RSA Conference 2016

San Francisco | February 29 – March 4 | Moscone Center

Connect to Protect

SESSION ID: STR-W02

The Three Principles of Effective Advanced Threat Detection

Zulfikar Ramzan

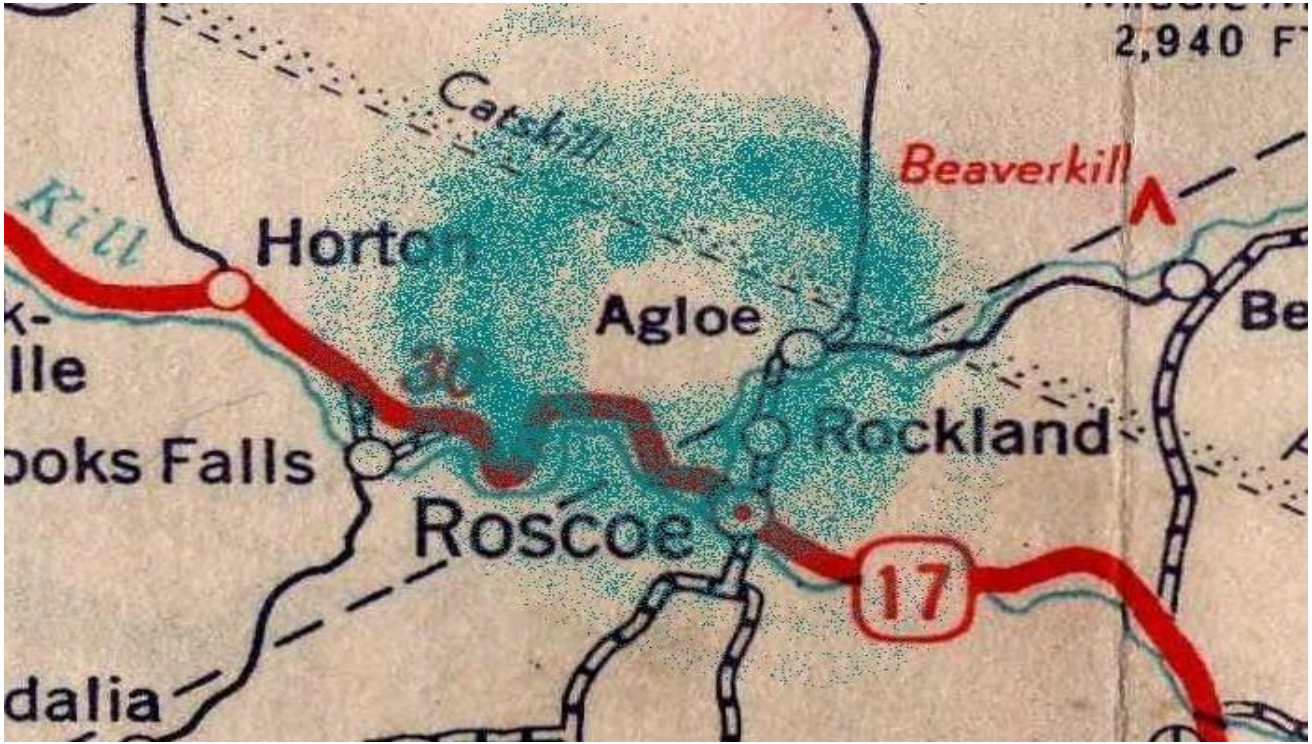
Chief Technology Officer

RSA

@zulfikar_ramzan

#RSAC

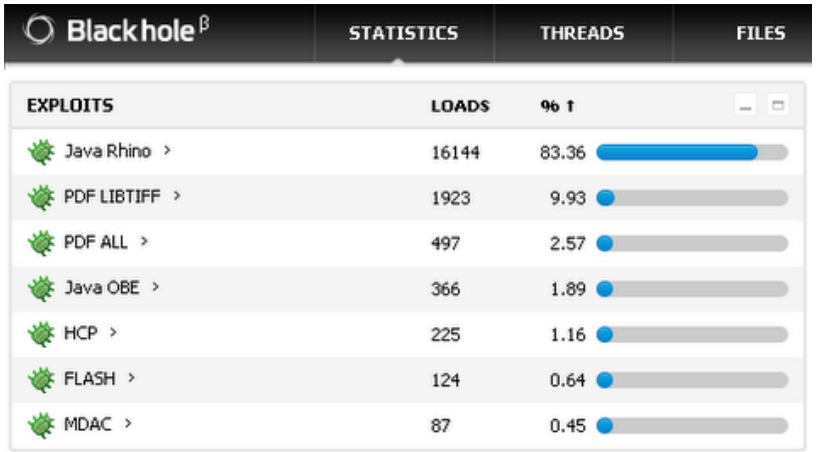
Paper Towns and Cybersecurity



What Came First: the Map or the Town?


Computer crime
Malicious website steals
Fraud eats into
Internet profits

Why Intrusions Are Successful



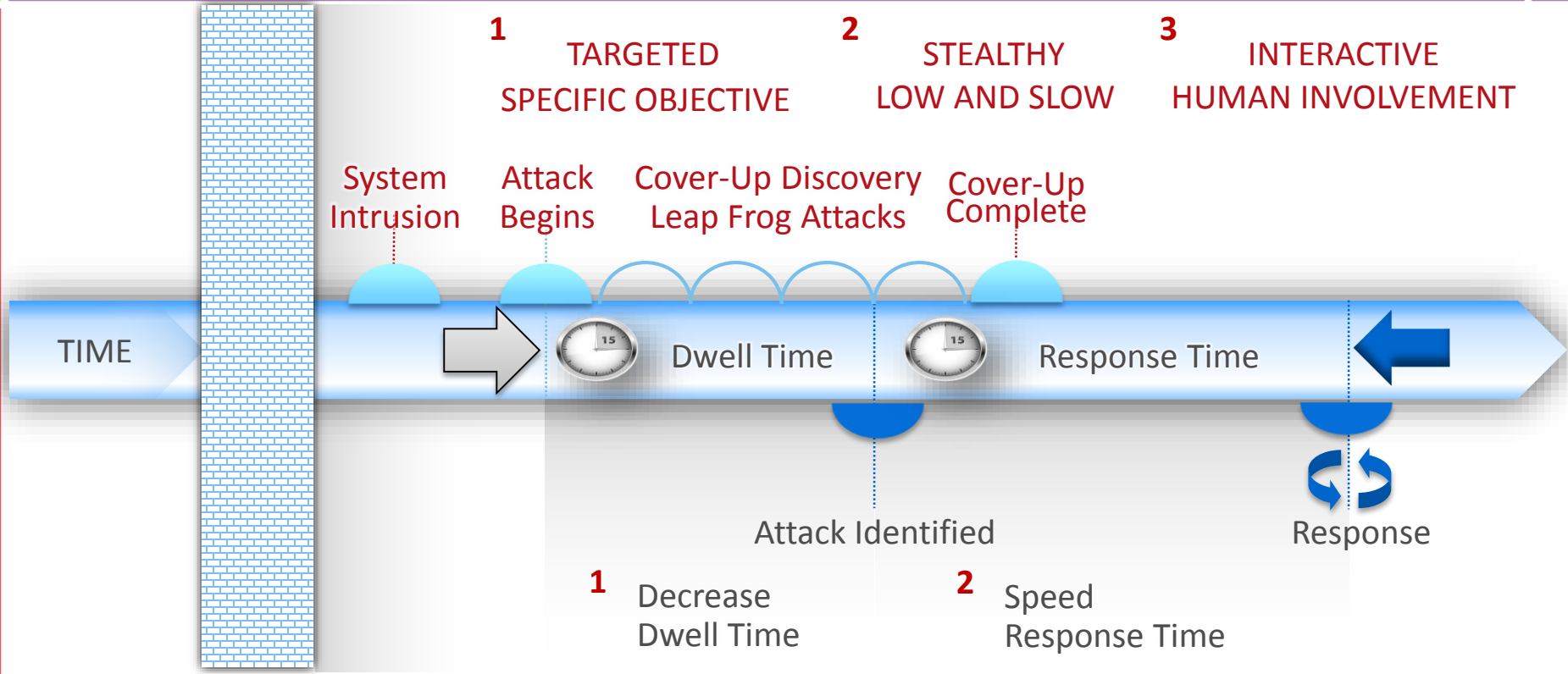
Attacks are targeted (e.g., via repeated use of polymorphism and metamorphism); Macro-distribution supplanted by micro-distribution.

Powerful attack toolkits available w/ tiered pricing, 24x7 customer support. Ecosystem for buying and selling tools and cybercriminal services democratizes advanced attacks

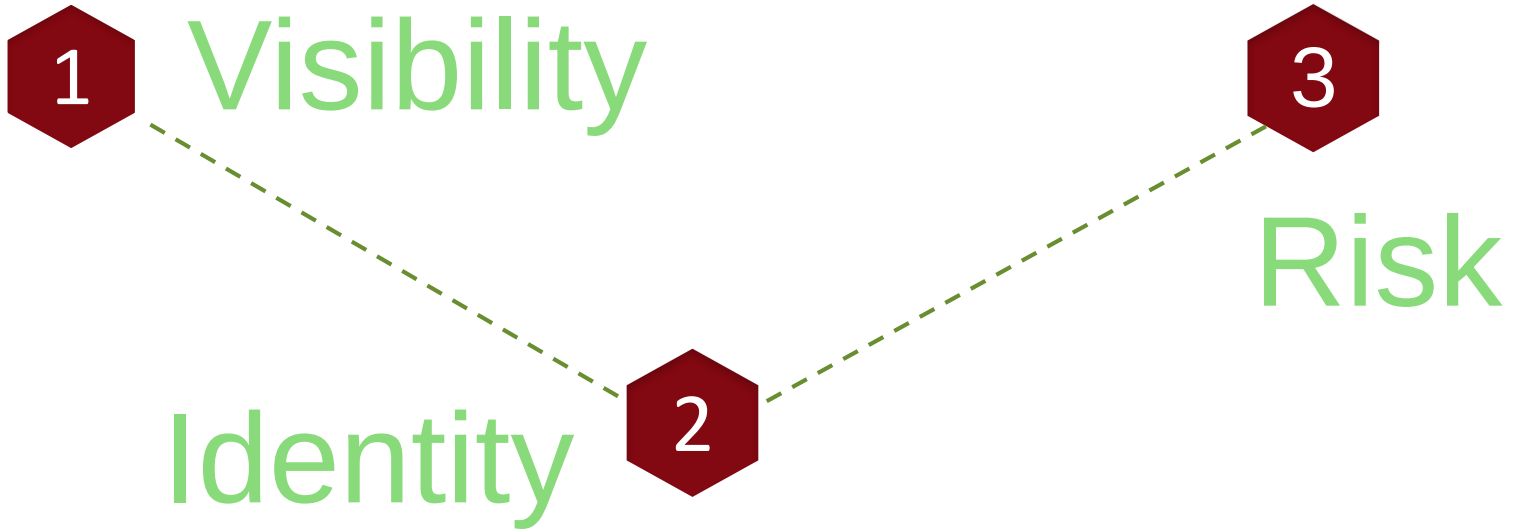
Stages of an Attack

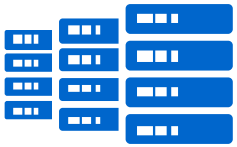
Scanning, Social network analysis	Spear phish, waterhole, web app vuln removable media, CVEs, 0-days	Privilege escalation, finding run keys, modifying scripts	Web shells, dropped secondary malware	Pass the hash, pass the ticket, RDP, CVEs, remote services	One or more hops, drop zones, data destruction / manipulation

Advanced Threats: Where to Focus



Three Strategic Pillars





visibility

is the foundation for mitigating the risk of advanced threats

If you really want to protect your network, you really have to know your network. You have to know the devices, the security technologies, and the things inside it.
-Rob Joyce, NSA TAO Chief, Usenix Enigma 2016

Key Visibility Points

Logs Netflow Packets Endpoints Cloud Identities

is foundational and will matter even more as the threat landscape evolves

Malware Reality Check

Advanced breaches don't have to involve malware: SQL Injection -> Web Shell -> RDP

Advanced breaches can be very simple – e.g., credential theft

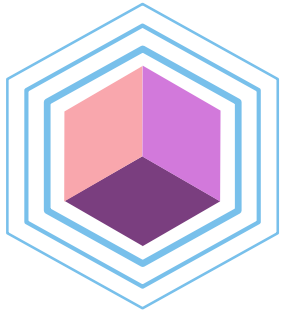
Every breach involves co-opting of identity (authentication isn't the same as identity assurance)

Identity is More Than Authentication

Financial risk

Physical risk

Operational risk



embrace

and **own** your risk

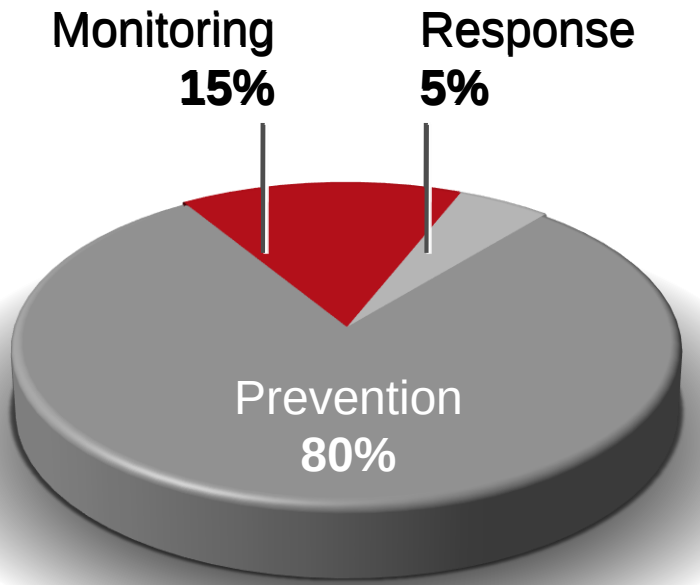
Currency fluctuation risk

IT Security risk

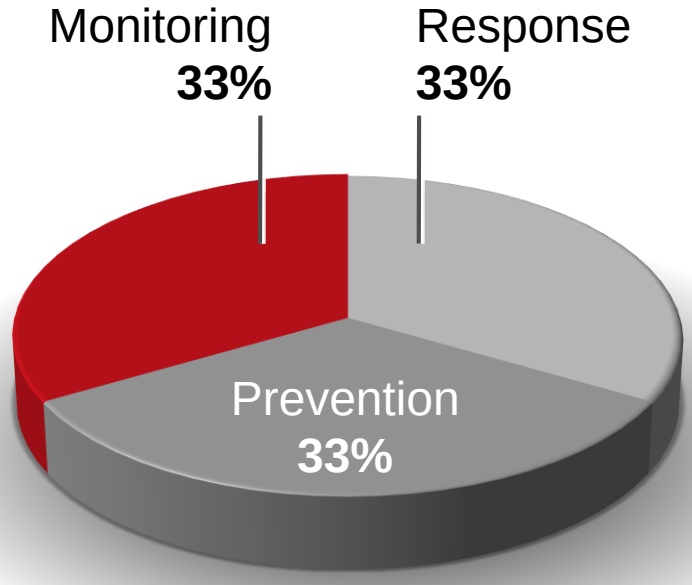
Regulatory risk

Supply chain risk

Shift Priorities and Capabilities



How we spend



How we *should* spend

The Revised Map

Security Operations / Governance, Risk, Compliance

Logs | Netflow | Packets | Endpoint | Cloud | Identity

Application: Short Term

- Review your security budget allocation – are you overspending on prevention relative to detection and response?
- Identify what blind spots you have across your IT assets

Application: Medium-term

- Review your identity strategy. Have you covered the breadth of identity-related use cases?
- Identify what assets are the most critical (and develop a regular cadence for reviewing and prioritizing those assets)

Takeaways

1. We need pervasive and true visibility
2. Identity and authentication matter even more
3. Embrace and own your risk