The Rise of Vulnerability Markets - History, Impacts, Mitigations

Thierry Zoller
EMEA Practice Lead

Threat and Vulnerability Management

altogetherbetter

Agenda

Short Version

- **Brief Introduction**
  - Me, Myself and I
  - Small Announcement & Plug
- **The history and rise of the "Vulnerability Markets"**
  - Crash course - Typical Vulnerability Lifecycle
  - The history behind the shift to Vulnerability Markets
  - Difference of Eco-Systems
  - Vulnerability Market Prices and Value
  - The split up between Mass and Targeted Attacks
- **The implications**
  - Attacker Class Model (Old vs. New)
  - The resulting impacts on the threat landscape and defensive mechanisms / compensating controls
  - Proposal : Use OWASP ASVS (align it to ISO/IEC 27034-1:2011) and adjust development and audit requirements around Assurance Levels

Me, Myself and I

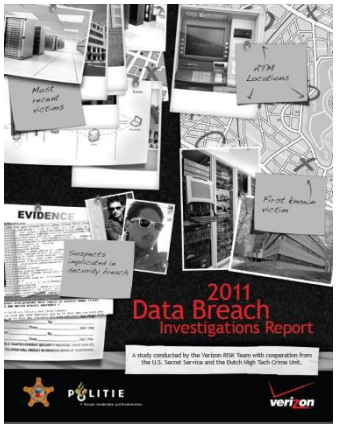
- **Thierry Zoller**
  - Born and raised in Luxembourg
  - EMEA Practise Lead for the Verizon Business "**Threat and Vulnerability Management**" Practice
  - Former Director of Product Security and Security Service @ n.runs
  - Leading the SDLC Efforts EMEA Wide / Microsoft SDL Pro Network Partnership
  - Act as a Application Security Subject Matter Expert

  - My analysis of several 0-Day vulnerabilities are referenced by multiple CERTs (US-CERT, FI-CERT, FR-CERT) and Vulnerability Management Solutions (Qualys,etc)
  - Discovered, reported and coordinated hundreds of Vulnerabilities in Software ranging from Oracle, Apple, Microsoft, Checkpoint to McAfee
  - Endorsed as a TOP 10 security researcher 2009 by IBM X-Force

Who are we ? (that's the plug)

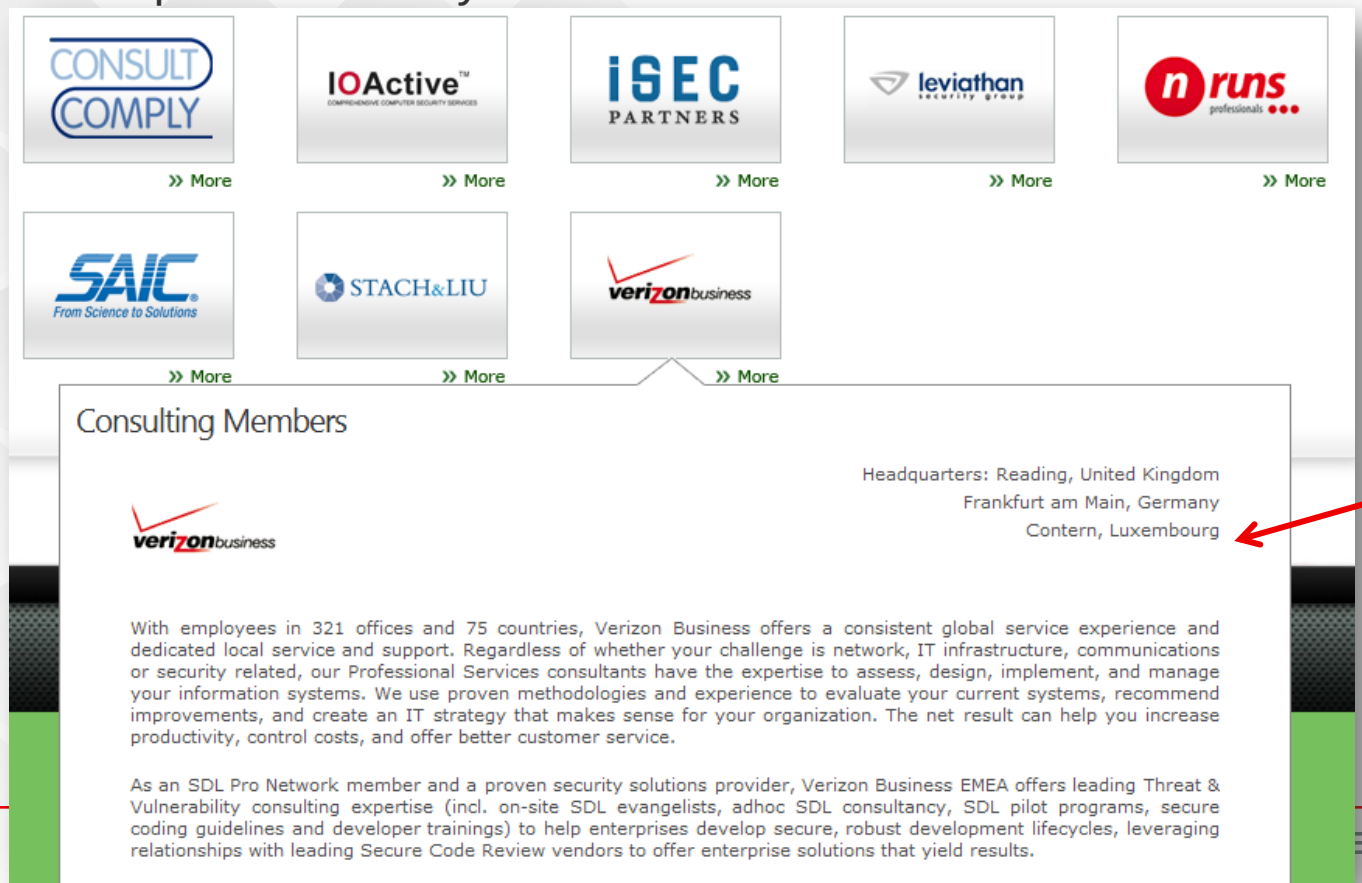
- **Who the heck is Verizon Business ?**
  - Part of Verizon
  - Security Branch is a buy in from Cybertrust (Ubizen), Netsec (Defcom),
  - Global IP Network (2700+ Cities, 150+ Countries, 200+ Datacenters, 4000+ Managed customer networks)
  - 4 SOCs Worldwide
  - 280.000 employees worldwide (VZ)

- **Quick Verizon Business Luxembourg PSF - Facts**
  - We exist.
  - Full Professional Service Capability (GRC, TVM, NIS, BR..)
  - Full SDLC capability
  - EMEA Forensic Lab is located in Luxembourg
  - SOC and Datacenter in LU / MSS 24/24 in LU (PSF)



Partnership (That's the announcement)

- **Announcement :** Verizon Business Luxembourg is now part and leading the Microsoft SDL Pro Network Partnership EMEA Wide
  - Partnership to be formally announced soon



Threat Intelligence

The basis of this talk :

- **Constantly Monitoring the Threat Landscape**
  - Empirical data / Empirical Risk Management
  - Intelligence sources : OSINT, Data breach Report, Underground Monitoring, Forensic Investigations, Security Research, SOC, our CERTs
  - Vulnerability Market Prices :
    - Jason Steer (Private survey amongst Sellers)
    - Charlie Miller (Public)
    - Internal Research (Private survey amongst Buyers, Trusted Contacts)
  - General Inspiration : Dan Guido

What commonalities exist?

83%	of victims were targets of opportunity (<>)
92%	of attacks were not highly difficult (+7%)
76%	of all data was compromised from servers (-22%)
86%	were discovered by a third party (+25%)
96%	of breaches were avoidable through simple or intermediate controls (<>)
89%	of victims subject to PCI-DSS had not achieved compliance (+10%)

- **Disclaimer:** This presentation will cover what we factually know exists, assumptions will be explicitly stated as such.

Introduction

Definitions

- **Notation used during this Presentation**

- **Vulnerability**
  - “A defect/bug that allows an external entity/agent to directly or indirectly influence the availability, reliability, confidentiality or integrity of a system/application/data ”

- **Exploit / Proof of Concept**
  - “ A program that makes use of a vulnerability to deliver a harmless payload such as a crash”

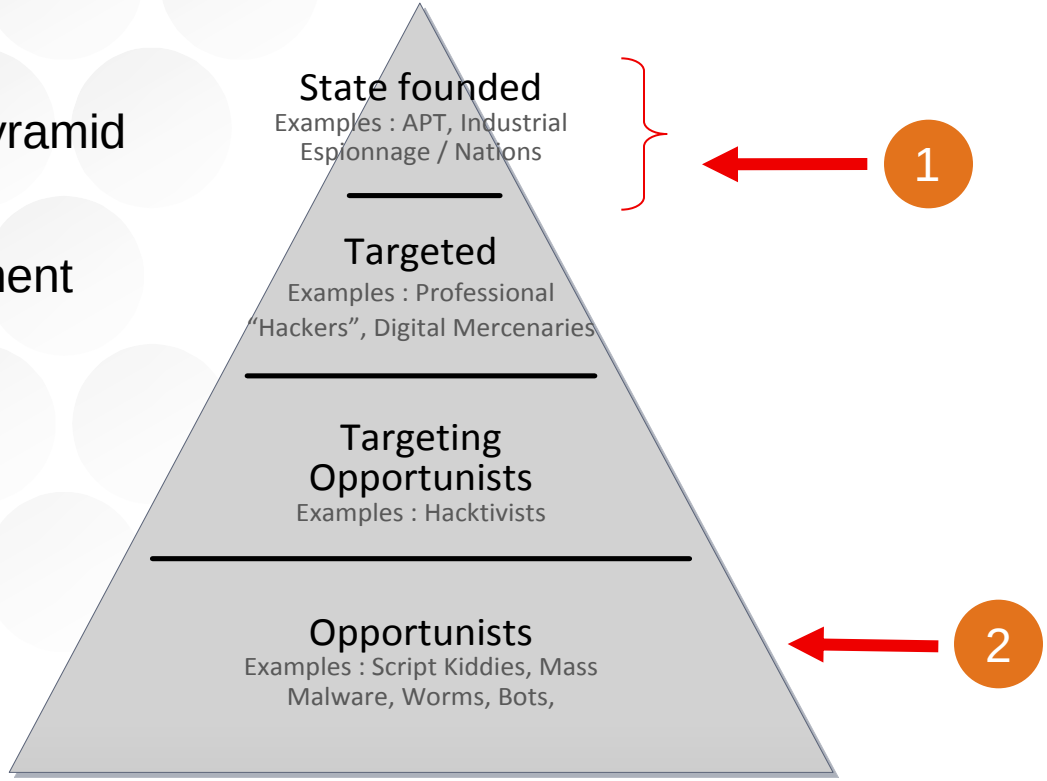
- **Weaponised Exploit**
  - “ A program that has been developed to deliver a particular payload suited for a particular range of target “ (Stuxnet, Custom Payloads)

Quick Recap 2000-2011

- **Quick Recap 2000-2011**
- **Mass Malware Market**
  - Exploit Kits, Botnets
  - Identity Theft, Banking Theft
  - “Pay to Install” schemes
- **Commercial Vulnerability Market Emerged**
  - Core Impact, Canvas
  - Secunia, Vupen, iDefense, Securiteam
- **Targeted Attacks on the rise**
  - Stuxnet, RSA Secureid, Northrop, Duqu (etc.)
  - Multiple zero days, highly targeted nature points to a sophisticated state founded attacker
- **Hacktivists**

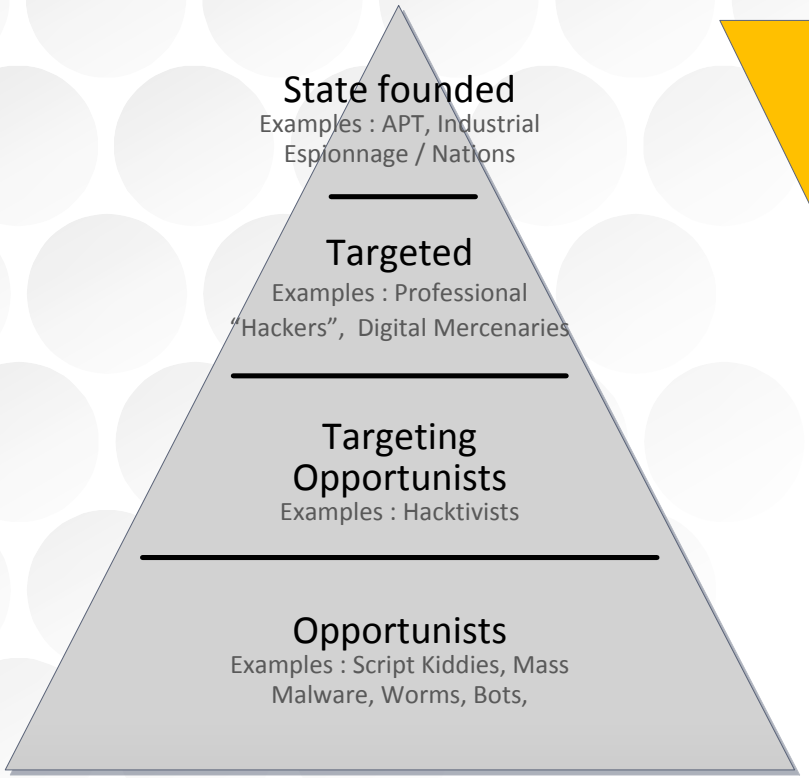
Attacker Classes and Model

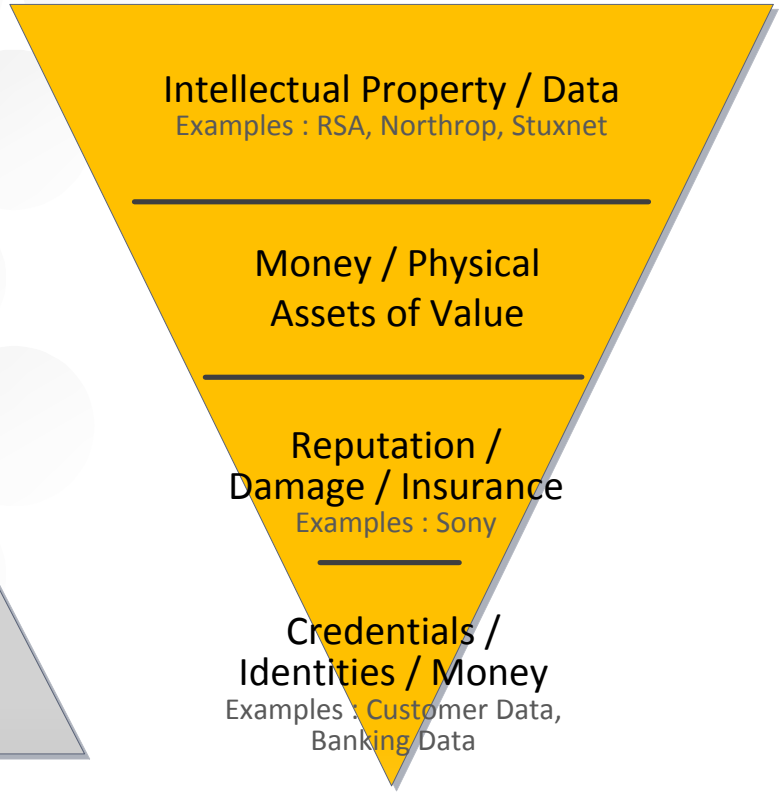
- **The premise for this talk**
- Attacker Classes / Attacker Pyramid
- Concentrate on 2 most prominent classes for this talk



Name → Attacker Class
Surface Area → Amount

Attacker Classes and Model

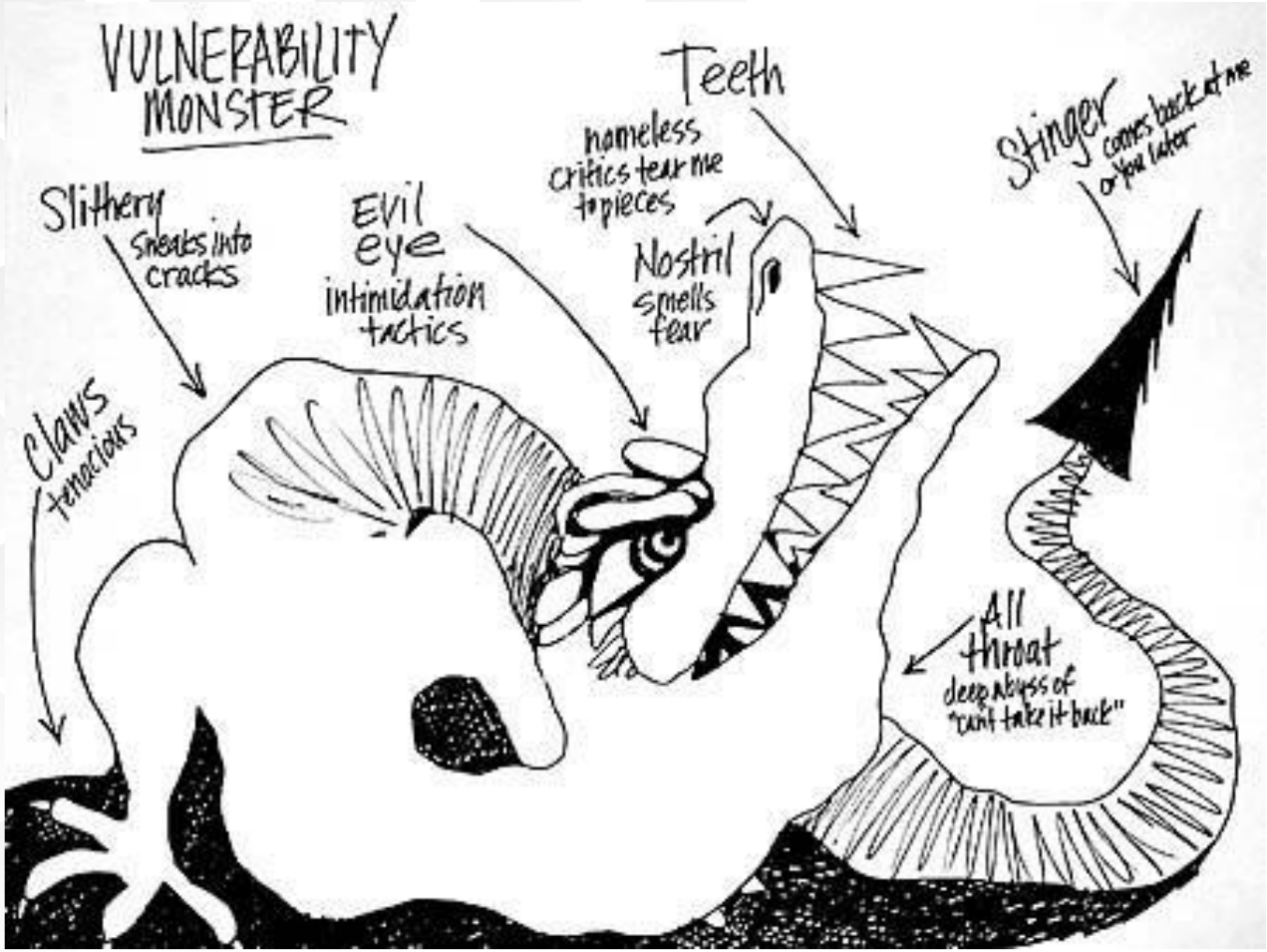




Name → Attacker Class
Surface Area → Amount

Name -> Business Asset
Surface Area -> Value to the Business

Evolution of the Vulnerability Markets



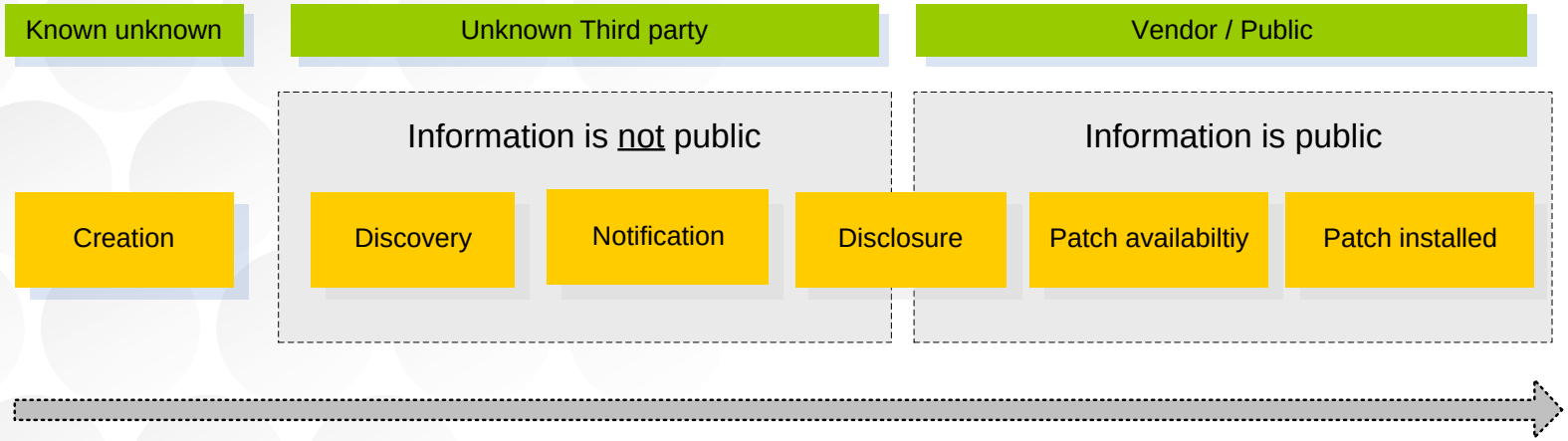
Source: Melanie Weidner

Evolution of the Vulnerability Markets

- **How did those 4 classes emerge ?**
- **Introduction to the Vulnerability Lifecycle**
  - Introduction
  - The evolution of the “Market”
  - The Split
  - Follow the money
- **Examples**

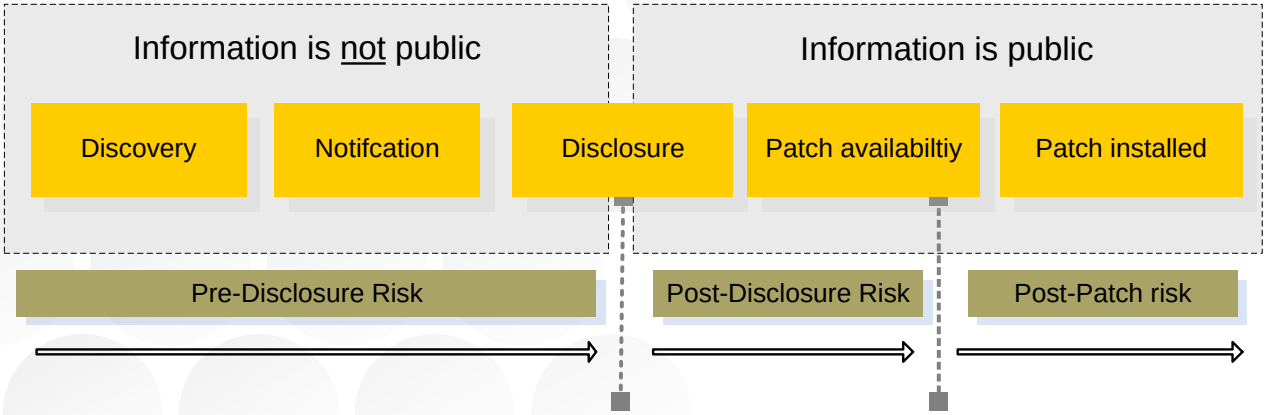
Vulnerability Lifecycle

- **Standard Vulnerability Lifecycle**



Inspired by: Frei, Plattner, Trammel

Risk Phases in Vulnerability Lifecycle



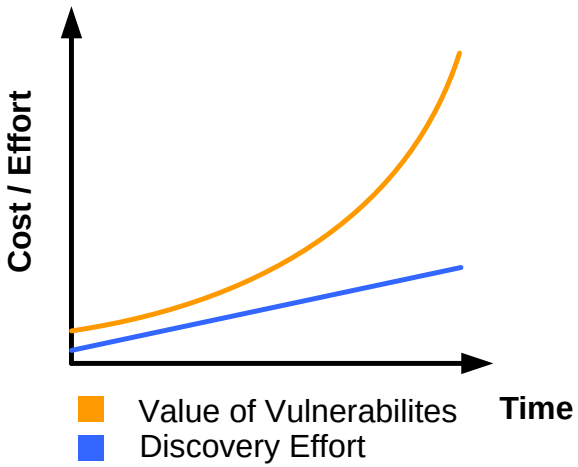
- **Pre-Disclosure Risk**
  - Possibility of **re-discovery/cross discovery** (by malicious entity)
  - Known unknown - Customers at Risk / Vendor at Risk
- **Post-Disclosure Risk**
  - Possibility that vendor silently fixes the vulnerability
  - Possibility of re-discovery
  - Customer at risk (not aware of any vulnerability, hence any risk)
- **Post-Patch Risk**
  - Time Window between awareness and patch deployment
  - Faulty patch

" For the three years between 2002 & 2004, at least [..] 8.47% of credited vulnerabilities were found to have been **independently rediscovered** during the relatively short time frame in which Microsoft worked on a patch."

Source: University of Cambridge

The shift to Vulnerability Markets

- **Quick Summary :**
  - It takes time, effort and knowledge to find security issues in commercial products
    → It is most often not something you just stumble upon. (“Oh look there we have a vulnerability”)
  - Vendors often demand proof that the bug is indeed a security vulnerability or fix it silently (or not at all)
    → Depending on the bug class that alone can take **days or entire weeks**
  - Enterprises are more and more dependant on IT Systems
  - Value of assets and data increased
  - Value of vulnerabilities increased in parallel
  - There is an **imbalance** between the **effort of the work** by the “discoverer” **vs. the value** of the vulnerability



* Totally non scientific graph..

- Market theory suggests that demand and offer automatically create an equilibrium in unbalanced Ecosystems.
  → **No different for this particular market / ecosystem**

The shift to Vulnerability Markets

The inevitable happened :

- **The early days (95-2004)**
  - Exploits circulated underground (Private)
  - Often driven by ego and skill
  - Leaked very often mostly used for private enjoyment

```
/*
 * (c) 2000 venglin / b0f
 * WUFTPD 2.6.0 REMOTE ROOT EXPLOIT
 * **PRIVATE**DO*NOT*DISTRIBUTE**
 */
```

- **Mid 2000 – Commercial**
  - Vendors buy vulnerabilities, coordinate and publish
  - iDefense started VPC in 2003
  - Tipping Point ZDI started in 2005

→ Vendors are informed, <u>there is pubic disclosure</u> and there is a patch

“ Between 2003 and 2007 7.5% of vulnerabilities affecting Microsoft and Apple were processed by ZDI or VPC “

Time

- **Late 2000 – “Black Market”**
  - Trade of Vulnerabilities
  - Government entities buy unknown vulnerabilities
    - Often must be in weaponised state
  - Sometimes they popup (Stuxnet)
  - This market is not a myth it exists and flourishes

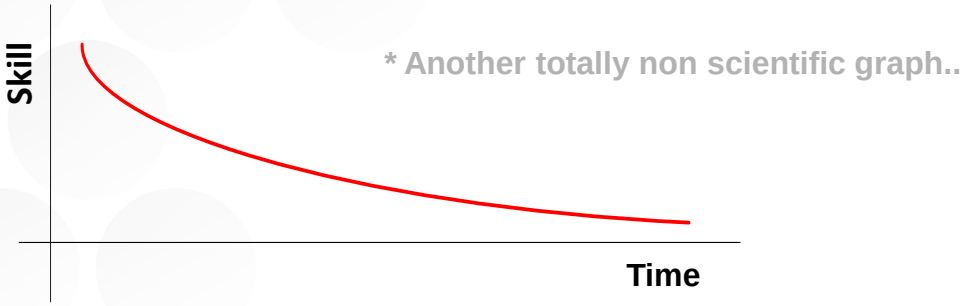
“ ? “

→ Vendors are not informed, the public is not informed, there is no patch

The shift to Vulnerability Markets

- **Today**
  - Companies offer access to exploit code for known vulnerabilities (Exploit Hub, Vupen, Secunia ..)
  - Companies offer access to root cause analysis of vulnerabilities (Secunia, Vupen, ..
  - Commercial exploit frameworks (Canvas, Core Impact, Exploit Packs)
  - Specialised companies produce Weaponised exploits by brokering and augmenting vulnerabilities they buy from “researchers”
  - Non transparent Market of unknown/unpatched vulnerabilities

- **Conclusion :**
  - Importance of SKILL as a factor to measure attacker sophistication decreased :



* Another totally non scientific graph..

  - Factors that increased in importance : Motivation, Funding and hence sophistication

The shift to Vulnerability Markets

- **Vupen offer - Credits actually equals cash**

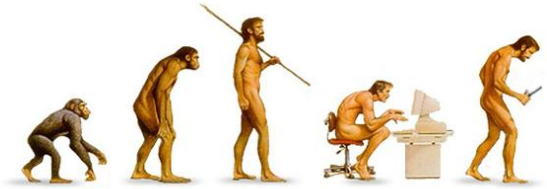
Threat Protection Levels

Basic Level	Enhanced Level	Comprehensive Level
• 30 credits[1] • Brief technical description • In-depth technical analysis • Workaround / mitigation[2]	• 40 credits[1] • Brief technical description • In-depth technical analysis • Workaround / mitigation[2] • Proof-of-concept (crash only)	• 50 credits[1] • Brief technical description • In-depth technical analysis • Workaround / mitigation[2] • Proof-of-concept (crash only) • Code execution exploit[2] • Attack Detection guidance[2]

(1) each research report costs 1 or 2 credits depending on the nature of the vulnerability
(2) when available

The split

Evolution



1

State founded
Examples : APT, Industrial Espionnage / Nations

Targeted
Examples : Professional Hackers
Digital Mercenaries

Targeting Opportunists
Examples : Anonymous

Opportunists
Examples : Script Kiddies, Mass Malware, Worms, Bots,

Name → Attacker Class
Surface Area → Amount

Intellectual Property / Data
Examples : RSA, Northrop, Stuxnet

Money / Physical Assets of Value

Reputation / Damage / Insurance
Examples : Sony

Credentials / Identities / Money
Examples : Customer Data, Banking Data

Name -> Business Asset
Surface Area -> Value to the Business

State founded
Examples : APT, Industrial Espionnage / Nations

Targeted
Examples : Professional Hackers
Digital Mercenaries

Targeting Opportunists
Examples : Anonymous

Opportunists
Examples : Script Kiddies, Mass Malware, Worms, Bots,

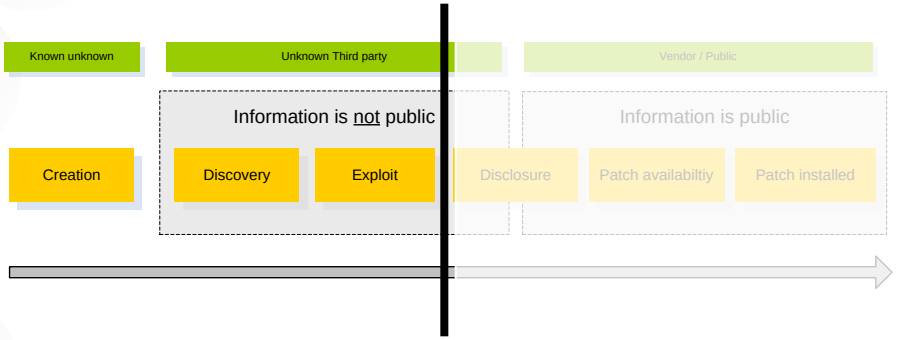
Name → Attacker Class
Surface Area → Amount

2

1 - State founded

- **Example: Government Agency**
  - Discovery
  - Details of flaw submitted to middle-man
  - Middle-Man submits to review to XYZ
  - Middle-Man comes back with price proposal
  - **Formal contract** is signed
  - Exploit is fine-tuned
  - Delivery of exploit + payload
  - 30 MD buffer (reduces risk for middle-man)
  - Money transferred

- **Middle Man reduces risk for end buyer. Who can often not directly buy from foreign or other wise non trusted sources.**



Public Log (Source: Charlie Miller)

Date	Action
6/05	Vulnerability discovered.
11/07/05	Submitted to prepub review at NSA.
7/27/06	Approved for release by prepub review.
7/27/06	Offered to government.
8/10/06	Verbally agreed to $80K conditional deal.
8/11/06	Exploit given for evaluation.
8/25/06	Hash of exploit published.
8/28/06	Agreed to lesser amount.
9/8/06	Paid.

1

1 - State founded

Value – How is value being determined ?

- This slide had an Form used to estimate value by a certain company.

This slide is intentionally left blank

1 - State founded

Summary : How is value being determined

- Popularity of OS and Application
- Reliability of Exploit
- Complexity of Access (Remote, Local)
- Privilege Level obtained (root, admin, user) / Integrity Level gained
- Sandbox bypass and exploit mitigation bypass capability
- Tactical or Strategical Operations planned or ongoing (“Operations” as in Military speak)

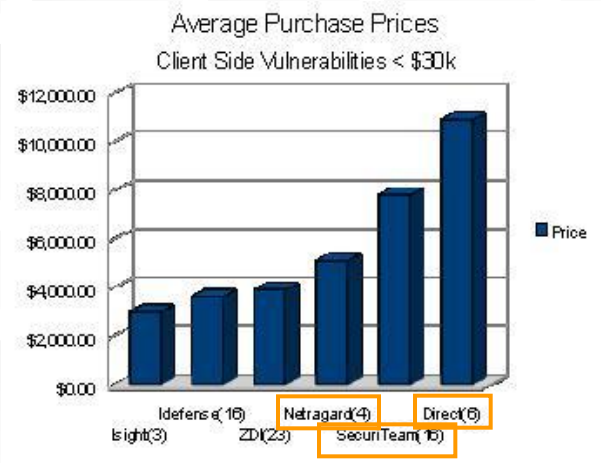
- Special cases likely dealt with on a case by case basis
  - (“We need an exploit for XYZ for Operation “Stuxnet” now..”)

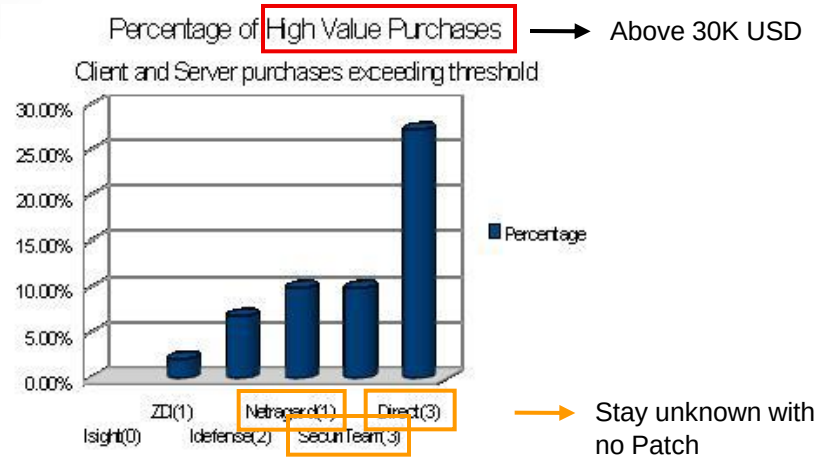
1 - The shift of Vulnerability Markets

Prices – What prices are being paid ?

- **Who pays the most :**
  1. Governments (Direct Buyer)
  2. Commercial (ZDI, VPC..)
  3. Organised Crime

- **Survey based on input of 25 vulnerability <u>sellers :</u>**





Source: unifysecurityresearch survey (based upon 25 vulnerability sellers) – Analysis by Jason Steer

1 - The shift of Vulnerability Markets

Prices – More Data

- Probably unreliable Dataset :

Vulnerability/Exploit	Value	Source
“Some exploits”	$200,000 - $250,000	Gov’t official referring to what ”some people” pay
Significant, reliable exploit	$125,000	Adriel Desautels, SNOSoft
Internet Explorer	$60,000 - $120,000	H.D. Moore
Vista exploit	$50,000	Raimund Genes, Trend Micro
“Weaponized exploit”	$20,000-$30,000	David Maynor, SecureWorks
ZDI, iDefense purchases	$2,000-$10,000	David Maynor, SecureWorks
WMF exploit	$4000	Alexander Gostev, Kaspersky
Microsoft Excel	$1200	Ebay auction site
Vendors offer :		
Google	up to $3177	Google bug bounty program
Facebook	up to $1000	Facebook bug bounty program
Mozilla	$500	Mozilla bug bounty program
Microsoft	**0$**	

Data Source: Charlie Miller + small parts Zoller

1 - The shift of Vulnerability Markets

Not to be published

Intelligence Feedback

- This slide included examples of zero-day vulnerabilities for which we have strong evidence to suggest that they have been sold

This slide is intentionally left blank

1 - The shift of Vulnerability Markets

Not to be published

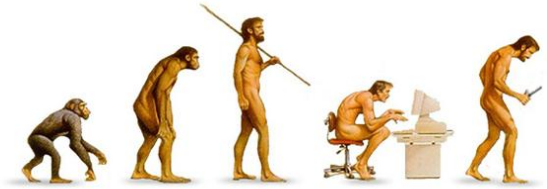
Intelligence Feedback

This slide is intentionally left blank

1 - The Consequences

The split

Evolution



1

State founded
Examples : APT, Industrial Espionnage / Nations

Targeted
Examples : Professional Hackers
Digital Mercenaries

Targeting Opportunists
Examples : Anonymous

Opportunists
Examples : Script Kiddies, Mass Malware, Worms, Bots,

Name → Attacker Class
Surface Area → Amount

Intellectual Property / Data
Examples : RSA, Northrop, Stuxnet

Money / Physical Assets of Value

Reputation / Damage / Insurance
Examples : Sony

Credentials / Identities / Money
Examples : Customer Data, Banking Data

Name -> Business Asset
Surface Area -> Value to the Business

State founded
Examples : APT, Industrial Espionnage / Nations

Targeted
Examples : Professional Hackers
Digital Mercenaries

Targeting Opportunists
Examples : Anonymous

Opportunists
Examples : Script Kiddies, Mass Malware, Worms, Bots,

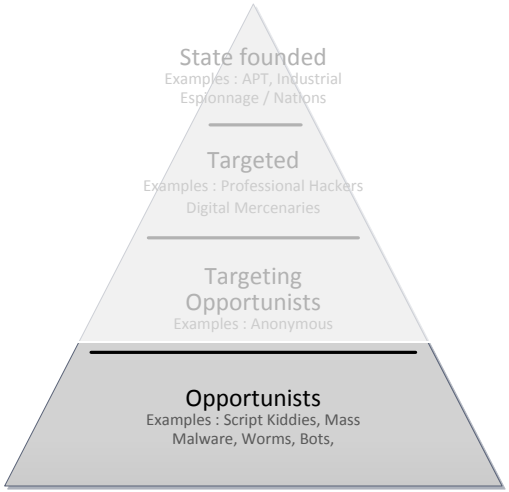
Name → Attacker Class
Surface Area → Amount

2

2 - Mass Market

- **Example: Organised Crime**
  - Interested in the Mass
    - Mass infection, Mass theft of Credentials
    - Increases the likelihood that an exploit works
  - Rarely buy 0day, but pick up that is left behind
    - Increase chances of compromise through mass distribution
  - Interested in compromising lot of hosts
  - Create Botnets / Infect Hosts

  - Spam
  - Steal identities and money
  - Steal banking credentials

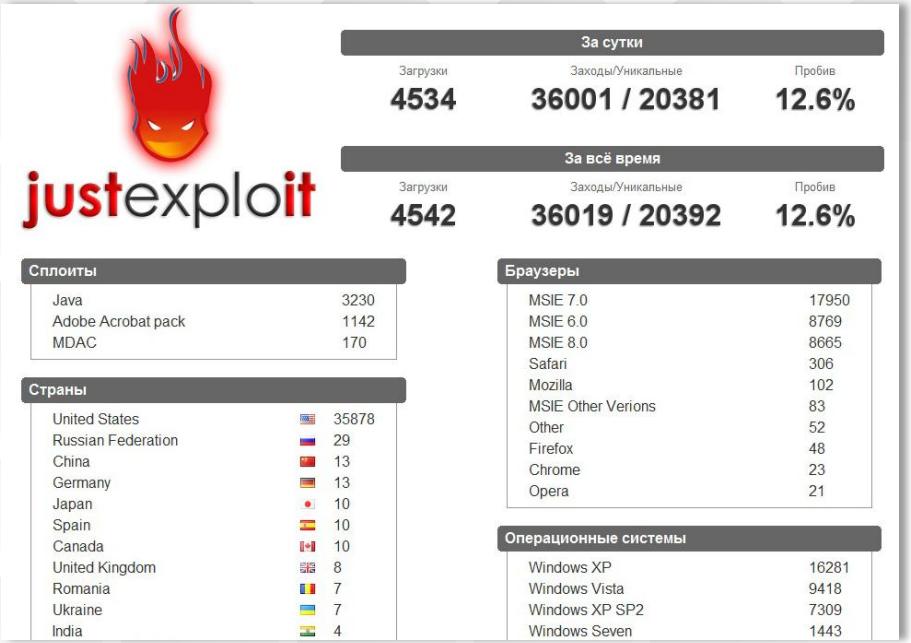


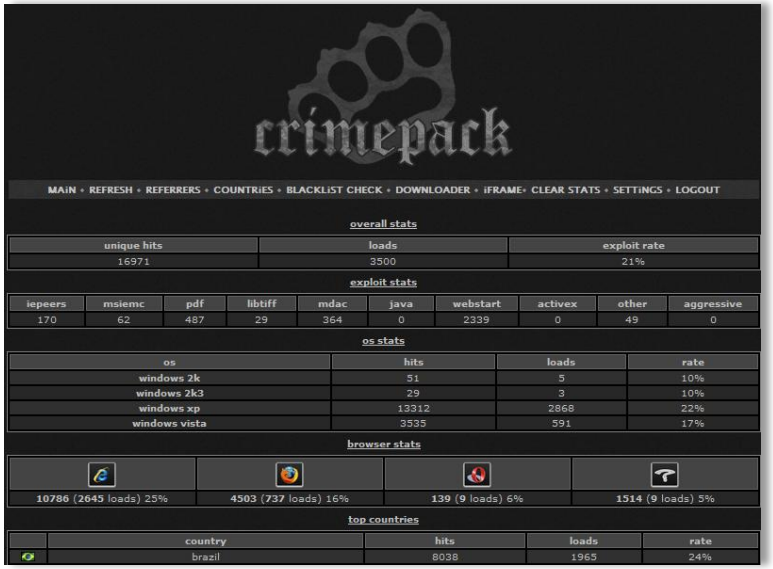
Name → Attacker Class
Surface Area → Amount

2

  - Data shows that they are Opportunists (They are after the Mass)

2 – Mass Market





2 - Mass Market

- Total number of Vulnerabilities (2010, Est.)

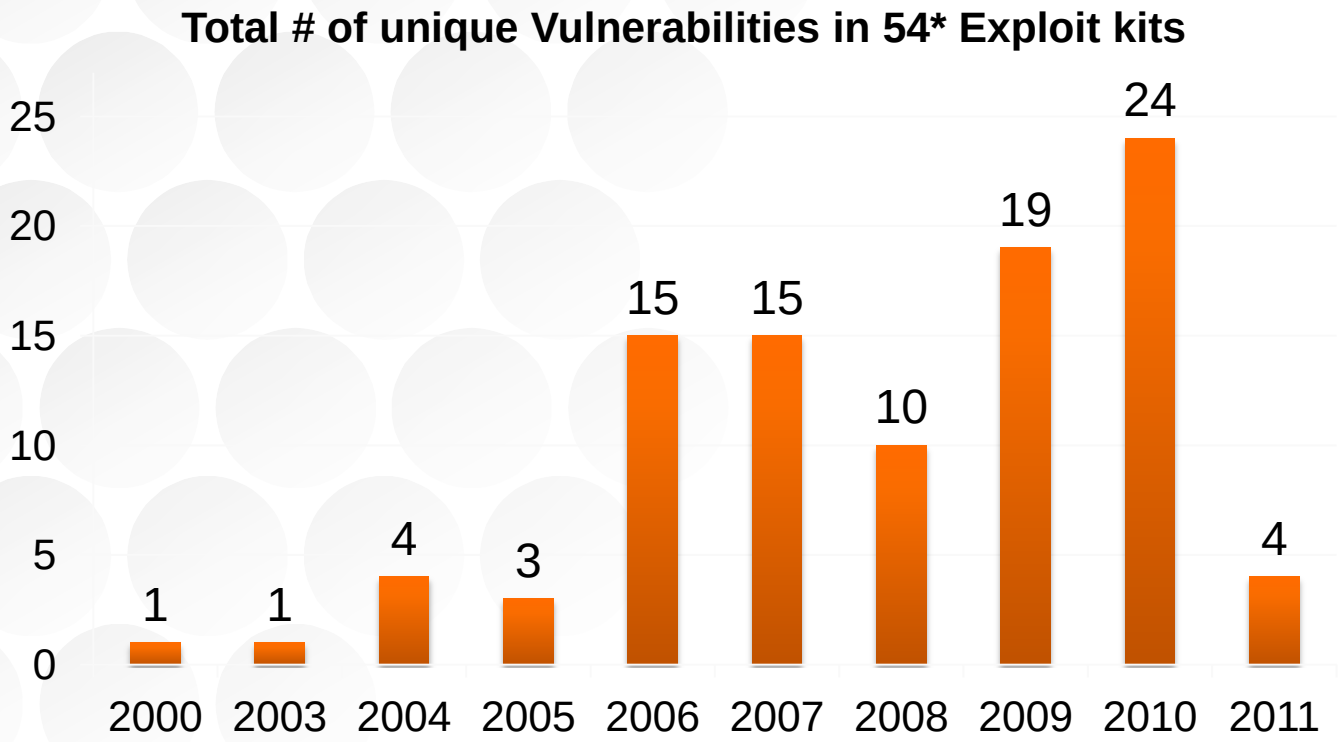
6300+

- To avoid Mass malware like “SpyEye, Zeus, Gozi...” you needed to address the following amount of Vulnerabilities :

19	24	4
2009	2010	2011

Raw data source: Contagio
Analysis inspired by Dan Guido

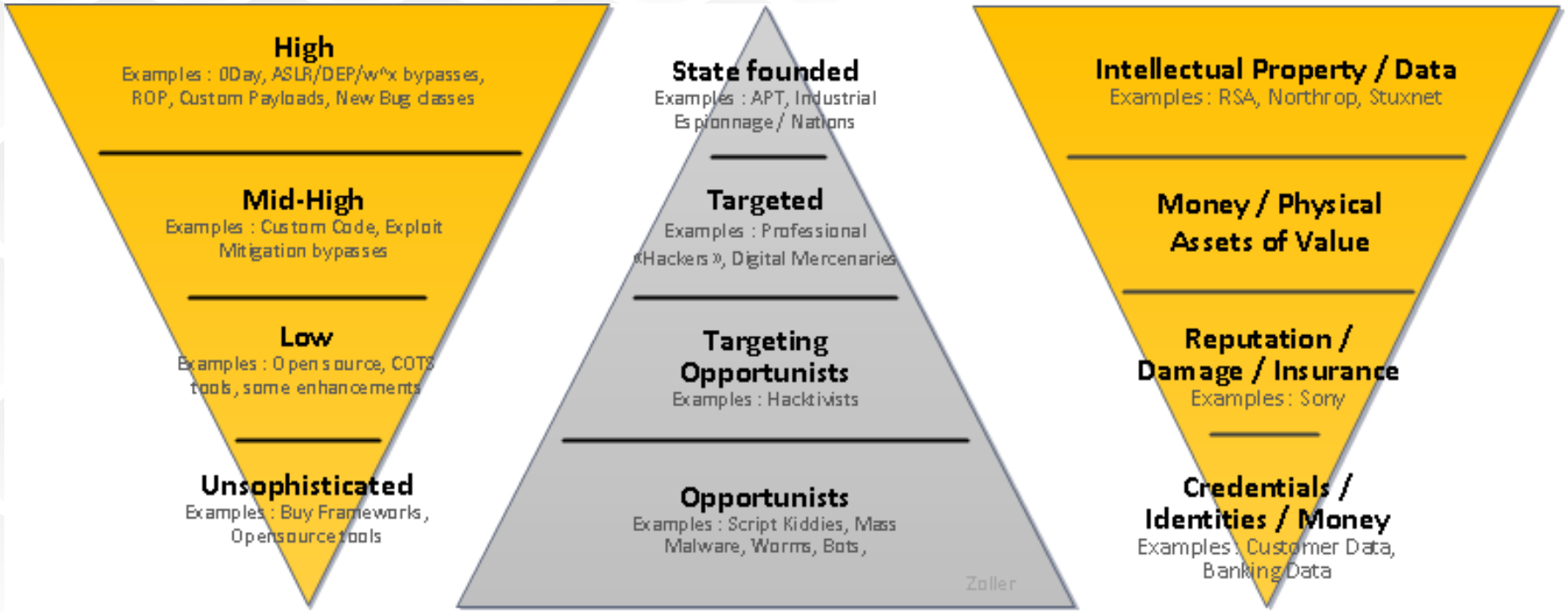
2 - Mass Market



Raw Data source: Contagio
* includes different versions

Summary

We can conclude that, there are differences in motivations, sophistication and typical targets groups:



Motivation / Sophistication / Funding

Name → Attacker Class
Surface Area → Amount

Name -> Typical Targeted Asset
Surface Area -> Value

The implications

- We may not like it, yet we have to face the fact the threat landscape has changed and this poses a concern for those that have to defend against it.

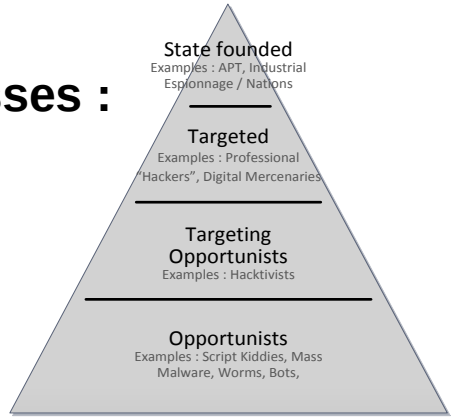
- “Penetrate and Patch” is not adequate (it has never been)

- **Defenses must be :**
  - Designed and built around the assumption that they fail (Sandbox, Exploit mitigation)
  - Built around the concept of “Reduced attack surface”
  - Have multiple layers of generic defence mechanisms (sandboxes)
    - Limit the impact of vulnerabilities
    - Reduce the likelihood of successful exploitation
    - Raise the bar (more effort required)
  - Work generically and not as a one time fix (patch)

Mitigations / Consequences

- **Adapt you Governance approach to the new Threat Landscape**
  - One option: An Attacker Centric Model

- **Create a Model around different Threat Agents and Classes :**
  - Decide on which classes of Attackers you want to protect an Asset against (Business Value, using as example the Attacker Pyramid)
  - Adapt **Audit requirements** (Assurance Concept) and **Development requirements** (SDLC) to the level above
  - Adapt Framework to the changes
    - Contractually enforce SDLC when in-sourcing s oftware development

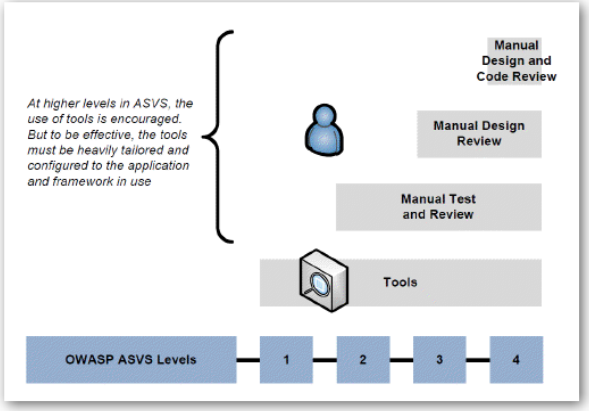


Name → Attacker Class
Surface Area → Amount

- Benefits : Less money "wasted" on assets of low value, more flexibility, better time to market.
- Benefits : Higher Assurance on Assets that are worth protecting
- **This is in line with ISO/IEC 27034-1:2011**

Mitigations / Consequences

- **Example : OWASP Application Security Verification Standard**
  - 4 Verification Levels, released in 2009
  - Currently appears to have a low adoption rate
  - We strongly recommend to look into it



  - Depending on the Verification Level the Scope, Requirements and controls change according to the targeted Verification Level
    - Uses a “Positive” approach to verification
    - Exhaustive list of controls to check for on each level
    - Allows for remediation plans to meet Verification Standard after initial test
      - Quick retesting possible
    - Detailed Reporting Guidelines

https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project

Mitigations / Consequences

- **Attacker centric risk management**
  - May revolve around the concept of **Assurance Level**
  - Depending on the Level of Assurance against a certain type of attacker, a different set of requirements, controls and scope are required to be covered.
  - Let's face it - there is no assurance in an automated Web application Scan, and there is only some assurance in a manual Web application Test.
  - Benefits :
    - Budget assurance at an early stage
    - Suitable Level of Assurance per Application
    - Permits Risk based management on Applications/Architectures
    - Mature way of Assessing Security of Applications

Mitigations / Consequences

Example only

- **For Web Applications, the concept could look like :**

Techniques

Assurance Level 1

Automated

Manual (Verification of Automated findings only)

Assurance Level 2

Manual Inspection

+

Level 1

Assurance Level 3

Source Code Review

Database Audit

+

Level 2

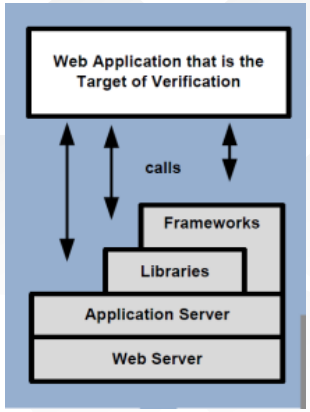
Assurance Level 4

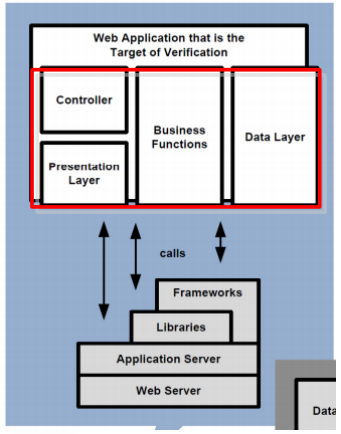
Architectural Review

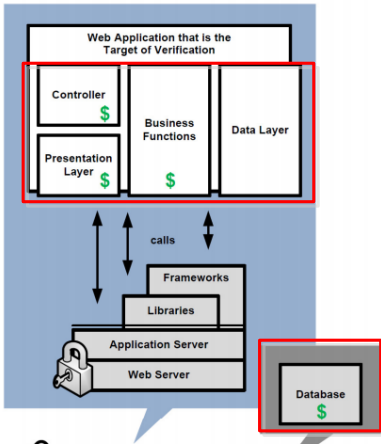
+

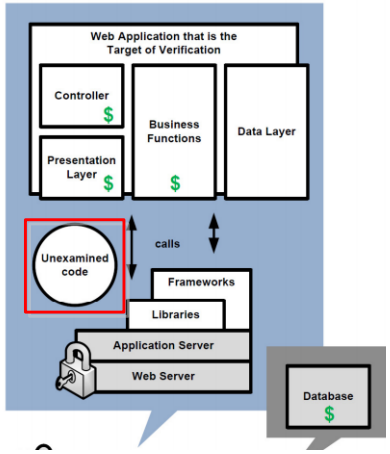
Level 3

Scope









Mitigations / Consequences

Example only

- (cont.)

Techniques

Assurance Level 1	Assurance Level 2	Assurance Level 3	Assurance Level 4
Automated Manual (Verification of Automated findings only)	Manual Inspection + Level 1	Source Code Review Database Audit + Level 2	Architectural Review + Level 3

Scope

Assurance Level 1	Assurance Level 2	Assurance Level 3	Assurance Level 4
Suitable to provide Assurance against : Unsophisticated Opportunistic Attackers Limitations : **Does not cover application Logic**	**Suitable to provide Assurance against :** **Targeting Opportunists** such as attackers with **open source attack tools**.	**Suitable to provide Assurance against :** **Determined attackers** who are skilled and motivated focusing on specific targets including using **purpose-built** attack tools	**Suitable to provide Assurance against :** Determined and Professional Attackers – Potentially State funded Attackers

Thank you for your Attention

altogetherbetter