RSA CONFERENCE
ASIA PACIFIC 2013

UNDERSTANDING AND BUILDING THREAT MODELS

Tas Giakouminakis
Rapid7

Session ID: SEC-T03

Session Classification: Intermediate

Agenda

- Threat Modeling – The Basics
- Understanding Attackers
- Understanding the Organization
- Building Threat Models

Threat Modeling – The Basics

Asset

Software

Attacker

Threat Modeling – Attackers

Attacker Motivation

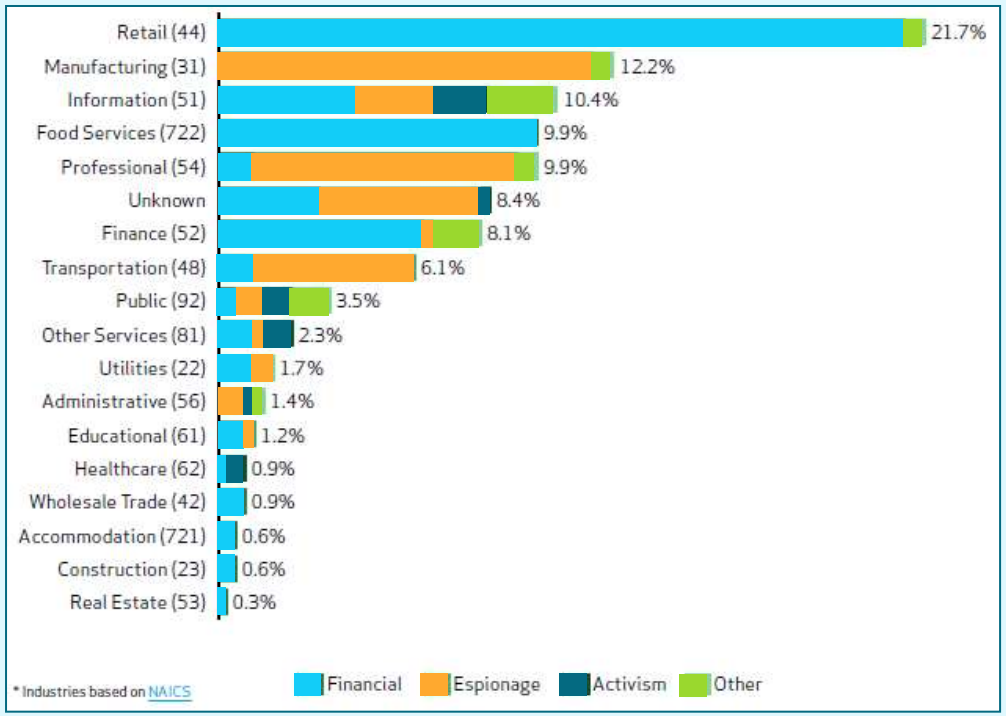
Common Targets

Attack Patterns

Organizational Readiness

Attacker Motivations & Targets

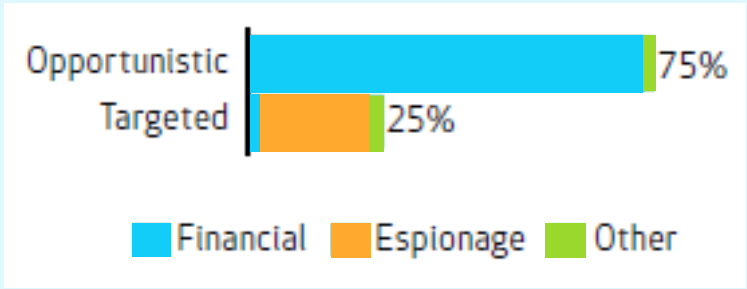
- Assume common threats impact everyone
  - Mass malware
  - “Unintentional” insiders
- Gain insight into industry specific threats
  - ISACs
  - UK CISP
  - US CISPA
  - Vendors



Verizon – 2013 Data Breach Investigations Report

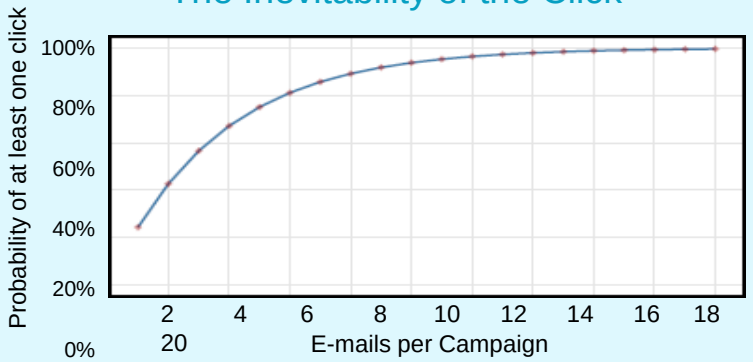
Attack Patterns

Attack Targeting



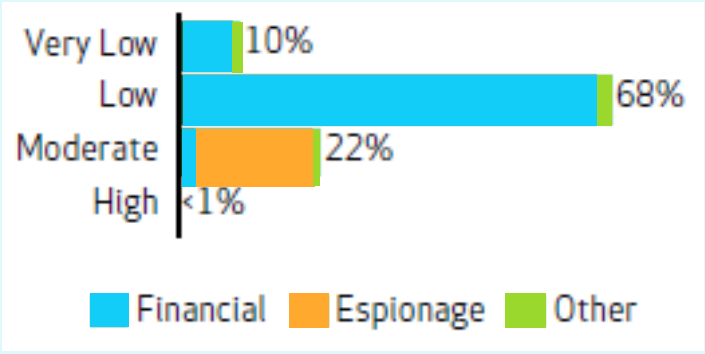
Verizon – 2013 Data Breach Investigations Report

The Inevitability of the Click



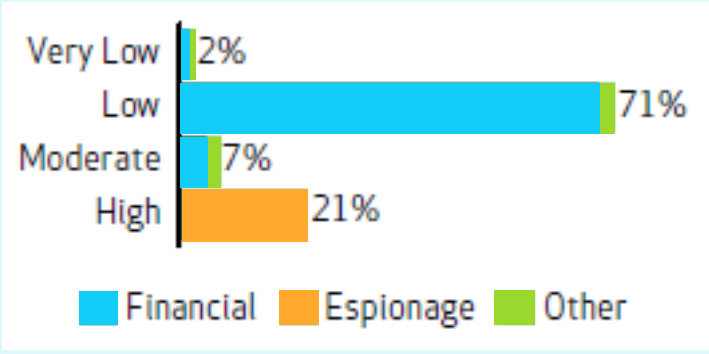
Verizon – 2013 Data Breach Investigations Report & ThreatSim

Difficulty Of Initial Compromise



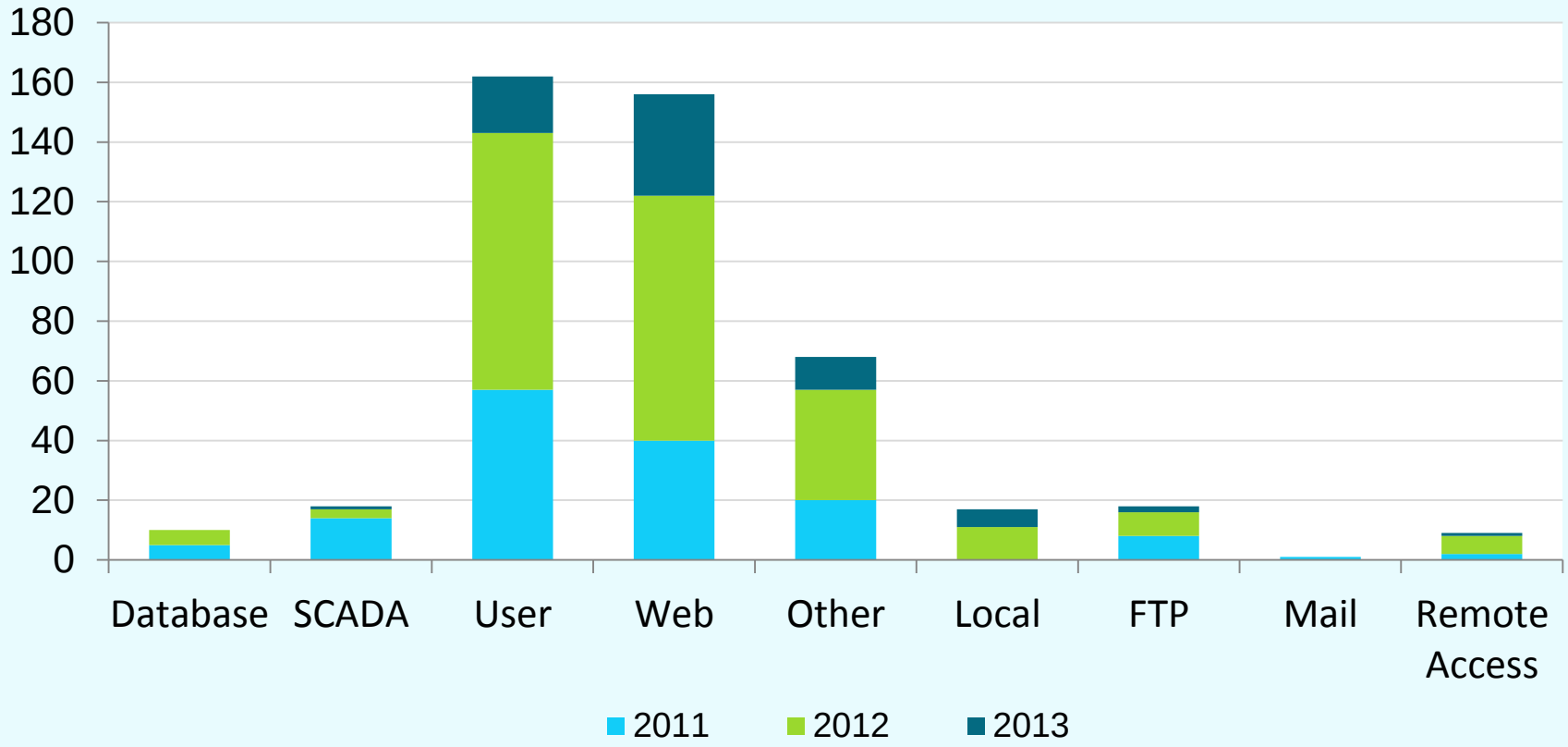
Verizon – 2013 Data Breach Investigations Report

Difficulty Of Subsequent Actions



Verizon – 2013 Data Breach Investigations Report

Public Exploit Targets

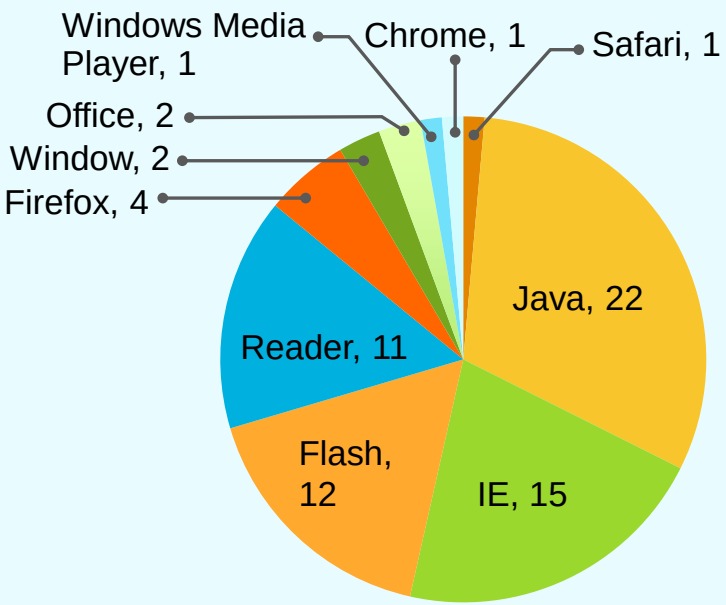


Rapid7 Metasploit Framework Exploit Contributions through May 3, 2013

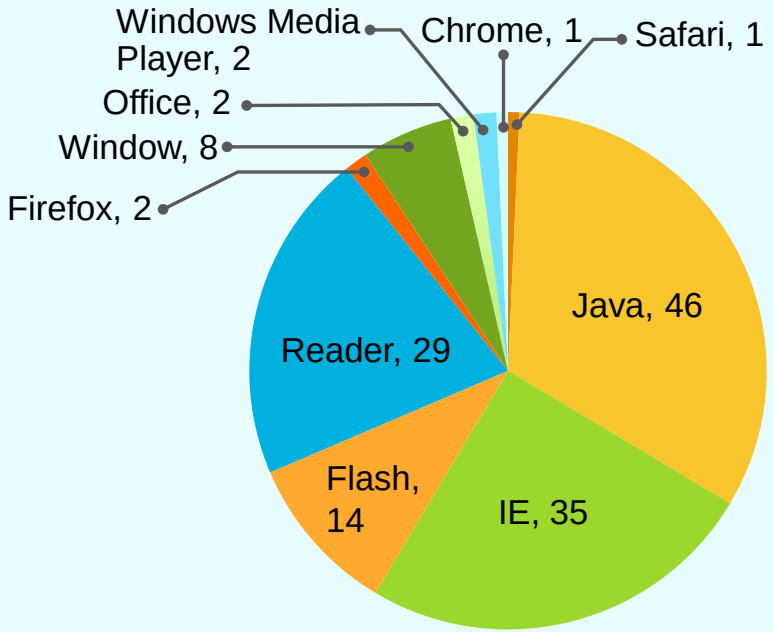
Mass Malware Targets

- Mass malware leverages Exploit (Crime) packs
- 49 Exploit (Crime) Packs Analyzed 2011 - 2013

Unique Vulnerabilities Exploited

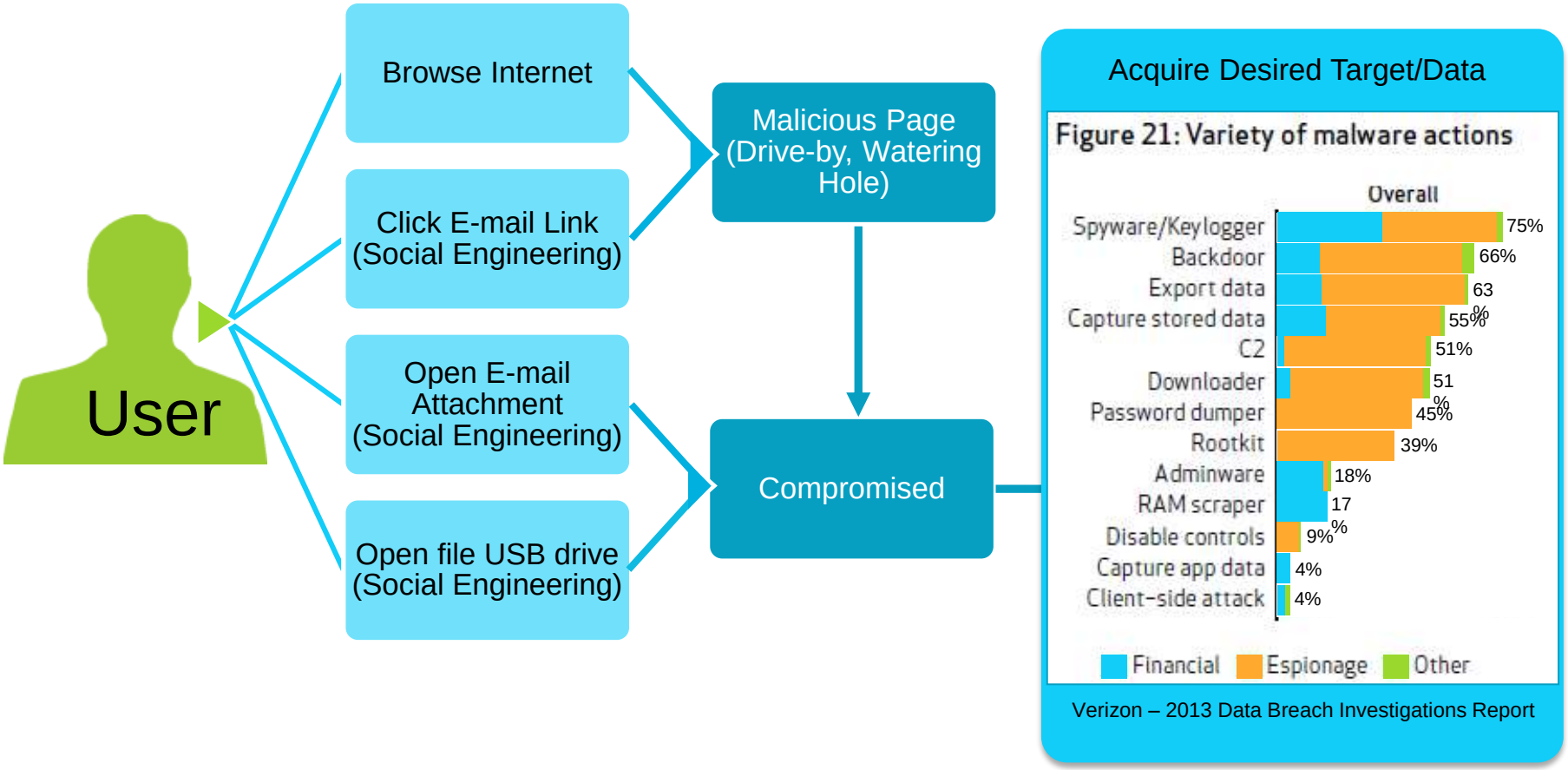


Exploit Packs Per App



Contagio Malware Dump & Exploit Intelligence Project/Dan Guido

User Targeted Attacks



Similarities in Attacks

Social engineering (eg: spear-phishing) common in APT, targeted and mass malware scenarios

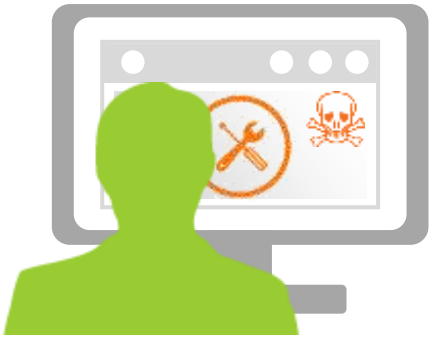
Users will click on links

How do we protect them?

Similarities in Attacks

Malware - Powered by compromised/abused web servers & web applications (eg: SQLi, RFI, brute force)

Drive-by downloads provide high yield for mass malware



Watering holes used in APT and targeted attacks

How do you avoid being part of the delivery network?

Understanding the Organization

Visibility

- Correlate attacker motivations with business functions
  - Look outside as well – who relies upon you?
- Identify potential targets & existing countermeasures
  - Compile complete inventory of users, assets, software, services and security controls across physical, virtual, VPN, wireless, cloud services and mobile
  - Classify assets & data
- Associate users with assets they own or access

Understanding the Organization

Baseline

- Baseline the IT & user environments
  - Review inventory to identify outliers, gaps & appropriateness
- Baseline user behavior
  - Review assets users access or own for appropriateness & access patterns
- Baseline “normal” data flows
- Investigate unknowns & anomalies
- Be prepared for false positives / spurious anomalies

Understanding the Organization

Response

- Business continuity requires effective security response
- Response will vary based on threat / attacker motivation
  - Understanding is key to taking appropriate action
- Staff & train resources accordingly to maximize identification & response capabilities

Taking Action

- Significant progress can be made
- Focus efforts on highest return
  - Increase complexity/cost to the attacker
- Be prepared – easier to contain incidents through planned response than reactive scrambling

Building Threat Models

Let's work through a few examples

Threat 1: Users will click on links

Threat 2: Serving Malware on the web

Threat: Users Will Click on Links

Motivation

All – Opportunistic through APT

Target

All

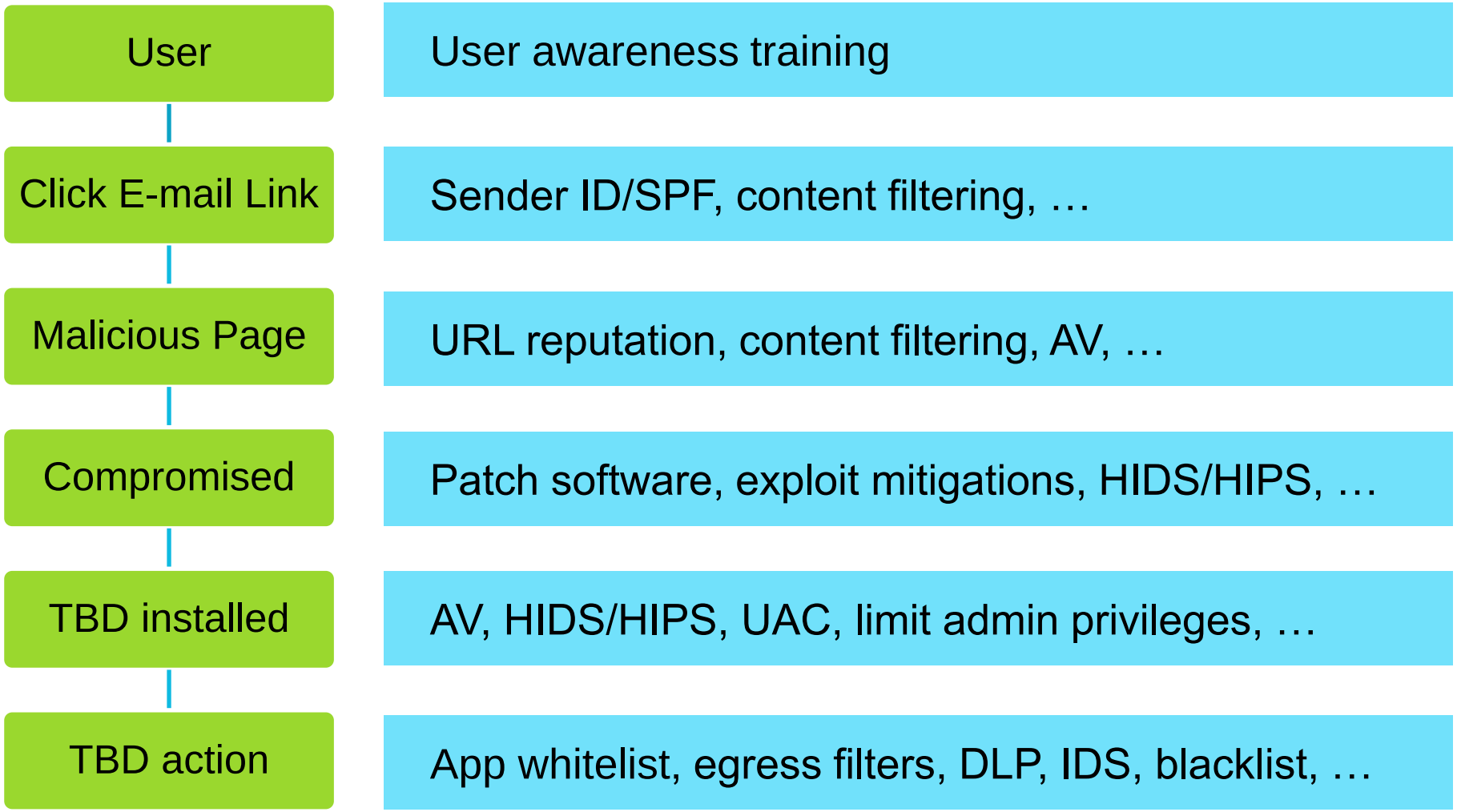
Attack Pattern

E-mail, Malware & Actions

Readiness

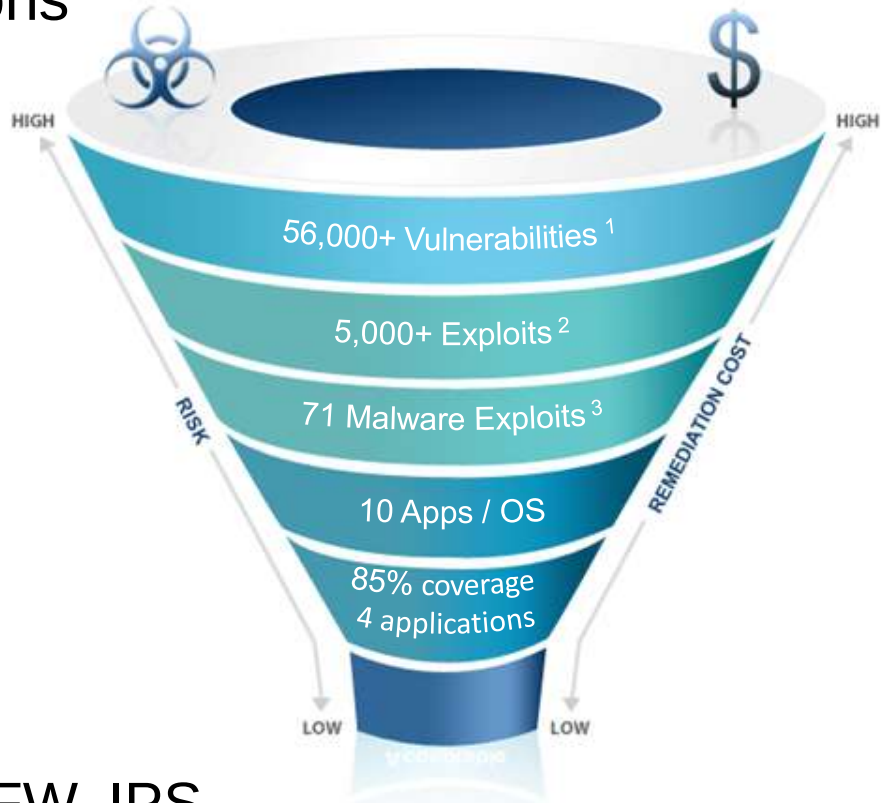
Varies

Analyzing The Threat



Reduce Exploit Exposure

- Automate deployment of software, patches, security controls & configurations
- Remove or patch commonly targeted applications
- Limit administrative privileges, User Account Control (UAC)
- Enable exploit mitigations
  - DEP, ASLR, EMET, SEHOP
- Endpoint security controls
  - Application whitelisting, AV, FW, IPS



1) Source: National Vulnerability Database
2) Source: ExploitDB
3) Source: Contagio Dump, Exploit Packs 2011 - 2013

Control Traffic Flow

- Gain visibility & increase defensive/response capabilities
- Consolidate ingress & egress points – including VPN & Cloud Services
- Perimeter doesn't exist – apply security controls closest to resources
- Centralized & consistent logging for network services and security controls
  - Network services: DNS, FW, VPN, Web, Email, File, Directory, Database
  - Security controls: IDS/IPS, DLP, WAF, Malware Protection, etc

Limit the Temptations

- Rollout user awareness training, tips & advice
- Reduce spear phishing attacks – leverage Sender ID or Sender Policy Framework (SPF)
- Deploy network-based security controls
  - Blacklist, Malware Protection, IDS/IPS, Content Filtering

Practice & Refine

- Automate social engineering campaigns
- Focus on real-world scenarios, not simulations
- Quantify user susceptibility
- Review security response for lessons learned
  - Failed controls, monitors, or people?
  - Appropriate parties in response chain?
  - Timely and accurate response?
- Refine & iterate

Threat: Serving Malware on the Web

Motivation

All – Opportunistic through APT

Target

All

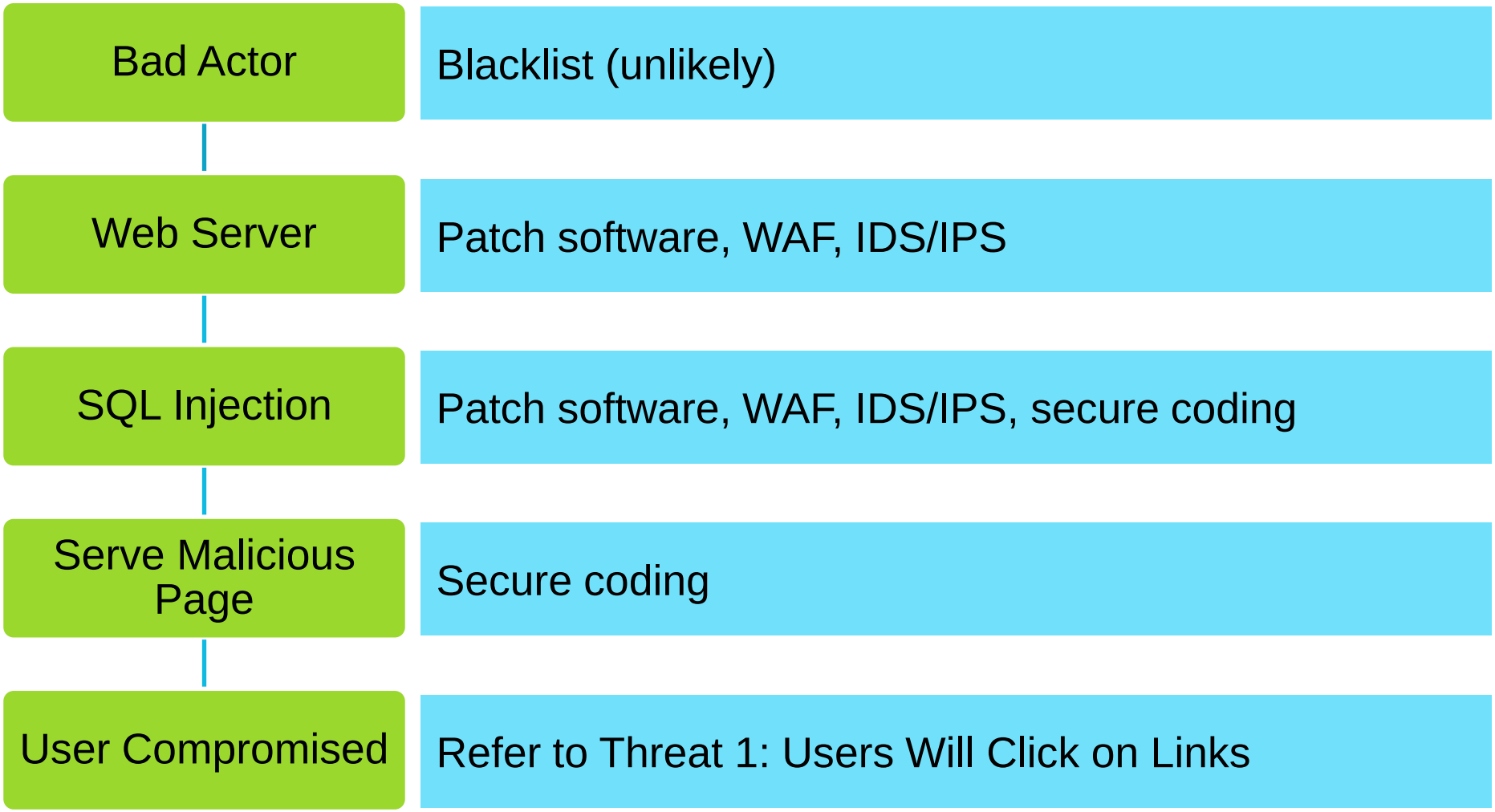
Attack Pattern

Compromise Web Server, Serve Malware

Readiness

Varies

Analyzing The Threat



Reduce Exploit Exposure

- Identify all web servers & applications
  - Perform static and dynamic analysis of web applications
- Train developers on secure coding practices
  - OWASP
  - Don’t forget output validation!
- Deploy security controls: WAF, IDS/IPS
- Automate deployment of software, patches, security controls & configurations

Detecting Compromise

- Centralized & consistent logging for network services and security controls
  - Network services: DNS, FW, VPN, **Web**, Email, File, Directory, **Database**
  - Security controls: **IDS/IPS**, DLP, **WAF**, Malware Protection, etc
- Compare dynamic website analysis against baseline for unexpected links

Practice & Refine

- Perform SQL injection attacks
- Focus on real-world scenarios, not simulations
- Review security response for lessons learned
  - Failed controls, monitors, or people?
  - Appropriate parties in response chain?
  - Timely and accurate response?
- Refine & iterate

Additional Reading – Methodologies

Intel Threat Agent Risk Assessment (TARA)

http://communities.intel.com/docs/DOC-4693

Factor Analysis of Information Risk (FAIR)

https://www2.opengroup.org/ogsys/jsp/publications/PublicationDetails.jsp?publicationid=12239

OCTAVE® (Operationally Critical Threat, Asset, and Vulnerability EvaluationSM)

http://www.cert.org/octave/

NIST Risk Management Framework (RMF)

http://csrc.nist.gov/groups/SMA/fisma/Risk-Management-Framework/index.html

OWASP Threat Risk Modeling

https://www.owasp.org/index.php/Threat_Risk_Modeling

Additional Reading – Related Works

Lockheed Martin Corp. - Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains

http://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf

Dan Guido – Exploit Intelligence Project

http://www.trailofbits.com/resources/exploit_intelligence_project_2_slides.pdf

Dino Dai Zovi – Attacker Math 101

http://www.trailofbits.com/resources/attacker_math_101_slides.pdf

Australian DSD – Strategies to Mitigate Targeted Cyber Intrusions

http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm

SANS/CSIS – Twenty Critical Security Controls for Effective Cyber Defense

http://www.sans.org/critical-security-controls/

Final Thoughts

- Enhance & maintain visibility into your business, your IT environment, your users, & the threats you face
  - Visibility is key to informed decision making
- Continuously refine your hypotheses & approach, adjust course as needed & validate your results
  - Attacks will continue to evolve – repeat this process frequently
  - Focus efforts on highest return – make attackers work harder
- Operationalize & optimize programs & processes to enable efficiency & effectiveness
  - Human resources as well, not just technology

RSA CONFERENCE ASIA PACIFIC 2013

Thank You

Tas Giakouminakis

Rapid7

Co-founder & Chief Technology Officer

www.rapid7.com

tas@rapid7.com