


black hat[®]
ABU DHABI 2012

DECEMBER 3 - 6, 2012
EMIRATES PALACE | UNITED ARAB EMIRATES

In partnership with:

TRAC
TELECOMMUNICATIONS REGULATORY AUTHORITY

KHALIFA
UNIVERSITY

Supported by:

CERT ^{ae}
Computer
Emergency
Response
Team
مركز الاستجابة لحوادث الحاسوب

Cybercrime Kill Chain vs. Effectiveness of Defense Layers

Dr. Stefan Frei & Francisco Artés

@stefan_frei

@franklyfranc


NSS LABS
Trusted Advice. Measured.



blackhat[®]
ABU DHABI 2012



DECEMBER 10 - 13, 2012
EMIRATES PALACE | UNITED ARAB EMIRATES

In partnership with:



Supported by:



THE FLIGHT TO ABU DHABI TOOK LONGER THAN TESTING IPS.



Speaker – Dr. Stefan Frei

- Professional

- Research Director @ NSS Labs
- Research Analyst Director @ Secunia
- Senior Researcher & Pentester
@ ISS X-Force



- Contact

- Email: sfrei@nsslabs.com
- Twitter: [@stefan_frei](https://twitter.com/stefan_frei)

Speaker – Mr. Francisco Artés

- Professional
 - Research Director @ NSS Labs
 - CSO/CISO
 - Trace3
 - Deluxe Entertainment
 - Electronic Arts
- Contact
 - Email: frank@nsslabs.com
 - Twitter: [@franklyfranc](https://twitter.com/franklyfranc)





DECEMBER 10 - 13, 2012
EMIRATES PALACE | UNITED ARAB EMIRATES

In partnership with:



Supported by:



ABSTRACT

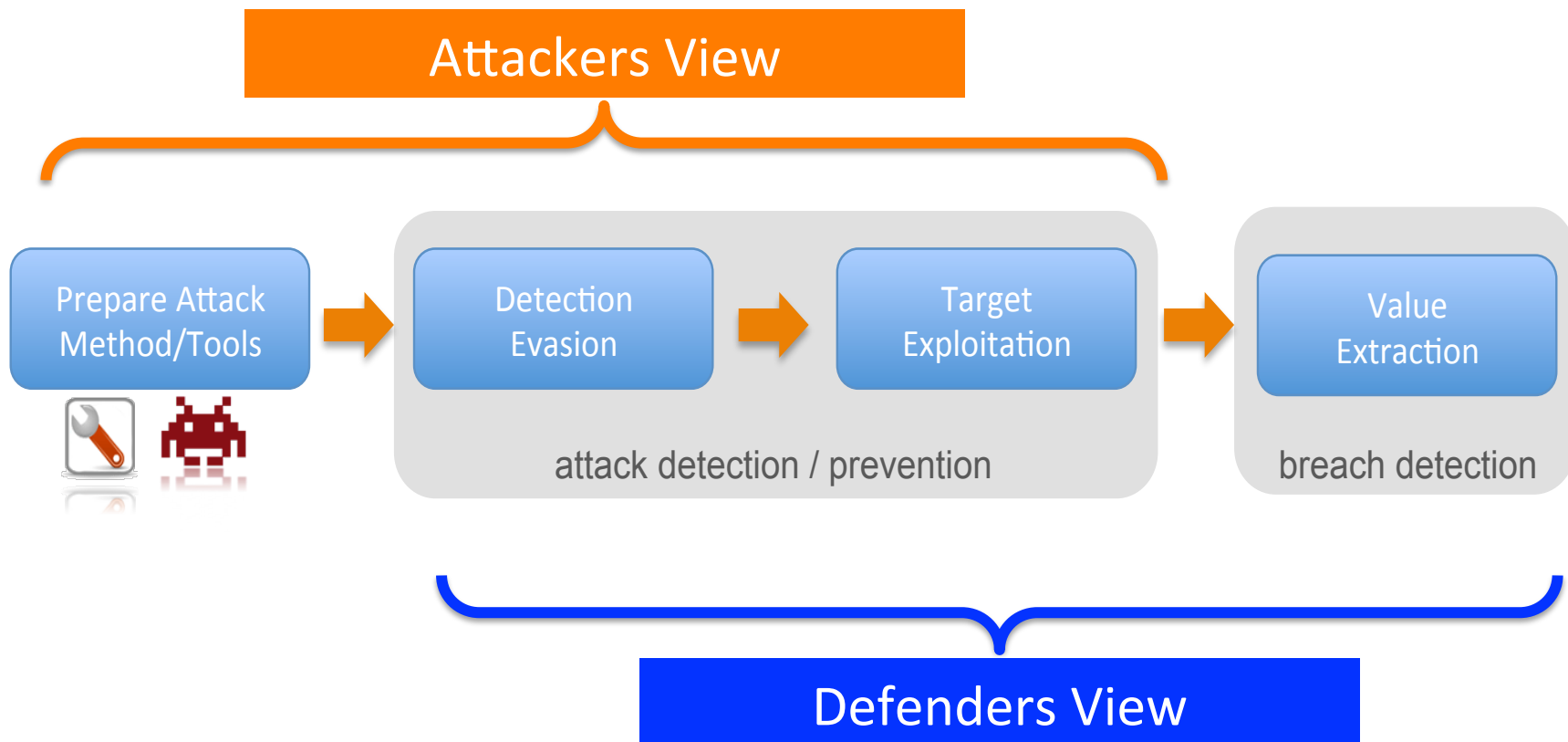
Cybercriminals persistently challenge the security of organizations through the rapid implementation of diverse attack methodologies, state of the art malware, and innovative evasion techniques. In response organizations deploy and rely on multiple layers of diverse security technologies. This talk examines the attackers' kill chain and the measured effectiveness of typical defense technologies such as Next Generation Firewalls, Intrusion Prevention Systems IPS, Antivirus/Malware Detection, and browsers internal protection. Empirical data on the effectiveness of security products derived from NSS Labs harsh real world testing is presented together with a live demonstration of successful evasion of malware detection. We find a considerable gap of protection levels within/and across different security product groups. Using Maltego complex correlations between undetected exploits, crimware kits, and affected software vendor and products are demonstrated.

Agenda

- How we get attacked
- Layered Defense
- Results from NSS Labs' testing
- Demonstration of Exploit vs. Layered Defense
- Conclusion

Attack Kill Chain

– Attacker vs. Defender



Attack Kill Chain

– Understanding the Attacker

Understand the threat and the
attackers motivation & methods



Attack Kill Chain

– Understanding Evasion

Understand how malware
bypasses detection



Assess the effectiveness
of layered defenses

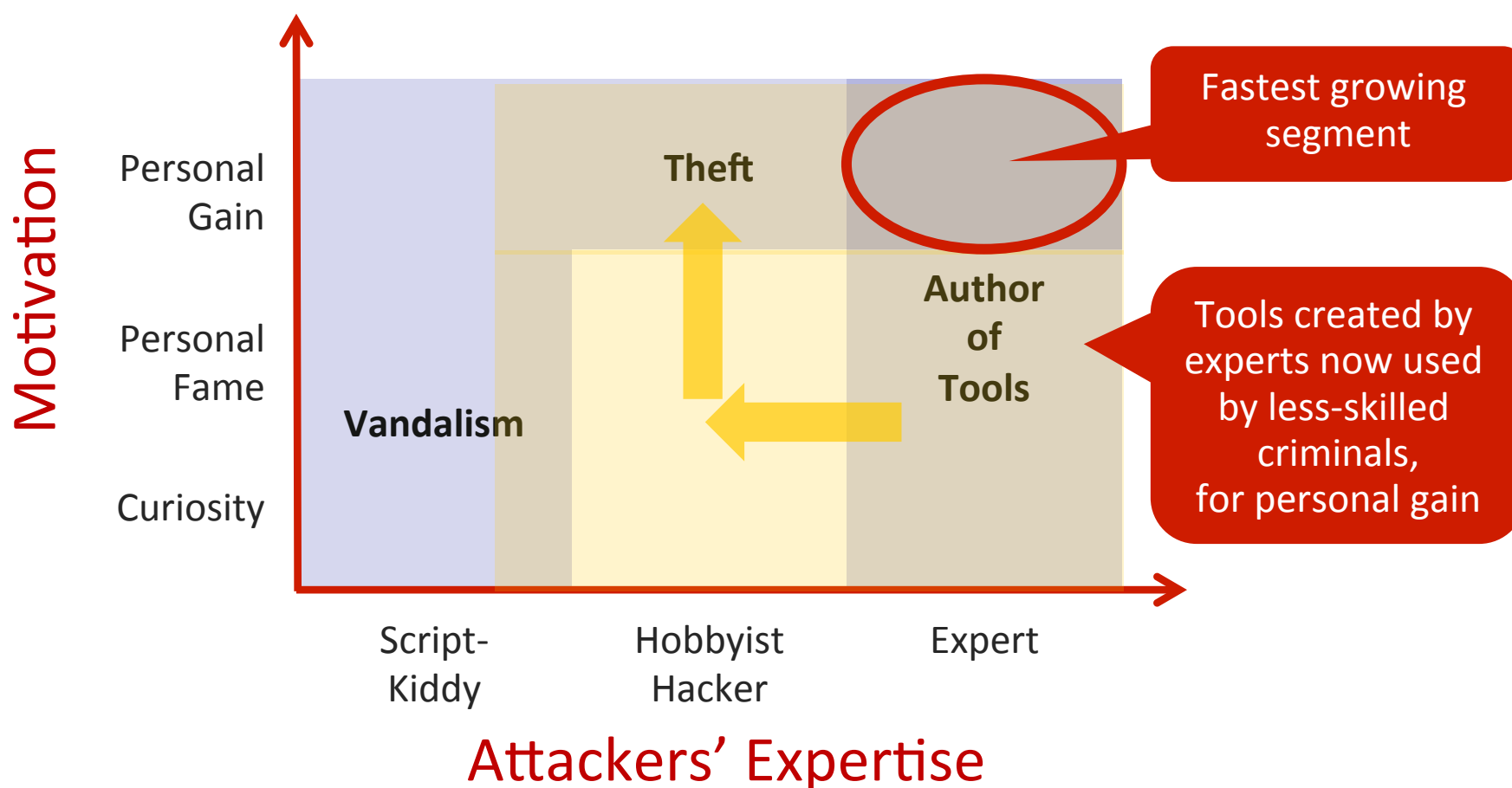
Attack Kill Chain

– If prevention failed



^
Detect &
neutralize

The Changing Threat Environment



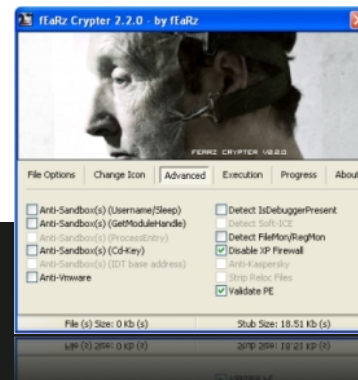
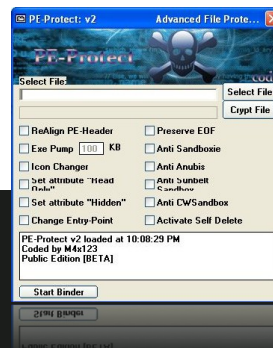
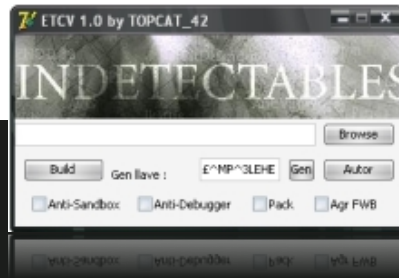
Malware Development & Tools

- Cybercriminals developed formidable tools

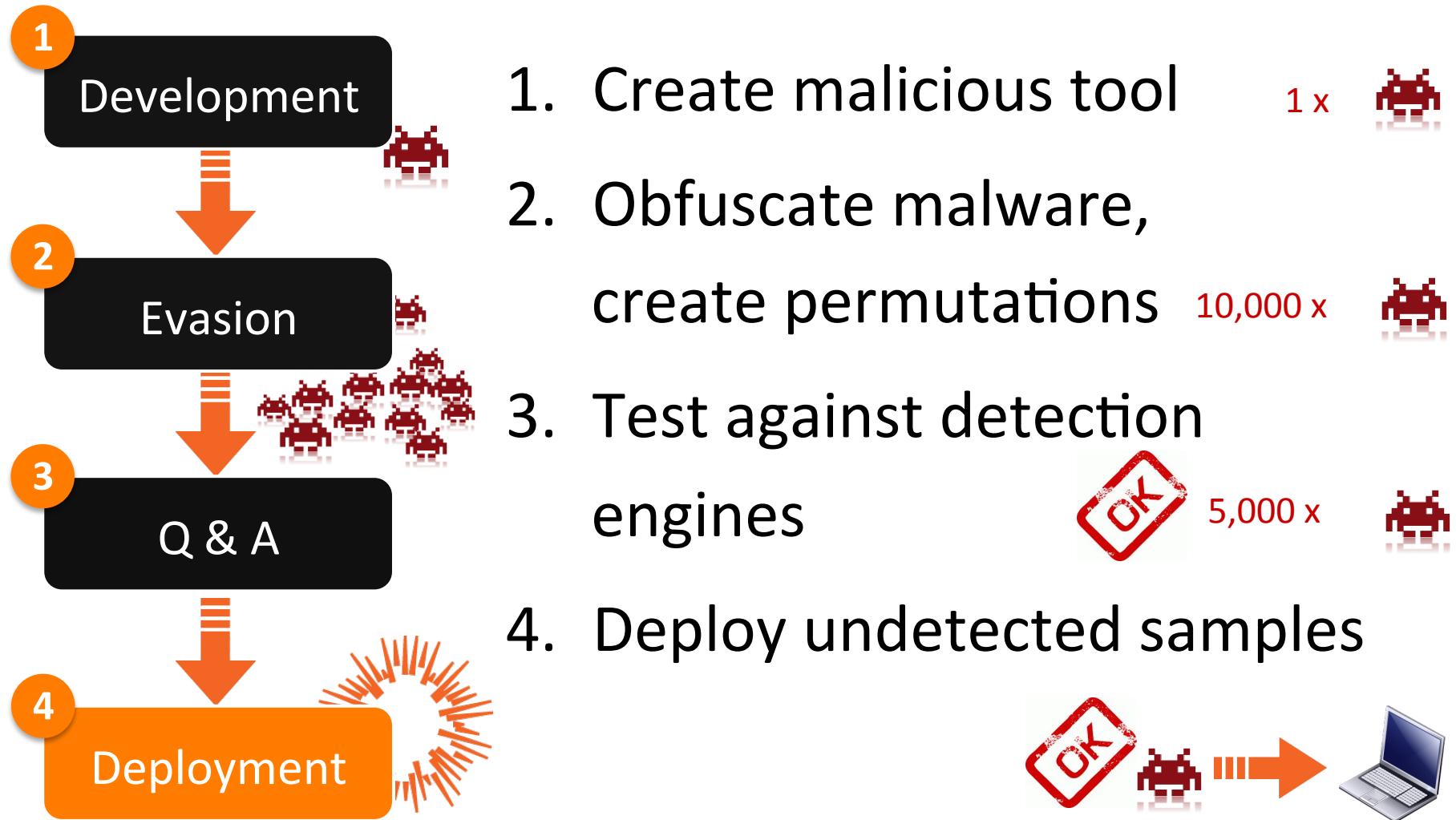
Easy to use development tools, Q&A, and service level agreements just as in every mature industry

- Detection Evasion and Resilience

By design, malware is developed and deployed with detection evasion in mind



Malware Development Process



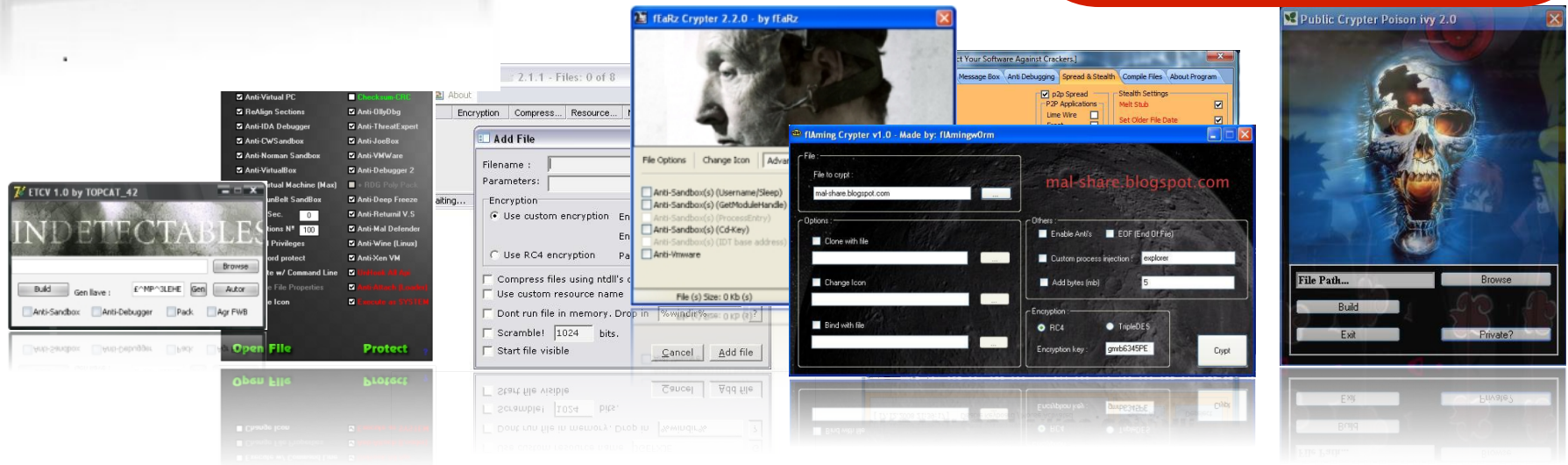
Underground Market



Gold Edition

- 6 months (unlimited) or 9 months(maximum 3 times) replacement warranty if it gets detected by any antivirus (you can choose 6 months or 9 months)
 - 7/24 online support via e-mail and instant messengers
 - Supports Windows 95/98/ME/NT/2000/2003/XP/Vista
 - Remote Shell (Managing with Ms-Dos Commands)
 - Webcam - audio streaming and msn sniffer
 - Controlling remote computer via keyboard and mouse
 - Notifies changements on clipboard and save them
 - Technical support after installing software
 - Viewing pictures without any download(Thumbnail View)
- Price : 249\$ (United State Dollar)

Malware offered for **\$249** with a Service Level Agreement and **replacement warranty** if the creation is **detected by any anti-virus** within 9 months



The Availability of Malware Tools



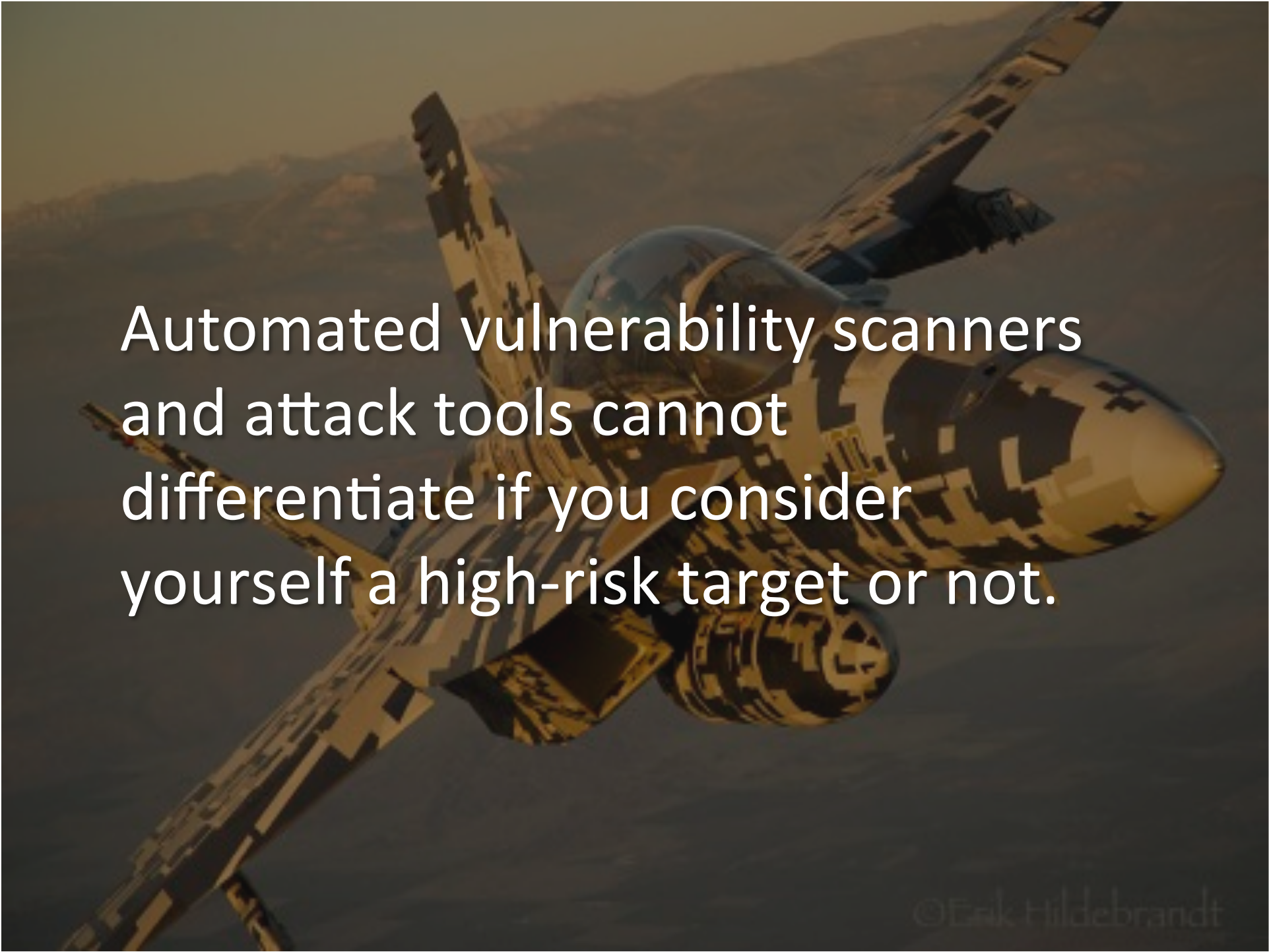
Results in a high degree of attack automation
from systematic identification of targets to fully automated exploitation



Leads to an increase in opportunistic attacks
as the attacker no longer needs expertise or special skills



***Any enterprise can become a victim of attack:
at any time, for any reason, and without being
specifically targeted.***

A fighter jet, possibly an F-16, is shown in flight against a backdrop of a hazy, mountainous landscape. The jet is painted in a dark camouflage pattern and is viewed from a low angle, emphasizing its speed and maneuverability. The text is overlaid on the left side of the image.

Automated vulnerability scanners
and attack tools cannot
differentiate if you consider
yourself a high-risk target or not.

Our Response: Layered Security

We respond and rely on layered security

Key Security Technologies available:

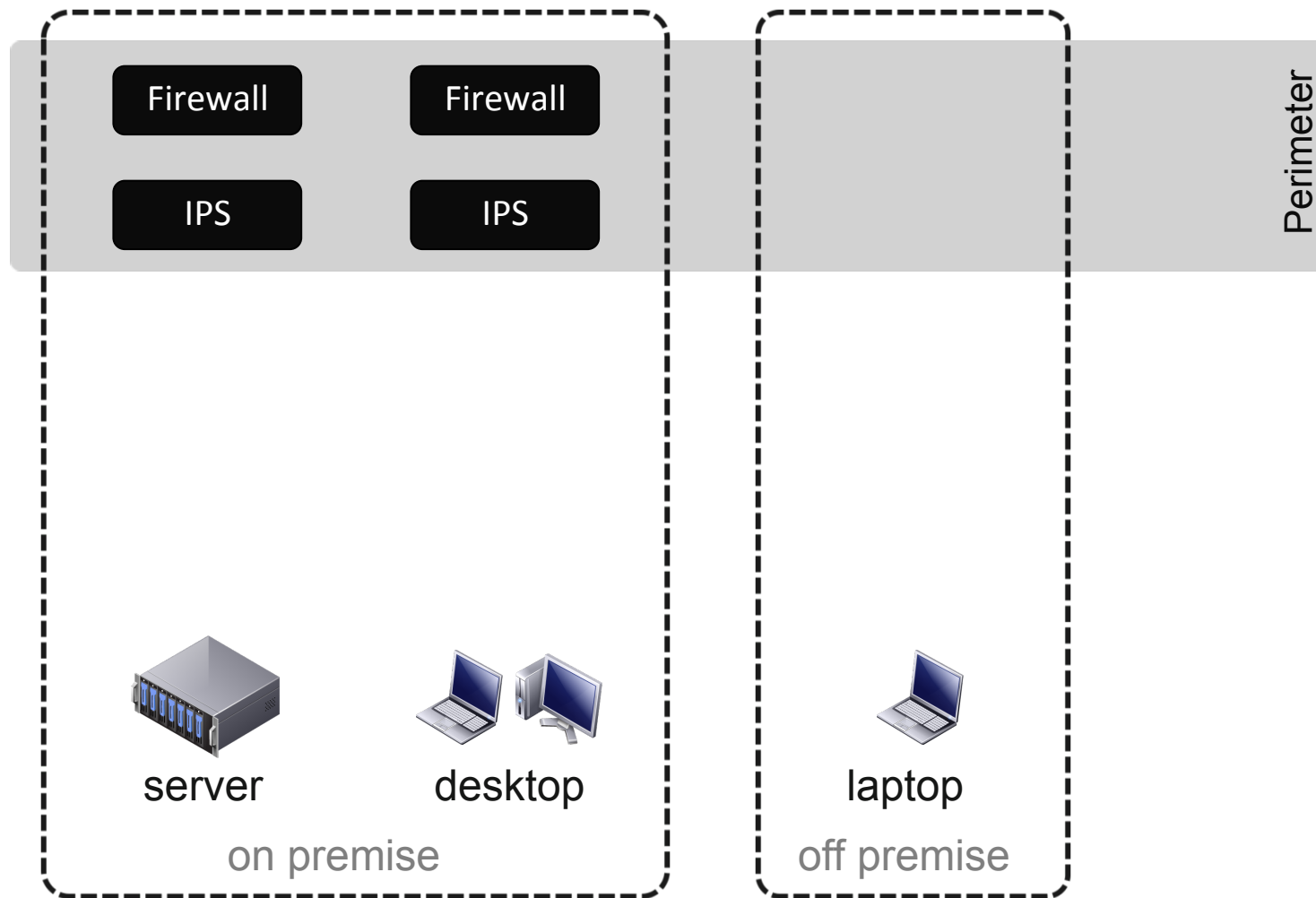
- *Network Firewall*
- *Next Generation Firewall*
- *Intrusion Prevention Systems (IPS)*
- *Antivirus / Antimalware*
- *Browser Protection*



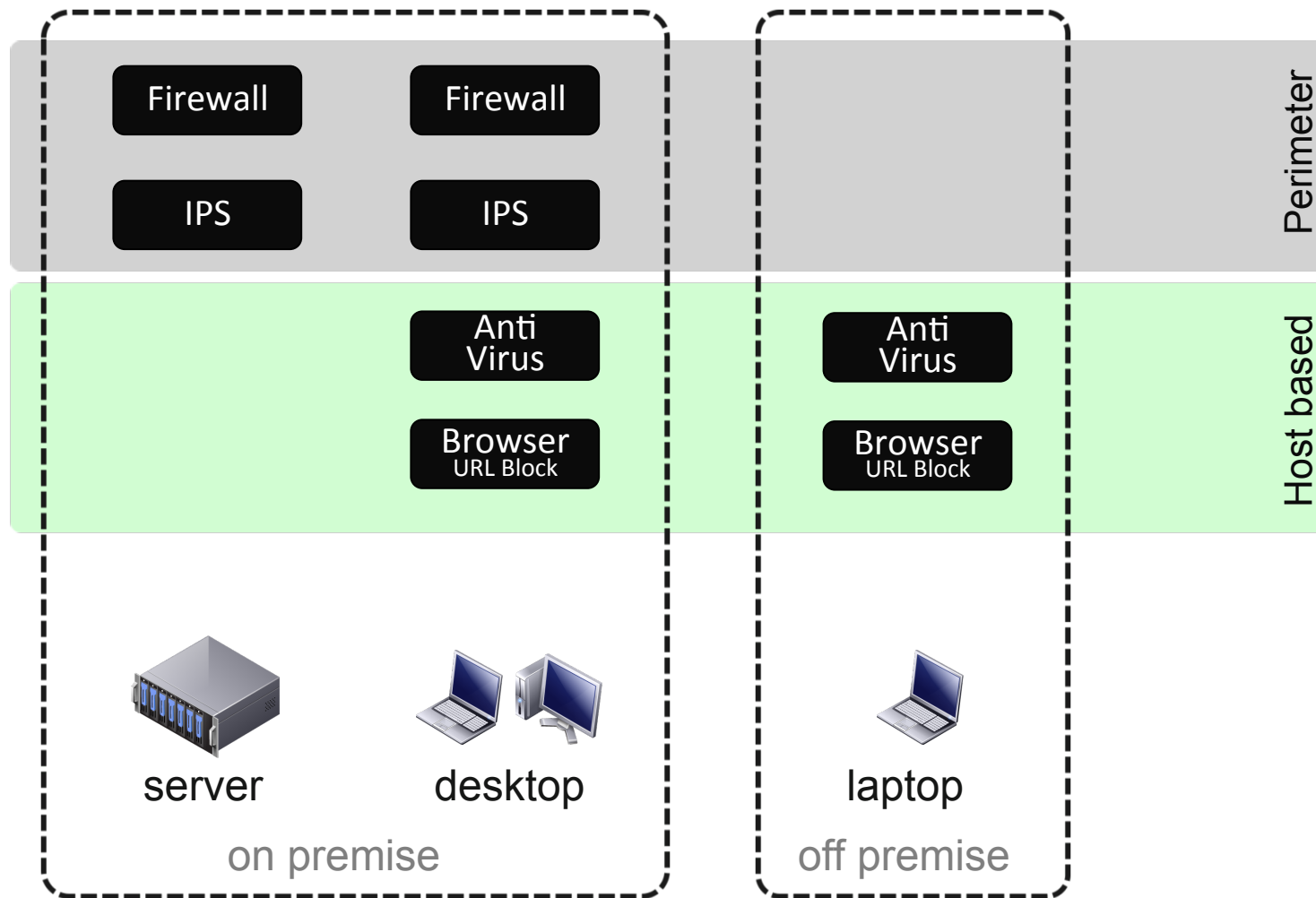
How effective is the defense ?

How do we know?

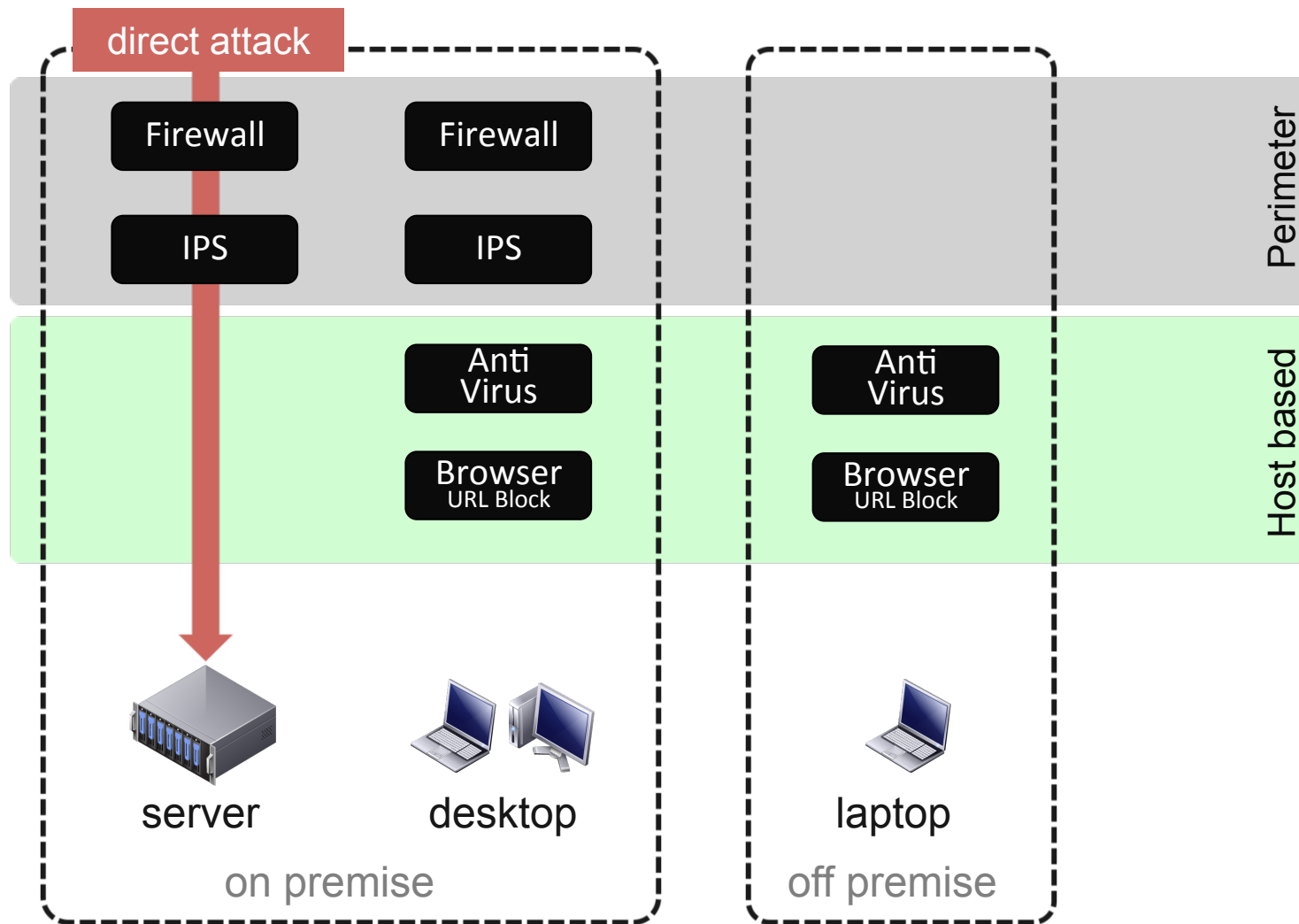
Layered Defense - Perimeter



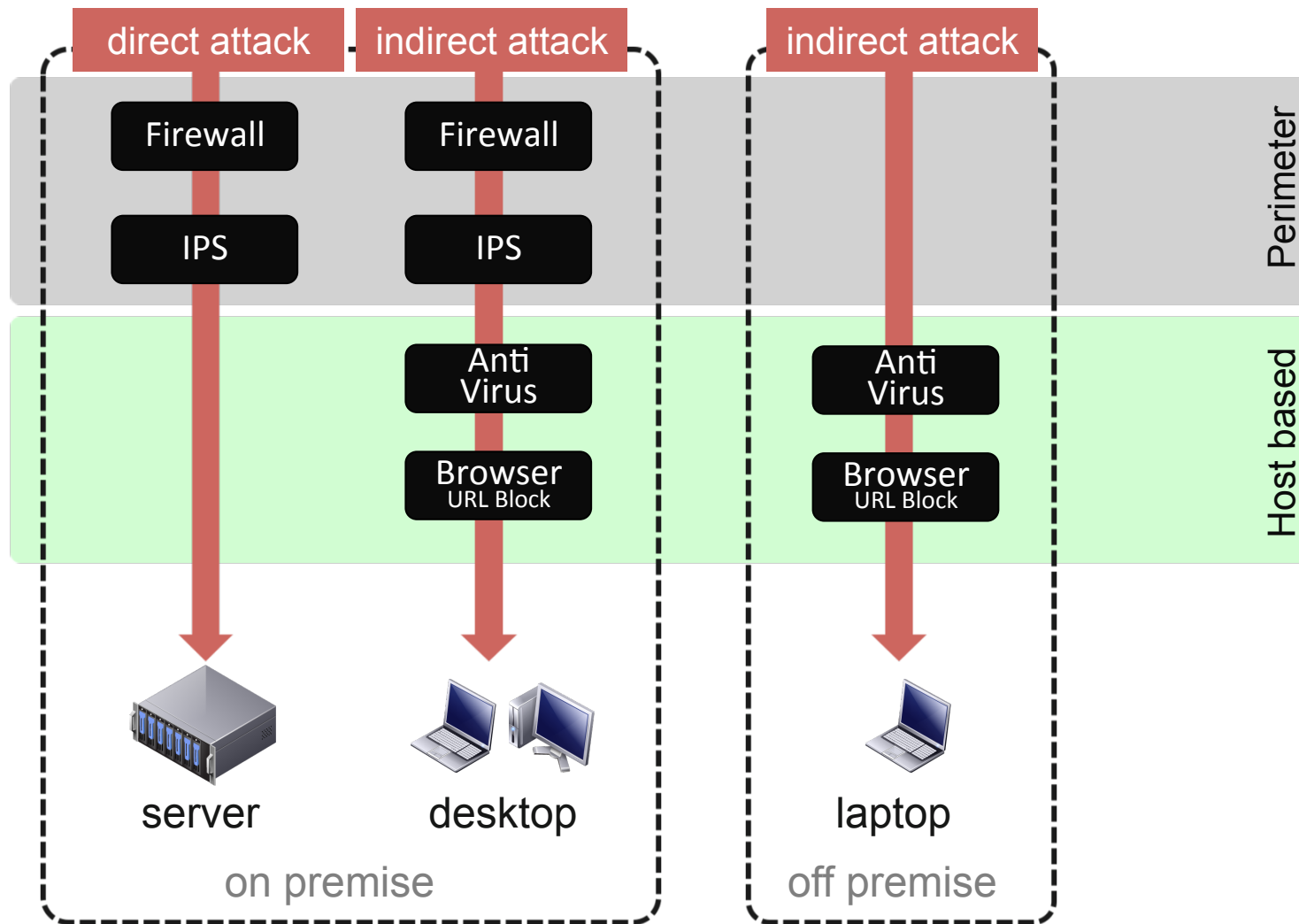
Layered Defense – Host Based



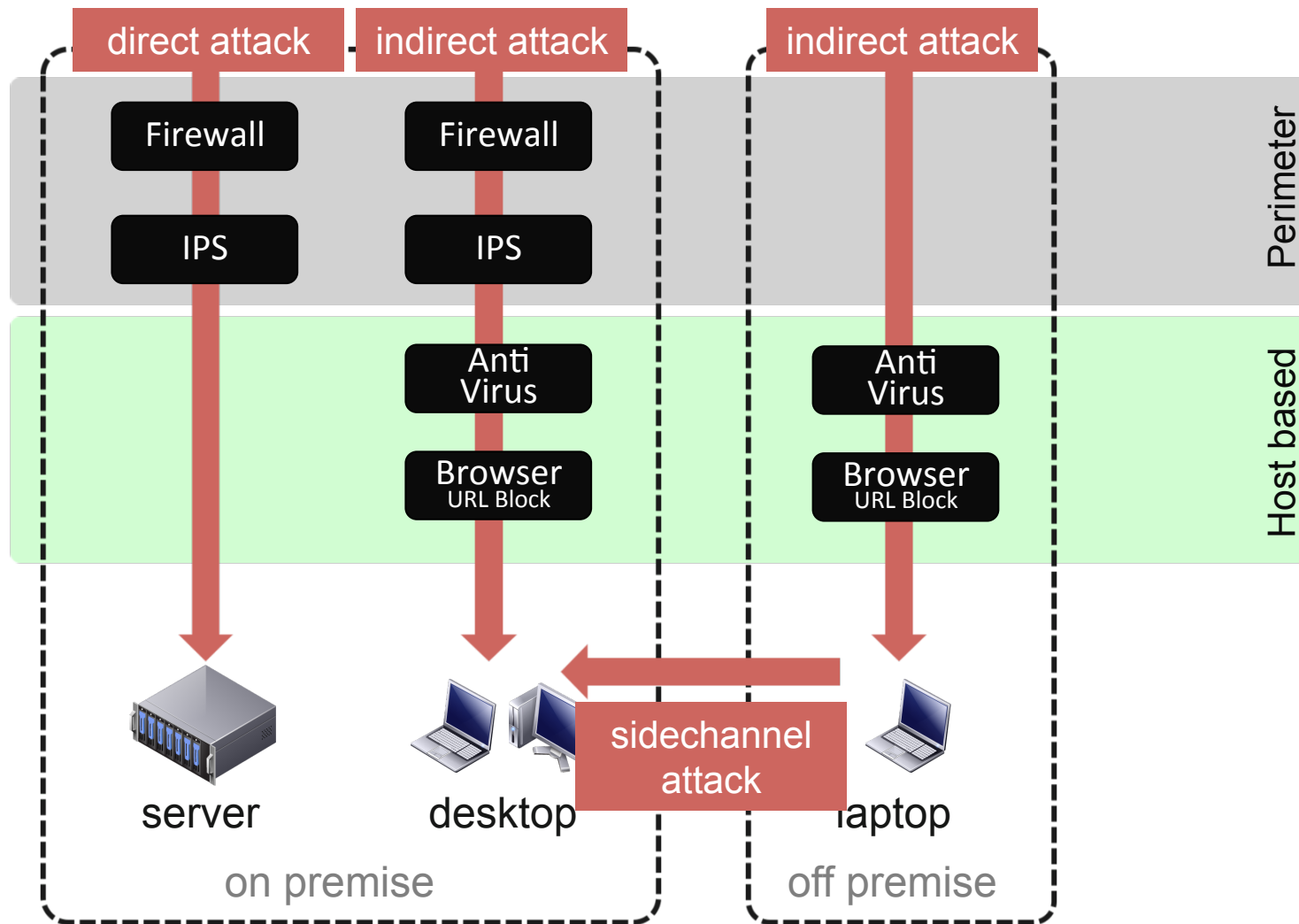
Layered Defense – Direct Attack



Layered Defense – Indirect Attack



Layered Defense – Side channel Attack



Or any of these:



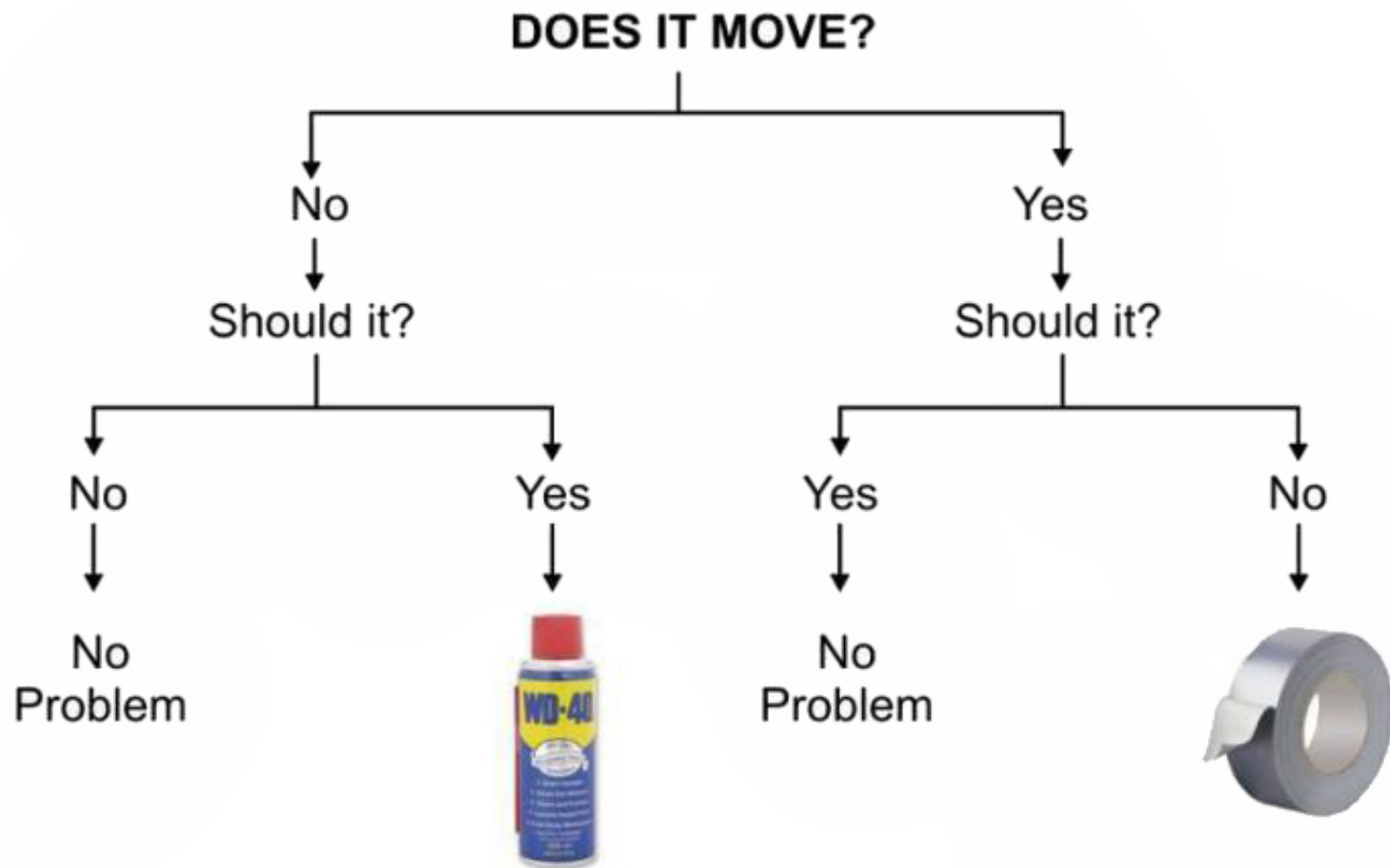
We are doing this:



A night photograph of a city skyline, likely New York City, with the Empire State Building prominently lit in green. The sky is dark and filled with several bright, jagged lightning bolts. The city lights are visible in the foreground and middle ground, creating a dense pattern of yellow and white lights.

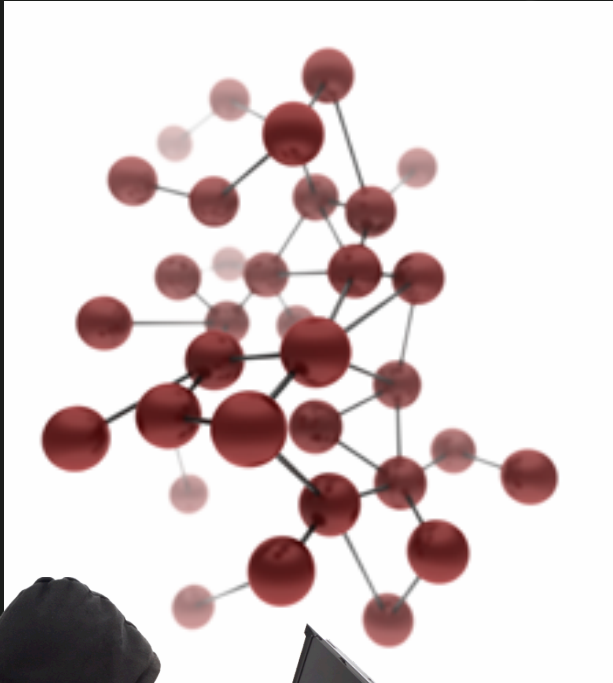
Wizard-like knowledge...

Engineering Workflow ..



.. sadly, security testing is not that simple

It's more like this -



Where does the data come from?

- Multi-million dollar research and testing facility in Austin, Texas
- Capable of 24 x 7 testing
- Global research network captures Internet threats, zero-days & trends live, as they arise



Security Test Metrics

To determine the security effectiveness of devices, the following metrics were used:

1. Exploit Block Performance
2. Anti Evasion Performance
3. Performance & Leakage
4. Stability & Reliability



Exploit Block Performance

Metric

1

- The same types of attack as used by modern cyber criminals
- Utilizing multiple commercial, open source and proprietary tools as appropriate
- More than 1,400 exploits, tested such that
 - a **reverse shell** is returned, allowing the attacker to execute arbitrary commands
 - a malicious **payload is installed**
 - a system is **rendered unresponsive**



Anti Evasion Performance

Metric

2

- Providing exploit protection without factoring in evasion/obfuscation is misleading
- Additional test cases are generated for each appropriate evasion technique.
 - At TCP, IP, and application protocol level
 - Fragmentation, Segmentation, Obfuscation, Encoding, Compression and all combinations thereof



Performance and Leakage

Metric

3

- Trade-off between security effectiveness and performance
Ensure vendors don't take **security shortcuts** to maintain or **improve performance**
- Evaluated based upon three traffic types
Based on hundreds of metrics such as connection rates, latency, delta in performance with different packet sizes and HTTP response sizes, stateful/connection tracking capabilities, ..
 - a mix of perimeter traffic common in enterprises
 - a mix of internal traffic common in enterprises
 - 21KB HTTP response traffic



Stability & Reliability

Metric

4

- Long-term stability is particularly important for an in-line device

Verify the **stability** of the device under test

- Tests the ability to maintain security effectiveness under normal & malicious traffic load

Products that **are not able** to sustain legitimate traffic (or which crash) while under hostile attack **will not pass**

Security Effectiveness

- Security Effectiveness
combines measured *cost of ownership*, *security protection*, *performance*, *leakage*, and *stability*
- Security Value Map (SVM)
shows *security effectiveness* and *value* (cost per protected Mbps) of tested product configurations
- Customizable
SVM is *customizable* to reflect individual weights of the different factors



NSS Labs tested:

6

Network Firewalls

Q3/2012

15

Intrusion Prevention Systems

Q3/2012

13

End-point Antivirus Suites

Q4/2012

4

Browsers

Q3/2012

6

Next Generation Firewalls

Q4/2012

Network Firewalls

- Three of the six products tested crashed when subjected to our stability tests

This **lack of resilience** is **alarming** and indicates the presence of a vulnerability that could be exploited

- Performance claims in vendor datasheets are generally grossly overstated

Performance based on RFC-2544 (UDP) does **not reflect real world** environments

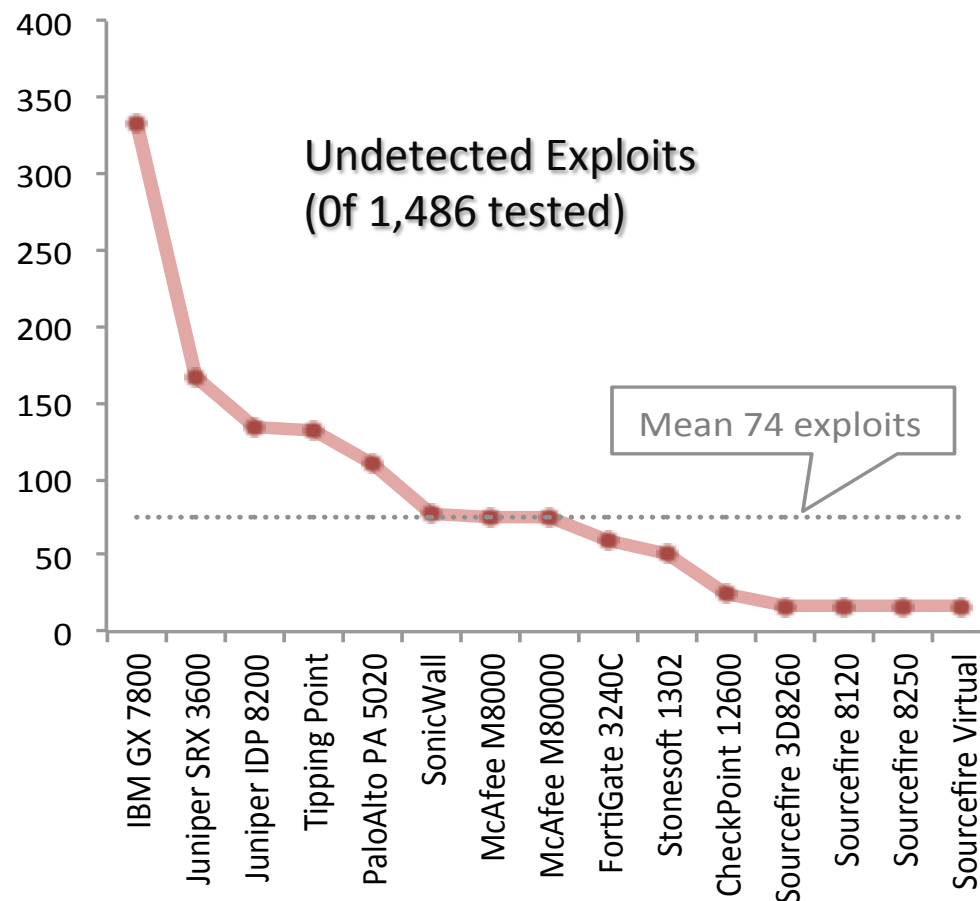
- Five of the six products failed the TCP Split Handshake test

Allowing an attacker to reverse the flow and bypass security. Four vendors released a patch within a month

Network Firewalls

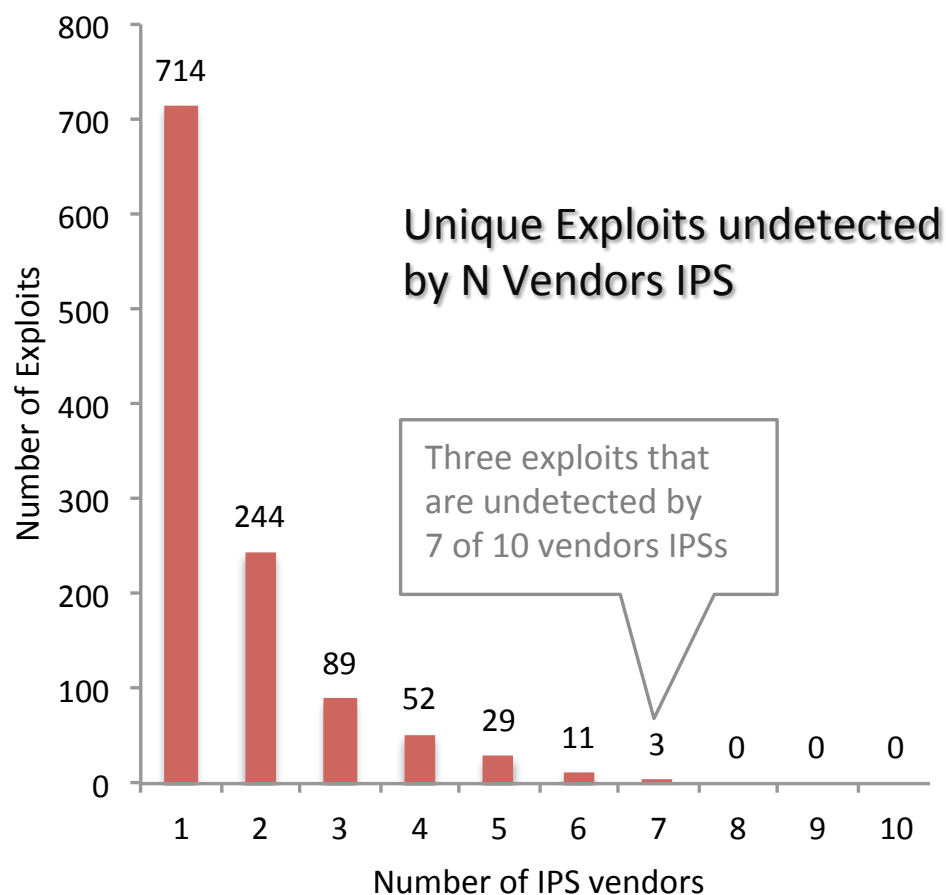
- Longstanding, tried, and field proven technology, such as firewalls, **can still fail** on basic networking attacks
- Attacks never expire – security devices must maintain protection for the **complete range** of attacks
- Independent tests are valuable to identify, and have **vendors remediate** shortcomings

● Intrusion Prevention Systems IPS



- Exploit block rate varies between **77% and 98%**
- Tuning of the **IPS policy** makes a difference, **up to 50%** less protection with default policy
- Evasion detection has **improved** considerably, all but one vendor tested passed

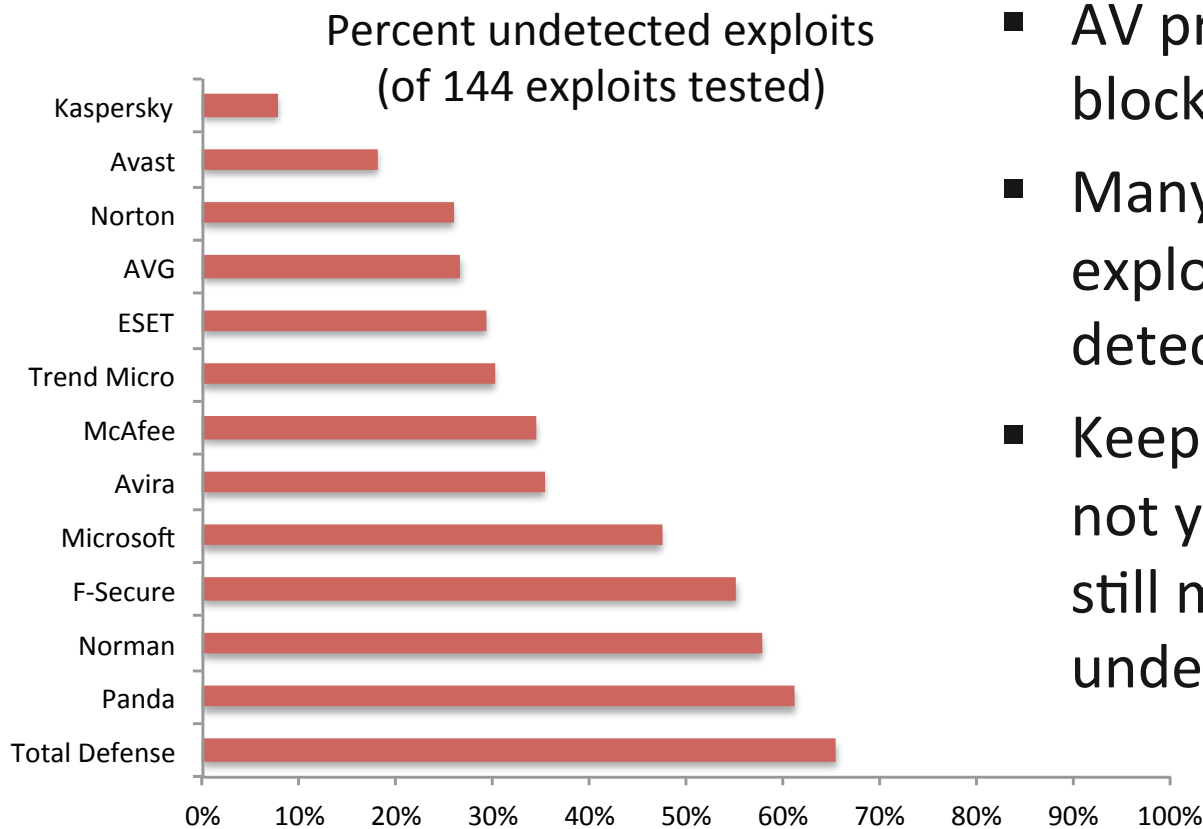
● Intrusion Prevention Systems IPS



- **Correlation** of undetected exploits between vendors products
- Only a **small set of exploits** is required to successfully bypass all IPS products
- Only one combination of different IPS products blocked all exploits



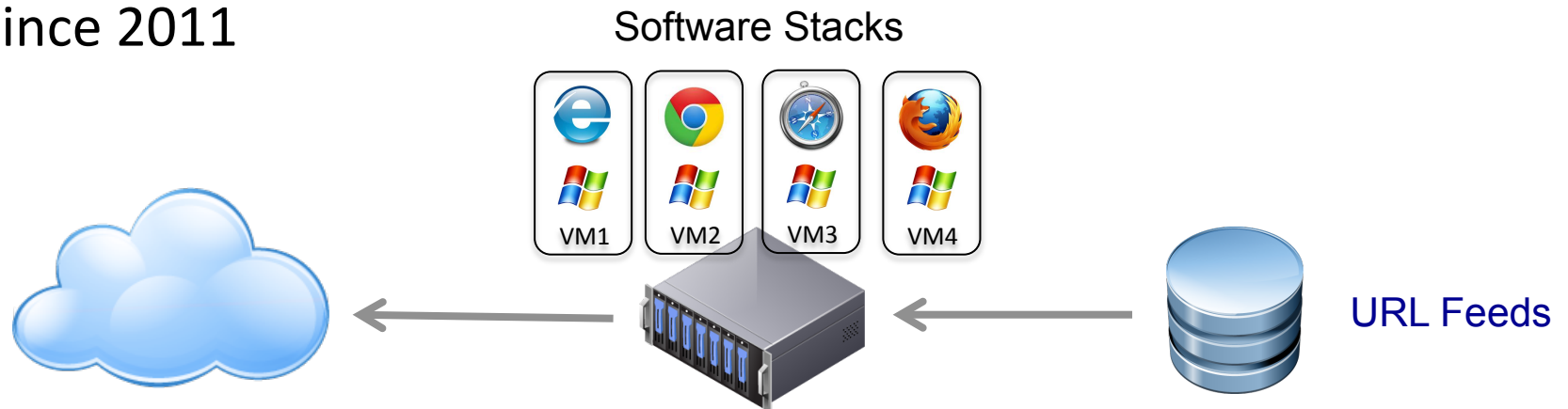
End-Point Antivirus



- AV products differ **up to 58%** in block performance
- Many products **failed to detect** exploits over HTTPS that were detected over HTTP
- Keeping AV up-to-date does not yield adequate protection, still many **old exploits** remain undetected

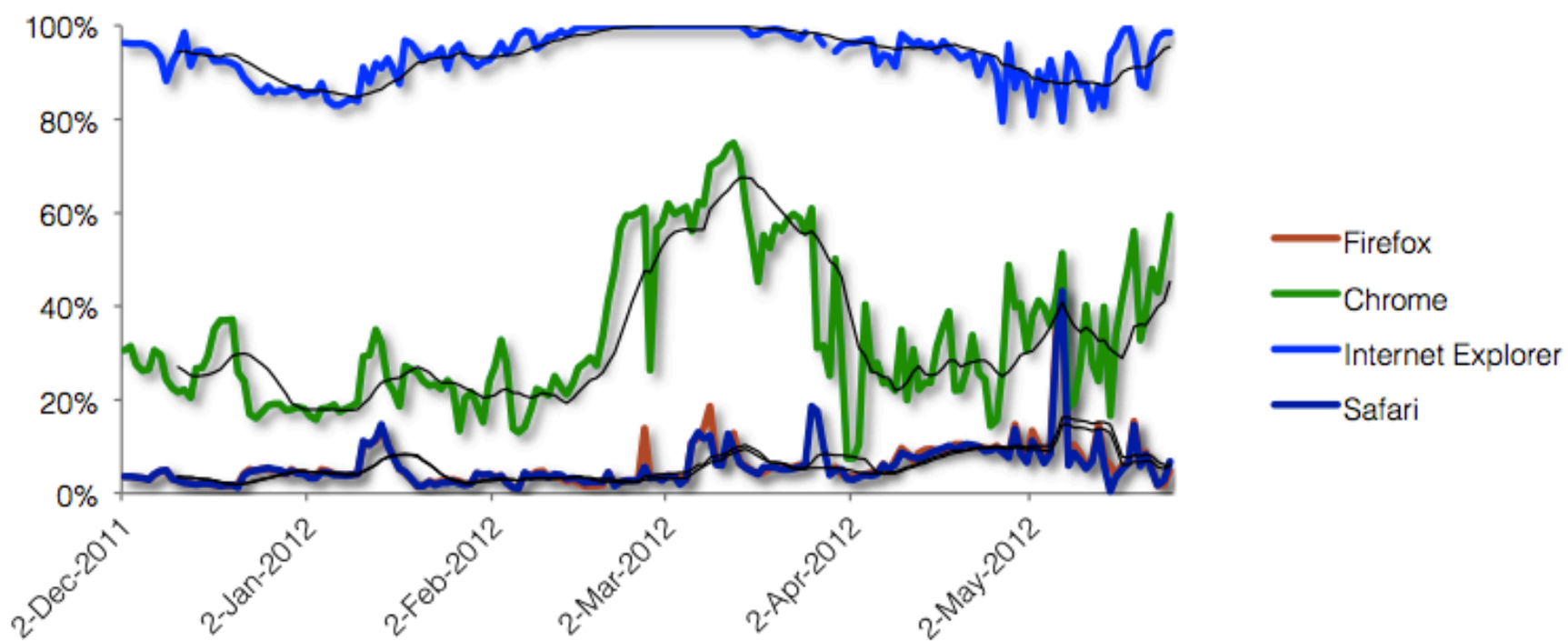
Browser Block Performance

- Browsers offer the largest attack surface in most enterprise networks
- Browsers are the most common vector for malware installations
- NSS Labs continuously measures browsers block performance since 2011



Browser Block Performance

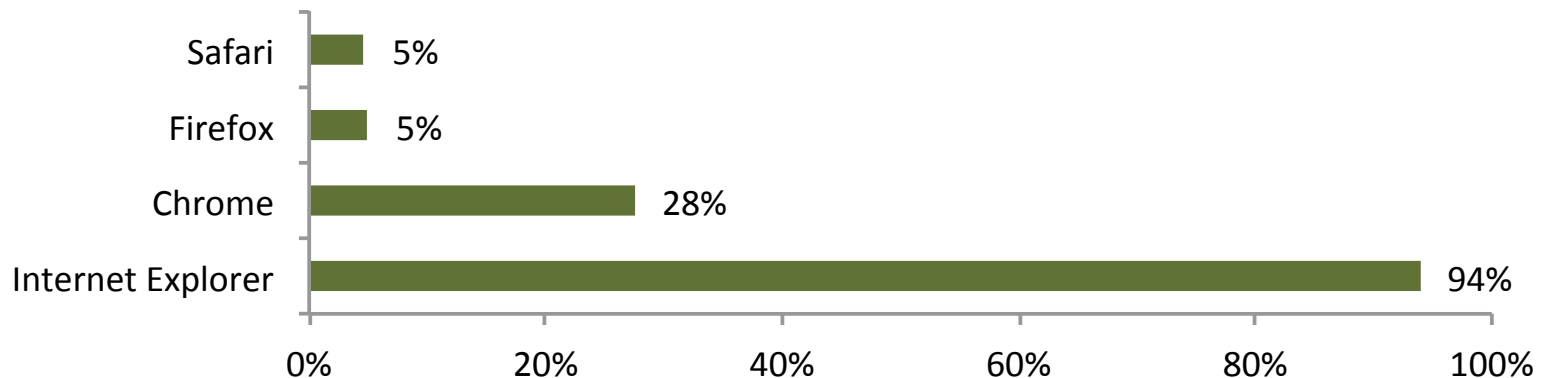
Suspicious URL block performance



Browser Block Performance

- Internet Explorer maintained a malware block rate of 95%
- Firefox and Safari's block rate was just under 6%
- Chrome's block rate varied from 13% to 74%

Percent blocked URLs





Opportunity for Cybercriminals

=

exploits

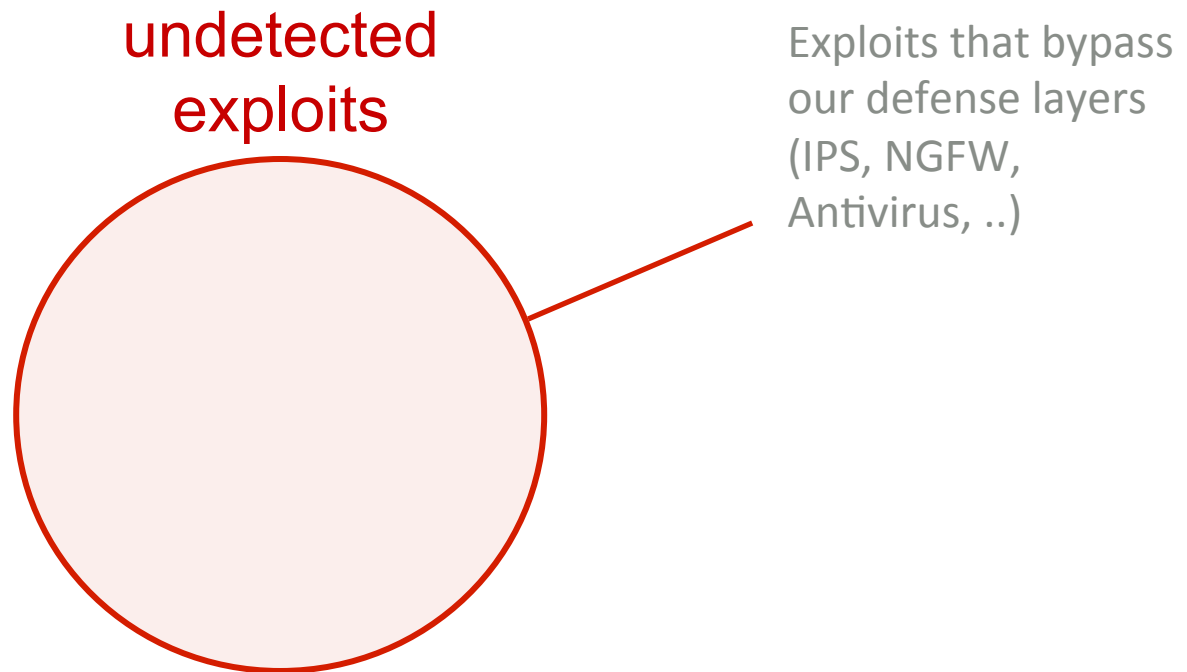
x

targets

x

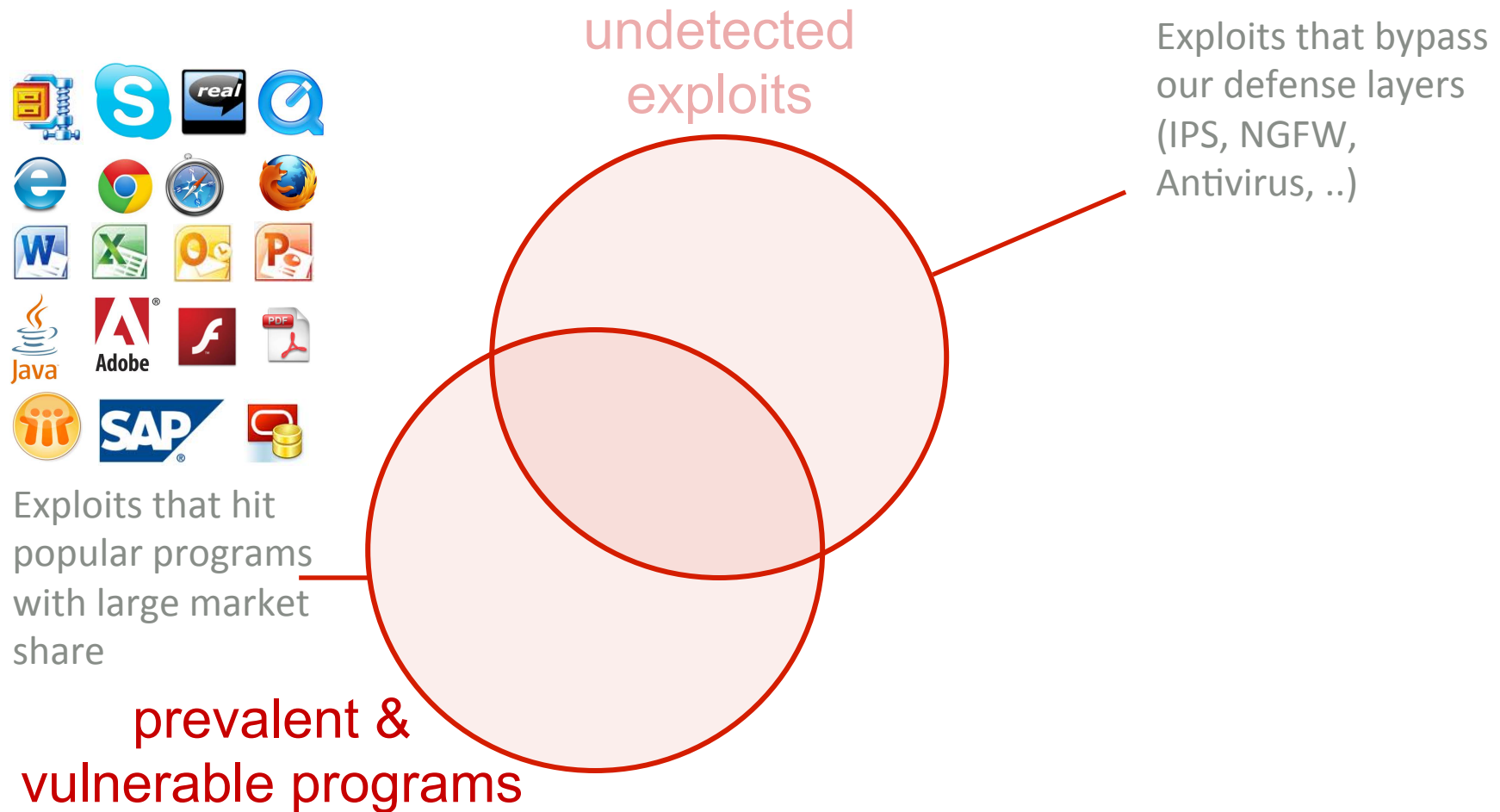
exploit
availability

Undetected Exploits



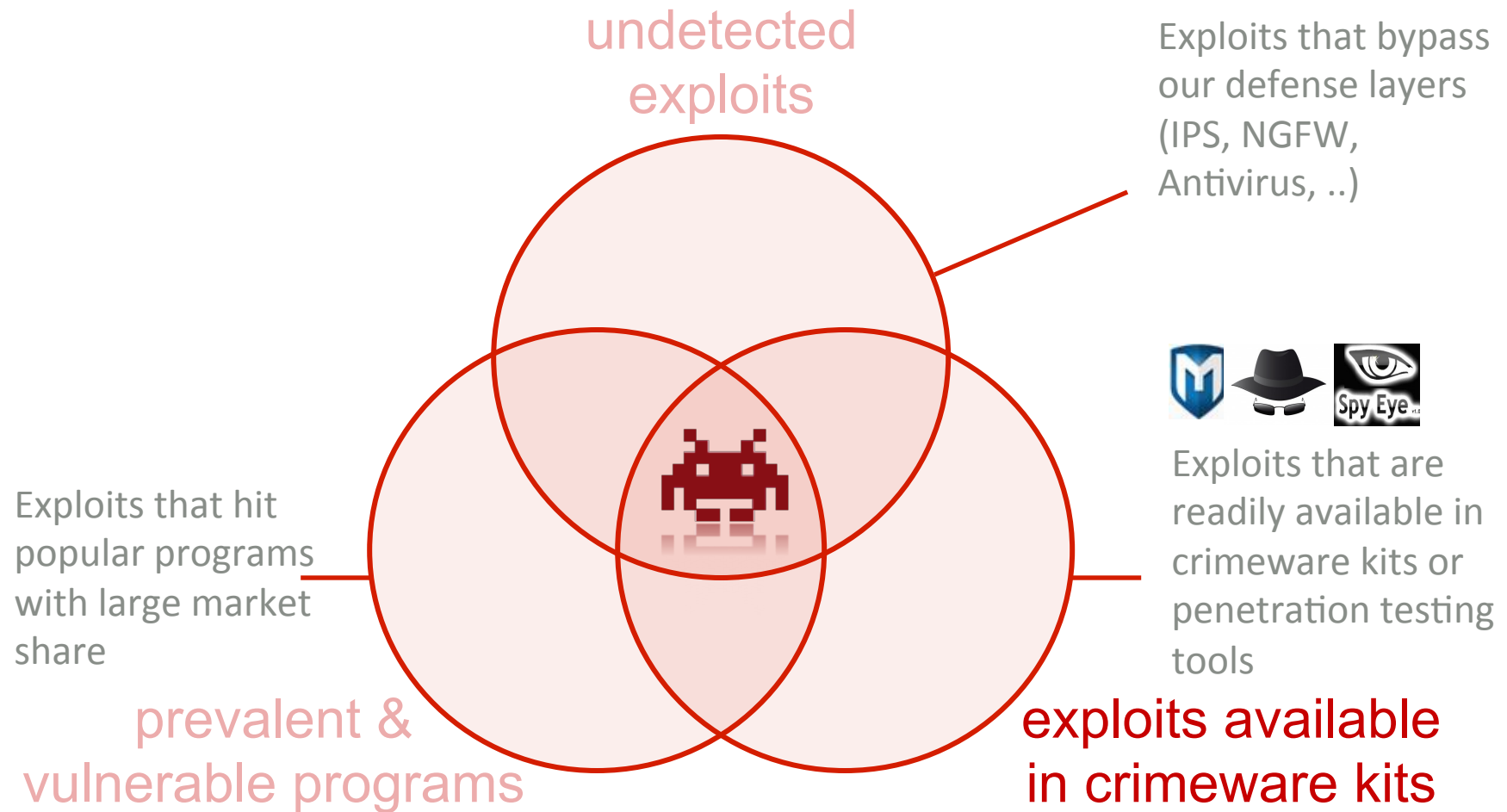
Sadly enough, these exploits exist and are plentiful ..

Exploits for prevalent programs



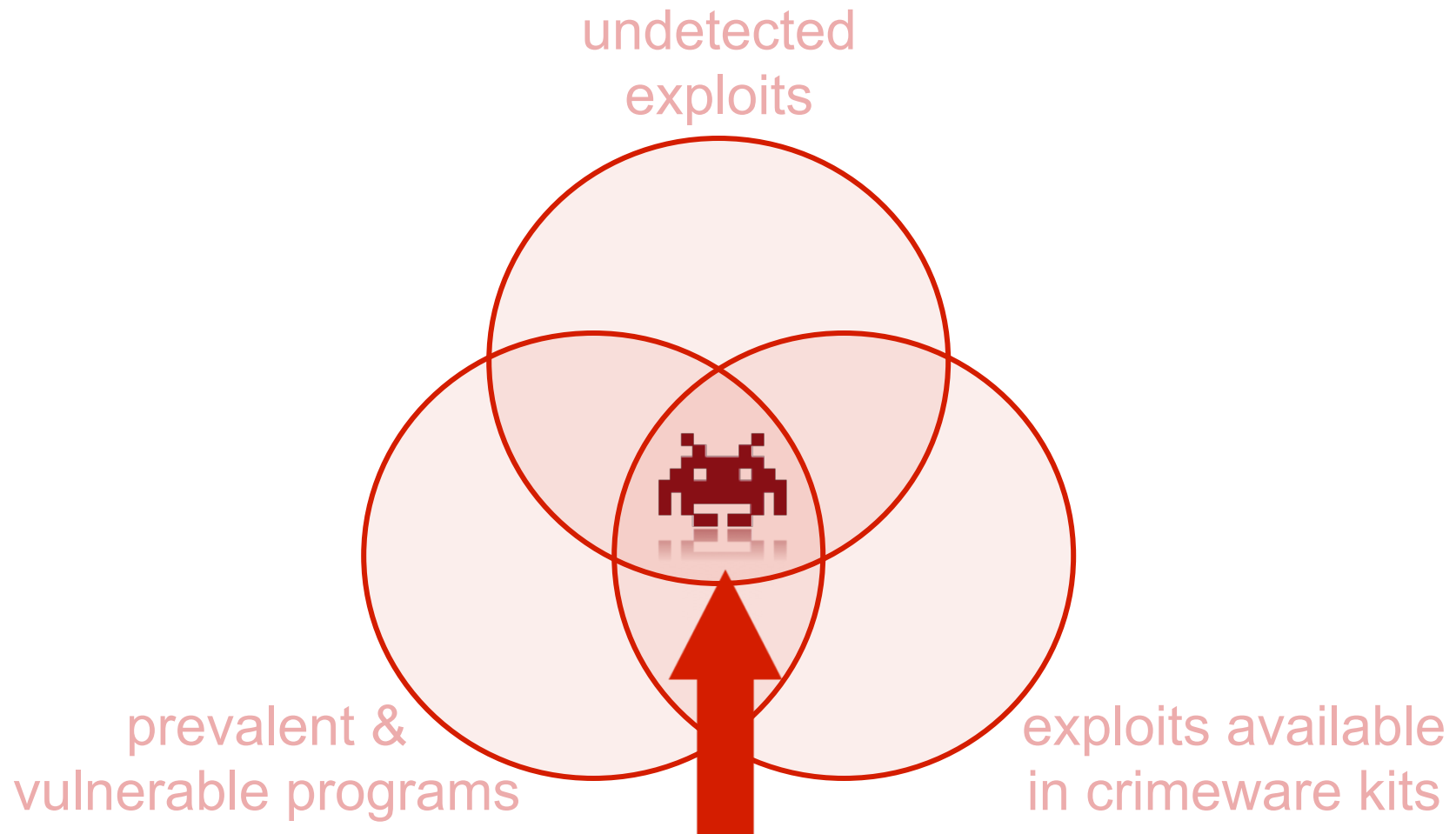
Exploits for popular programs are a dangerous beast ..

Proven and readily available exploits



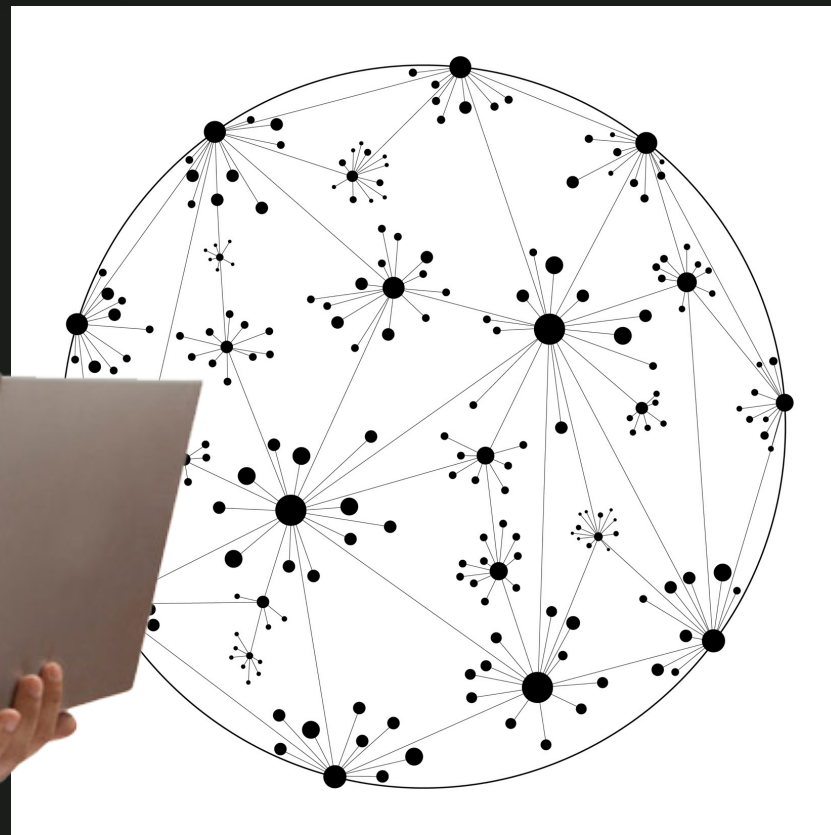
Make them readily available for everyone with a criminal mind calls for disaster!

Failure of the security industry



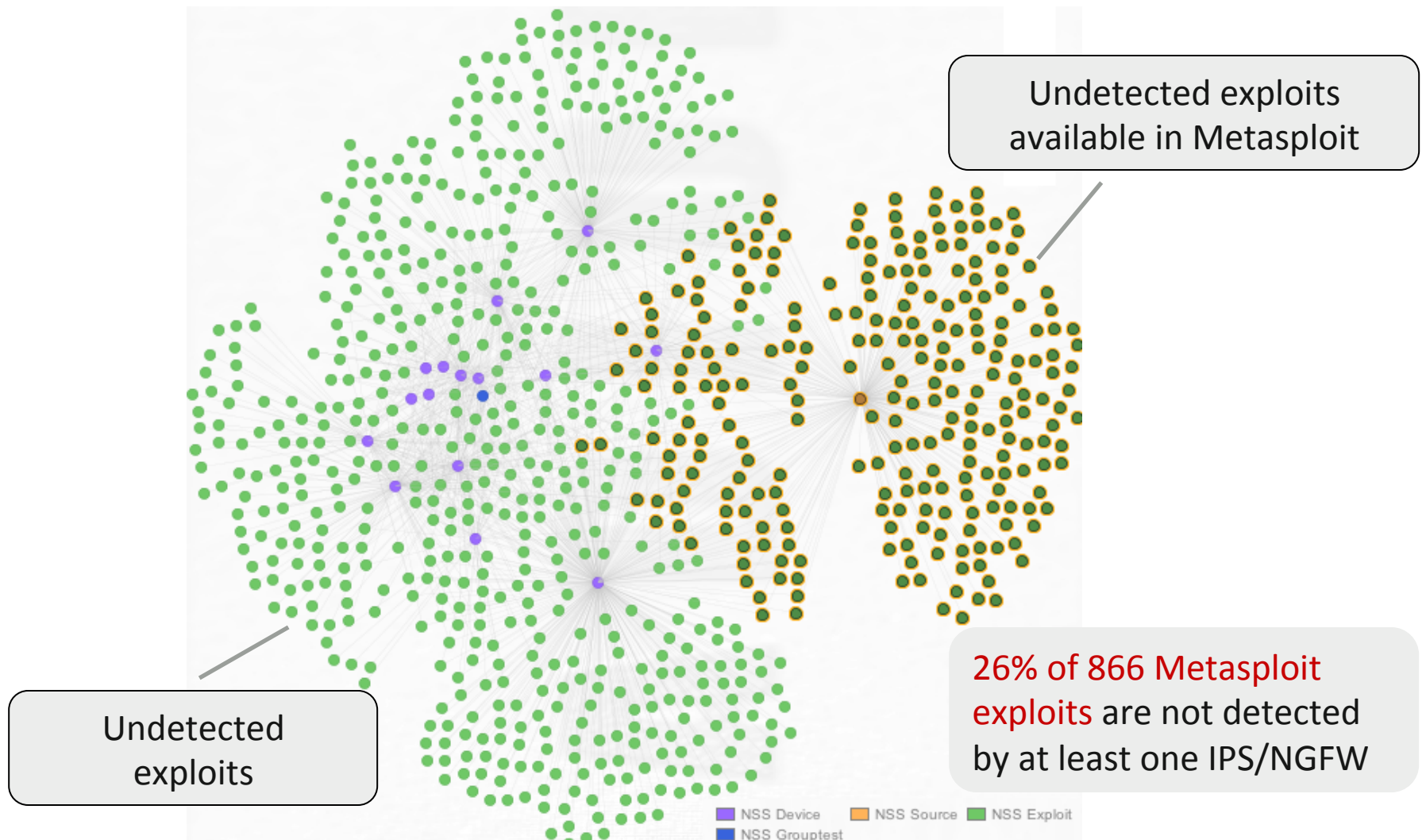
Security products failing to detect these exploits are hardly acceptable

Demonstration



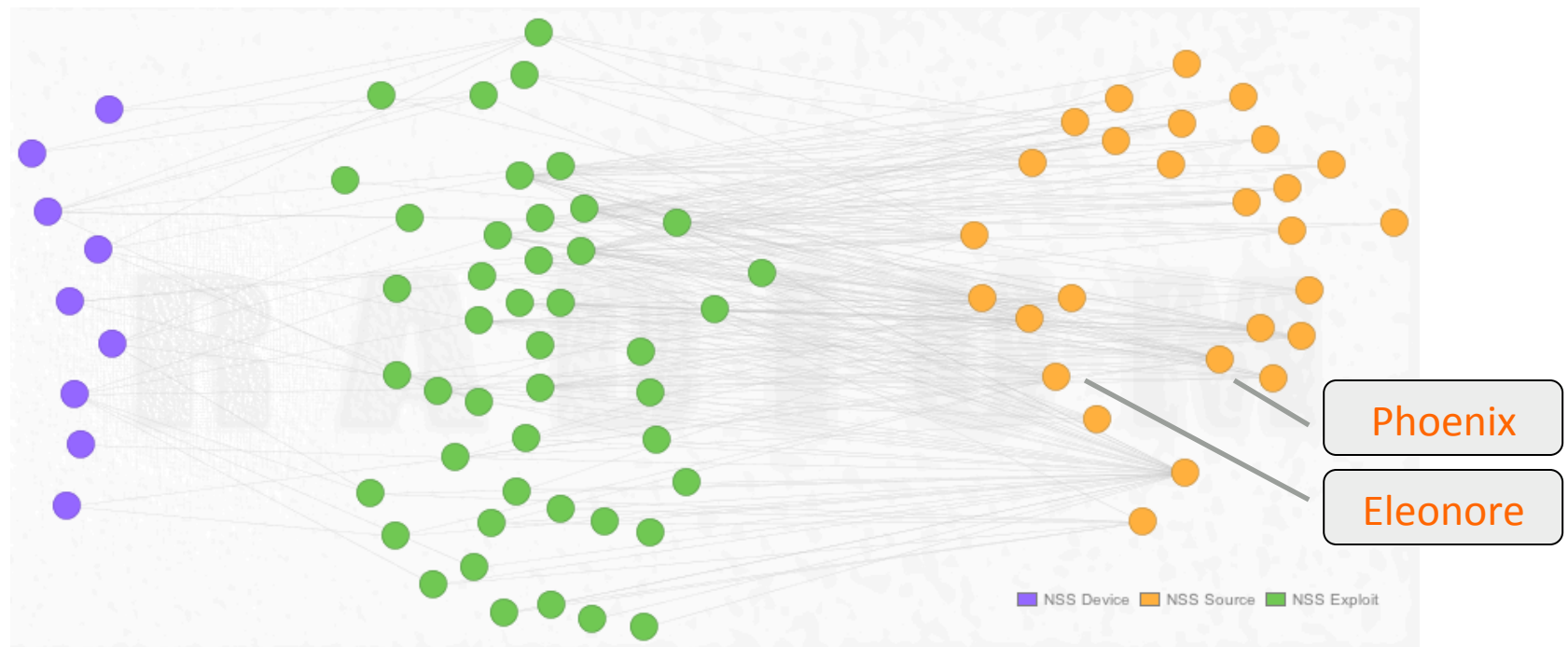
Undetected Exploits vs. Metasploit

Correlation of exploits not detected by IPS/NGFW with exploits available in Metasploit
Many publicly available and easy to use exploits bypass detection



Correlation of undetected Exploits

Exploits available in crimeware kits are still undetected by IPS or NGFW engines.
43 of 117 exploits that could be attributed to crimeware kits bypassed detection
of 9 of 23 detection engines



IPS/NGFW devices
that missed exploits

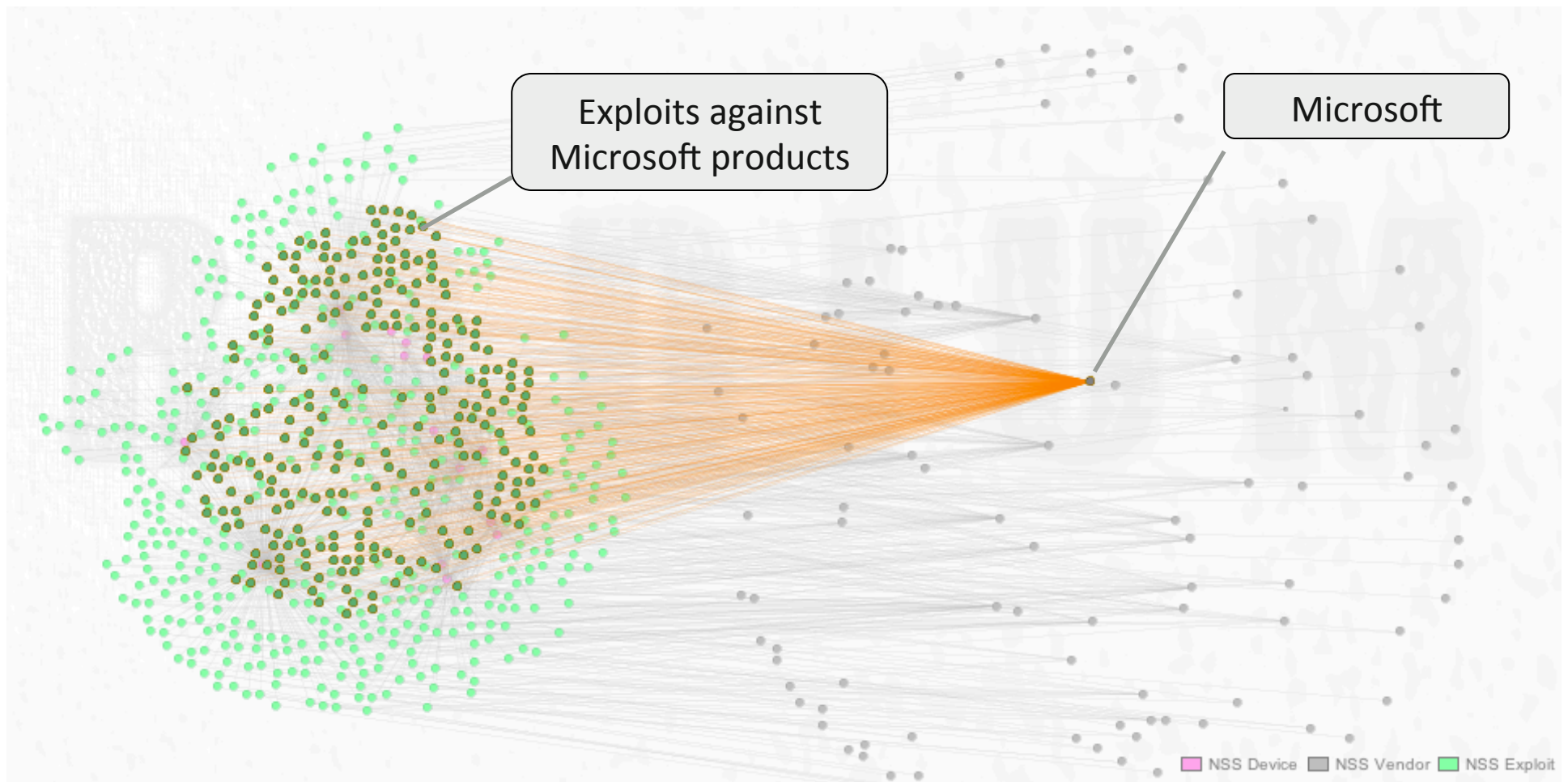
Undetected exploits
from crimeware kits

Crimeware kits

Undetected Exploits vs. Attacked Vendor

Correlation of exploits not detected by IPS or NGFW with the software vendors of the programs targeted by these exploits

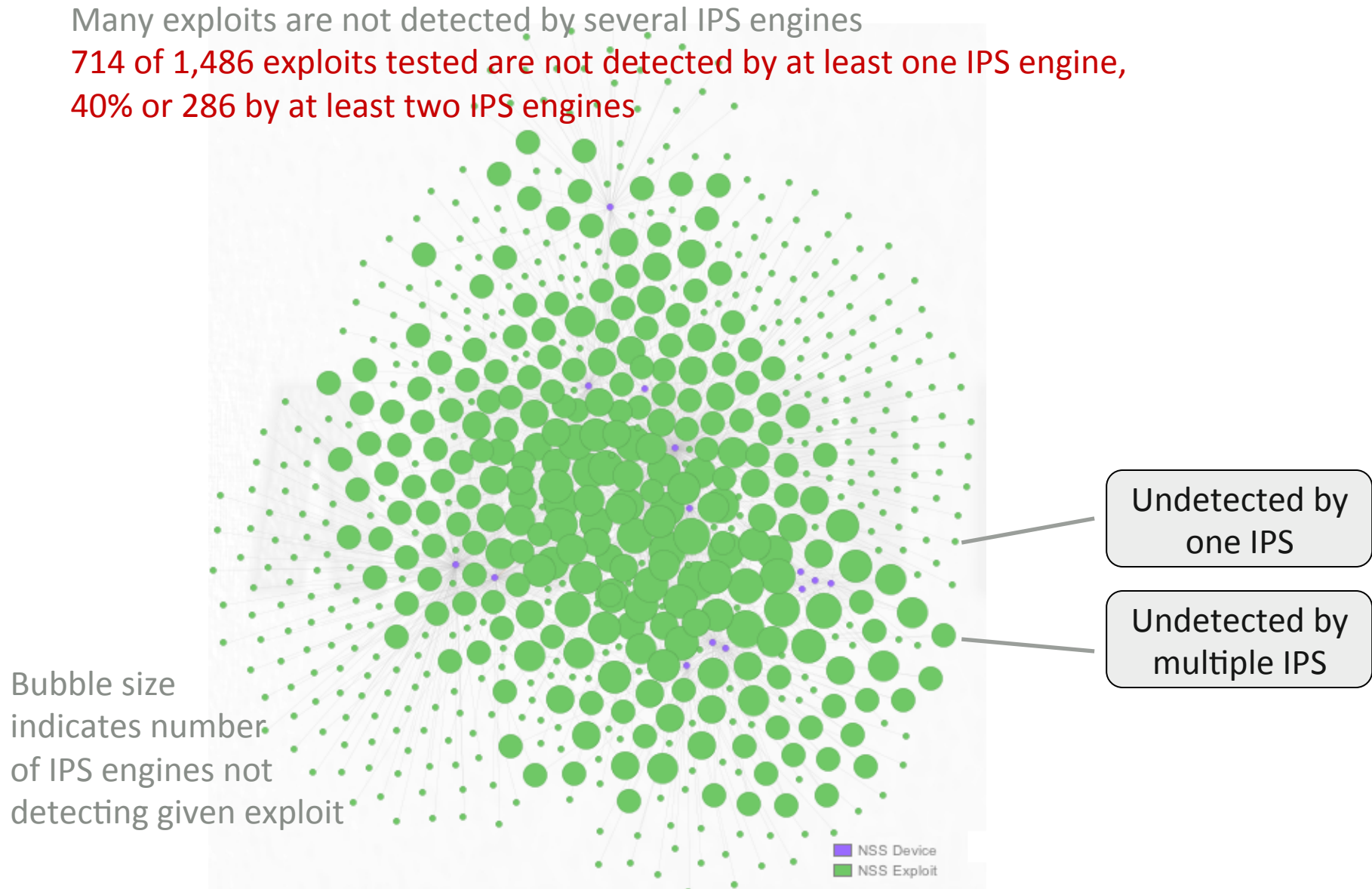
Most undetected exploits target Microsoft products – relevant exploits go undetected!



Correlation of undetected Exploits

Many exploits are not detected by several IPS engines

714 of 1,486 exploits tested are not detected by at least one IPS engine,
40% or 286 by at least two IPS engines



Combined Failure Rate

Attacker



Layered Defense

Device A



Failure Rate

 P_A

10%

Device B



Failure Rate

 P_B

10%

Target



Combined Failure Rate

 $P_{A \circ B}$

?

$$P_{A \circ B} = P_A \cdot P_B = 1\% \quad (?)$$

Correlation Fallacy

- Rethink your risk assessment

$$P_{A \circ B} \neq P_A \cdot P_B$$

- Failures are correlated, they are not independent events

- The combined failure rate is typically considerably higher $P_{A \circ B} > P_A P_B$

Conclusion & Findings

- Vendor claims on the effectiveness or performance of products are frequently overstated, or based on non-realistic assumptions
- Several network firewall products tested crashed when subjected to our stability tests
- Antivirus does not prevent a dedicated attacker from compromising a target
- Several products failed detection of exploits when switching from HTTP to HTTPS

Recommendations

- There is no product or combination of products tested by NSS Labs that provide 100% protection
- Assume that you are already compromised
- Organizations should complement prevention with breach detection and SIEM to identify and act on successful security breaches in a timely manner
- Access to independent information on security product effectiveness and performance is important

Complexity

- Technology alone cannot provide the highest protection
- Competent and motivated security personal is key to effective security – and make the best use of the tools



Thank you

sfrei@nsslabs.com

frank@nsslabs.com



Resources

- Network Firewall Group Test 2011
<https://www.nssslabs.com/reports/network-firewall-group-test-2011>
or <http://bit.ly/RzLX3a>
- IPS Comparative Analysis 2012
<https://www.nssslabs.com/reports/ips-comparative-analysis-2012>
or <http://bit.ly/SvHfjQ>
- Consumer AV/EPP Comparative Analysis - Exploit Protection
<https://www.nssslabs.com/reports/consumer-avepp-comparative-analysis-exploit-protection>
or <http://bit.ly/S5Mqs7>
- Is Your Browser Putting You At Risk?
<https://www.nssslabs.com/reports/your-browser-putting-you-risk-part-1-general-malware-blocking>
or <http://bit.ly/SvGHur>
- Targeted Persistent Attack (TPA)
<https://www.nssslabs.com/reports/analysis-brief-targeted-persistent-attack-tpa-misunderstood-security-threat-every-enterprise>
or <http://bit.ly/SvGO99>