

Modern Malware

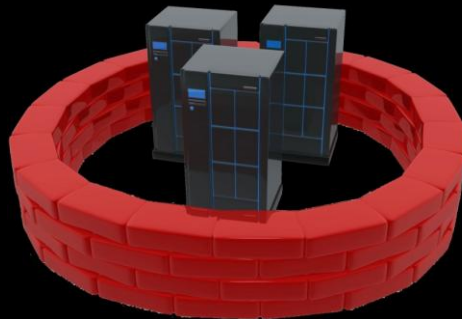
Nir Zuk

Founder and CTO

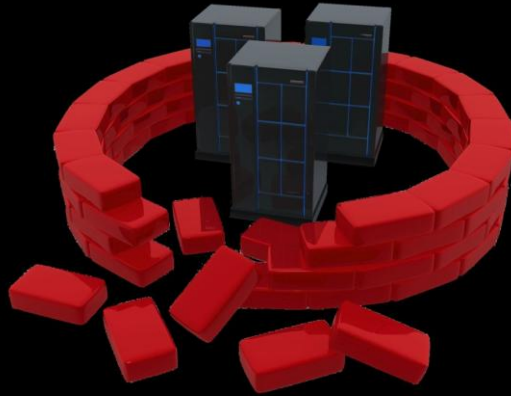


data breach mythology

we invest in protecting our data centers



rarely the datacenter is **attacked** directly



no more **vulnerability** scanning



the new **attacker**

the **attacker** is not a bored geek



nation states and organized crime



data breaches in 2011

step one: **bait** an end-user



step one: **bait** an end-user



spear phishing

step one: **bait** an end-user



step two: **exploit** a vulnerability



step three: download a **backdoor**



step four: establish a **back channel**



step five: **explore** and **steal**



the ☹️ state of **malware** protection

protection is needed at all stages



bait



exploit



download



back
channel



steal

☹ **bait** protection



☹️ **exploit** protection



exploits come in thru many applications

☹️ **exploit** protection



many months pass between black-hat discovery, white hat discovery, and protection being available

☹️ download protection



targeted attacks mean few instances in the wild

☹️ download protection



anti-malware vendors take several days to come up with a signature

☹️ back channel protection



+



+



not only attacks are targeted and IPS signatures take time to develop, back channels are often encrypted

☹️ explore-and-steal protection



minimal internal security means that once inside, an attacker can roam the network freely

blueprint for **stopping** modern malware

need to protect all **applications**



Dropbox



Salesforce



Microsoft
SharePoint

webex™

response time is key



automation is a must



a **sandbox** at the core



perform the analysis for all devices **centrally**



automatically generate multiple **signatures**

- Anti-malware download signatures
- IPS back-channel signatures
- Malware URLs
- IPS signatures for identified new vulnerabilities

deliver signatures with one hour



stopping modern malware in practice

need to protect at all stages



bait



exploit



download



back
channel



steal

bait protection 😊

- Block unneeded applications
- Control file transfers by user, application, and file type
- Block access to Malware URLs

exploit protection 😊

- Discover vulnerabilities before the bad guys
- IPS signature for newly identified vulnerabilities

discovering Microsoft **vulnerabilities**

Palo Alto Networks	McAfee	Tipping Point	Check Point Software	Sourcefire	Juniper & Cisco
20	7	7	3	1	0

number of vulnerability discoveries credited to each vendor over the last 4 years

Source: OSVDB; as of June 15th 2011

discovering Adobe Flash **vulnerabilities**

Palo Alto Networks	McAfee	Tipping Point	Check Point Software	Sourcefire	Juniper & Cisco
12	1	1	0	0	0

number of vulnerability discoveries credited to each vendor over the last 4 years

Source: OSVDB; as of June 15th 2011

download protection 😊

- Anti-Malware signatures available to the entire participant base within one hour of first discovery
- Generic drive-by-download protection for HTTP/S downloads

back-channel protection 😊

- Block unknown application traffic
- Use heuristics to detect back channel communication
- C&C signatures available for newly discovered malware

explore-and-steal protection 😊

- Network segmentation
- Control access to data by user and application

the role of NGFW in stopping modern
malware

solution has to be enterprise-wide



protection has to be real-time, inline



needs **user-based** access control



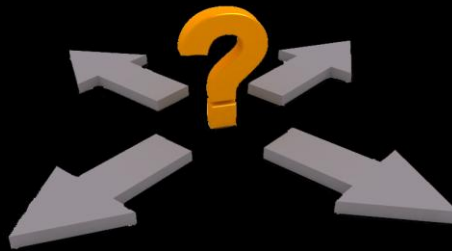
needs **high-speed** IPS and AV



need to perform across all **applications**



need to **block** the unknown



conclusion: advanced-**malware** protection
belongs in a **next generation firewall**



Thank You



the network **security** company™