack:
 - Wait for someone to notice bad file
 - Send it to their vendor
 - Develop signature
 - Deploy signature

The turning point



- September 2001 - W32/Nimda
- Why?
- One of the first blended threats
- Recognized the importance of web sites as an infection vector
- Showed the way for financially motivated attacks
- Used vulnerabilities & social engineering

Fast-forward to 2005



- Blended threats the norm
- Rubble of the virus wars (Bagle, Netsky, Mydoom)
- Spyware now a top concern and a big business
- Bots rising under the radar
- Some financial attacks (starting with Bugbear, late 2002, password-stealers), but immature (barring adware)

Vendor

- A huge number of products
- Lots of time spent talking to lawyers
- Scale has passed capabilities of purely human efforts
- Sig releases daily or hourly
- Sig sizes ~5Mb

Customer

- Defense in depth quite common
- Patching strategies in place
- Risk management as a concept

- Everything is computerized
- Economy is terrible
- Political world is complicating
- You ARE infected
- We're still using 20-year-old technology as our primary defense
- Bad guys are well-organized, well-educated and financially savvy
- Cybercrime is a multibillion dollar industry
- Releases in nearly real-time
- Static sigs >40Mb

Bad Guy Motivations



1995

2000

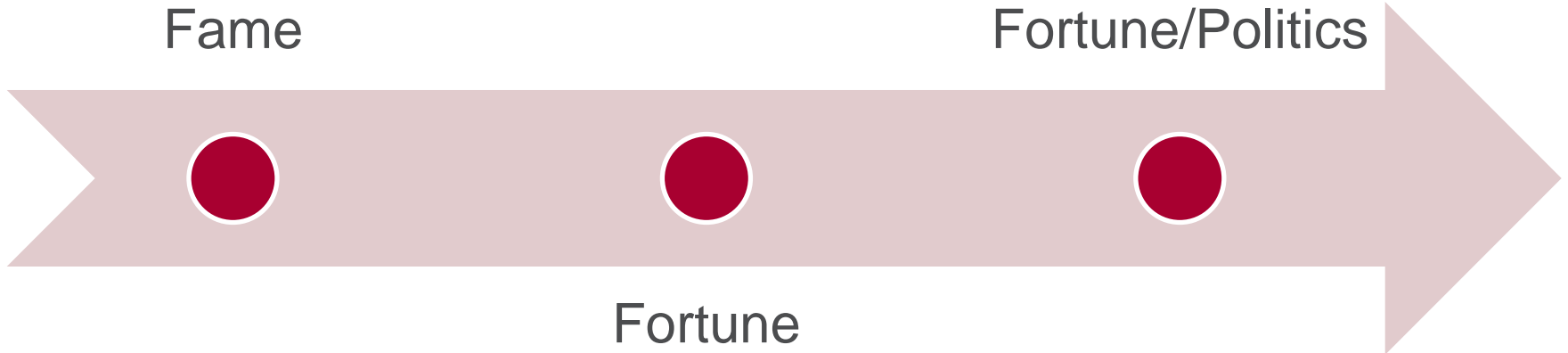
2005

2010

2015

Fame

Fortune/Politics



Bad Guy Techniques



1995

2000

2005

2010

2015

Cleverness/
Complexity

Combinations?



Vendor Techniques



1995

2000

2005

2010

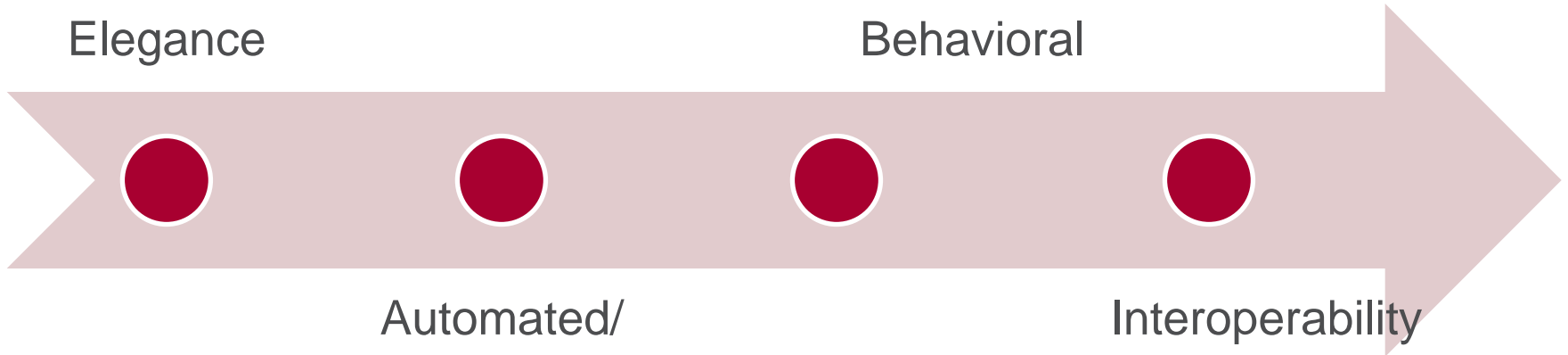
2015

Hand-Crafted/
Elegance

Cloud/
Behavioral

Automated/
Fast

Interoperability



Vendor Techniques



1995

2000

2005

2010

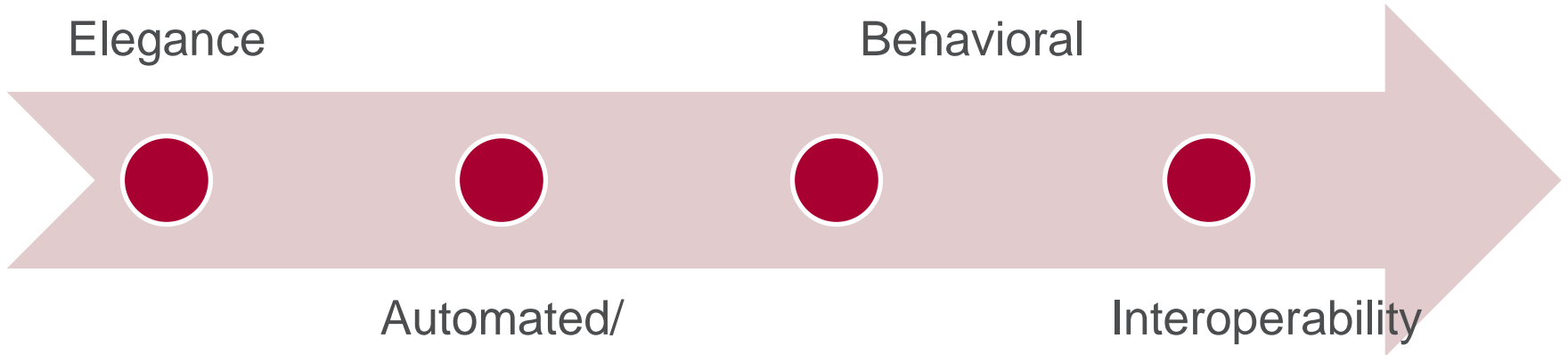
2015

Hand-Crafted/
Elegance

Cloud/
Behavioral

Automated/
Fast

Interoperability



Some vendor stats



Defender Approaches



1995

2000

2005

2010

2015

Single-
Layer

Risk Mgmt



Defense-in-
Depth/
Mgmt

?????

- Solutions are statistical and reputation-based
- Signatures have a lifespan
- Users decide which protections to enable
- Products “talk” to each other and adapt to attacks
- User-based protection is implemented
- Truly critical infrastructure moves off the public internet
- Privacy takes a back seat to security legislatively

Vendor perspective

- Testing and support are more complicated
- Product interoperability & standards compliance will become important
- Forensics & DLP integrated into malware protection

Customer perspective

- Consumerization, cloud, SaaS technologies reduce PCs in the workplace
- Security/Risk Mgmt/ Systems Mgmt/Networking lines blur
- Education has a resurgence
- Biometrics hits critical mass

What will life be like in 2015? 2020?

Questions?

Joe_Telafici@mcafee.com