RAPID7

INCIDENT DETECTION AND RESPONSE

Oct 2015

- Contemporary Challenges
  - Attacks are Fast
  - We are all Special Snowflakes
  - Uniqueness is the Common Denominator
  - Real-Time Incident Detection
- Cases
  - Golden Ticket Attacks
  - Spear Phishing Campaigns
  - Machine Learning in Security
- Technical Dive into our Solutions
  - Data
  - Integrity
  - R&D

INCIDENT DETECTION

Attacks are Fast

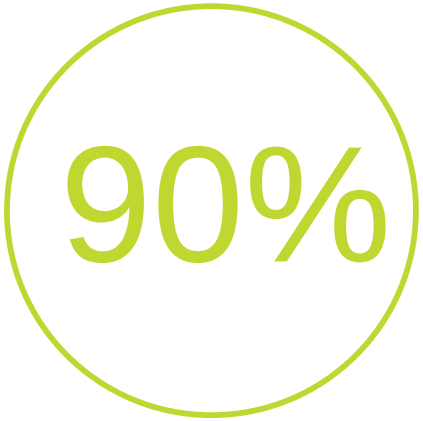
- In 60% of cases attackers are able to compromise a target in minutes
- 23% of recipients open phishing campaigns
- 50% of those click on phishing links within the first hour
- With 10 emails the chance of a successful campaign is 90%

-2015 Data Breach Report, Verizon

“A CVE BEING ADDED TO METASPLOIT IS PROBABLY THE SINGLE MOST RELIABLE PREDICTOR OF EXPLOITATION IN THE WILD.”

-2015 DATA BREACH REPORT, VERIZON

We are all Special Snowflakes



70-90% of malware samples are unique to an organization

-2015 Data Breach Report, Verizon

Uniqueness is the Common Denominator

- Anomaly detection is the name of the game
- Corporate environments are highly managed
- The more data you collect the easier it is to find outliers
- The big problem: How do you do it fast?

Real-Time Incident Detection

- Too many alerts reduces confidence
- Too few alerts misses actionable breaches
- Signal-to-noise ratio is crucial
- These are software problems, not security problems

GUTS & GLORY
AKA
TODAYS ATTACKS

Golden Ticket Attacks

- Modern evolution of pass-the-hash attacks
- Escalate privileges on a box
- Dump memory with tools like mimikatz
- *Modify the ticket and be whoever you want!*

- http://www.slideshare.net/gentilkiwi/abusing-microsoft-kerberos-sorry-you-guys-dont-get-it

Golden Ticket Attacks – How to Detect

- Security identifier (SID) to user mismatch
- Need to know all SID-User mappings
- Need to collect all tgts in the network for full coverage
- Detection needs to be fast, because mitigation is painful

Golden Ticket Attacks – Detection Tech

- Endpoint monitoring
- AD log collection
- SID-User attribution
- Detection needs to be fast, because mitigation is painful
- Hint: *Burn it with fire*

Spear Phishing Campaigns

- Easiest to overlook, but the scariest attack
- Harder to detect then you might think
- Public information makes these attacks easy

Spear Phishing Campaigns - Embarrassment

- Internal phishing campaign launched against Rapid7
- Used named executives in a targeted manner
- Used our SAML as a weakness
- I failed.

Spear Phishing Campaigns - Continued

- Newly purchased domains
- Domain names that look similar to the real deal
- Forged header
- Links that don’t add up
- Attachments that are malicious

Spear Phishing Campaigns - Detection

- Threat intelligence on links
- Detect anomalous processes in the network
- Intelligence sharing between organizations
- *Can a computer see a spoofed domain?*

Machine Learning in Security

- Learn how to “see” spoofed domains
- Each organization is different
- Static models with dynamic weights work.
- Spoofing detection is just the beginning

HOW DO WE DO IT?

How do we do it?

01011011101010
1000101101010 0

Data Collection

Normalization

Attribution

Behavior Generation

Incident Detection

Behind the scenes - Data

- Amazon S3
- Cassandra
- RDS
- Redis
- EleasticSearch

Behind the scenes - Integrity

- Fault tolerance is paramount
- Stateless services
- Queuing data
- Auto-scale everything

Behind the scenes – R&D

- Use the right technology for the job
- Fail fast
- Decouple as much as possible
- Deploy in a reproducible manner
  - Convection: https://github.com/rapid7/convection

userinsight

DEMO TIME

QUESTIONS?