MIRcon 2014

Taming the Wild West:
Finding Evil with Cloud-Based Analytical Tools

Christian Schreiber
CISO
The University of Arizona

Outline

- Understanding a research university
- Unique challenges
- Cloud-based analytics
- Results and lessons learned

Understanding a research university

Understanding a research university:

The University of Arizona by the numbers

- More than 41,000 students
- More than 15,000 employees
- More than $2 billion annual operating budget

- More than $625 million in annual research expenditure

- Statewide job and economic impact (2011)
  - Combined from University, Health Network, and Tech Park
  - Contributes $8.3 billion in annual economic impact
  - Creates more than 65,000 direct and indirect jobs

Understanding a research university:

UA “Real World” comparisons

- More than $320 million in credit card sales annually
- Health Network serves 100,000 patients / Level 1 trauma center
- Campus Health serves more than 15,000 patients annually
- Arizona Poison and Drug Information Center
- Power plant generates 30% of electricity; university manages multiple substations including one supporting hospital
- CALEA accredited Police Department with 66 sworn officers and 46 civilian employees, 9-1-1 dispatch
- More than 7,000 residents living in campus housing

Understanding a research university:

Information technology comparisons

- Highly decentralized: 37 IT departments with 900+ staff
- $110 million annual IT expenditure (50/50 central and unit)
- 7,600+ wireless access points on main campus
- More than 100,000 BYOD devices during typical week
- Central IT: ERP, core network + Internet, datacenter colocation and hosting, research supercomputers
- Unit IT: manage thousands of servers with little oversight from central IT or security teams

Understanding a research university:

More like a small city!

MIRcon 2014

Why are universities targeted?*

Sensitive Enterprise Data	Research with Potential Economic Value	Politically or Commercially Sensitive Information
• Employee data • Student records • Financial data • Recruitment and marketing data	• Energy technology • Biotechnology, medical, and pharmaceuticals • Engineering • New materials, such as semi-conductors • Information technology	• Climate modelling • Economic data and projections • Live animal research • Product development data • Information used for expert testimony

* Adapted from: Universities UK. "Cyber security and universities: managing the risk." November 2013.

MIRcon 2014

Information security challenges

- Decentralized decision making
- Culture focused on idea creation and sharing
- Limited ability to require preventative controls

- High population turnover
- Limited budget and manpower

- And… remember those 37 IT departments?

Why cloud-based analytical tools?

- Needed visibility without burden on local IT staff
- Limited security staff to deploy and maintain local solution
- Needed to ingest and act on variety of log sources

- Began using Threat Analytics Platform in June 2013

- Techniques here could be done with any SIEM and analytics tool

Example 1: VPN sessions using compromised user credentials

Used subsearch function

- Search for all usernames with WiFi authentication events
- Search for matching usernames from VPN authentication events with non-US GeoIP data
- Group by unique username

Results: Identified 10 – 20 compromised accounts/day

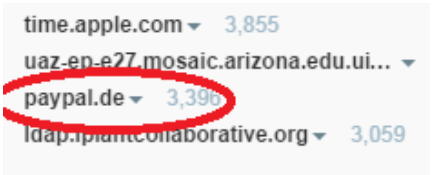
Example 2: Open Recursive DNS servers participating in DDoS

Step 1: Identify unusual domains in DNS logs

Search “metaclass” using pivot feature

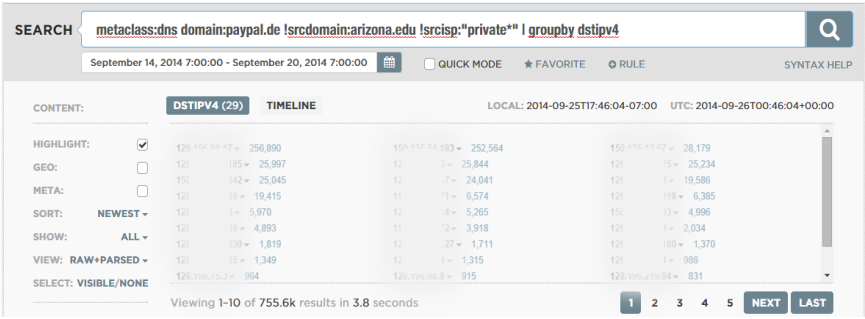
- Metaclass:DNS combines BIND syslogs and DNS grabbed off wire by BRO network sensors
- Group by domain and sort by highest frequency

Results: Visually identify unusual domains



Example 2: Open Recursive DNS servers participating in DDoS

Step 2: Identify Open DNS Resolvers being queried



Example 3: Employee direct deposit modification from outside Arizona

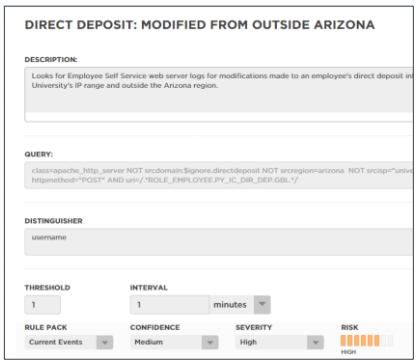
Used alert rules

- Search Apache logs for POST method and unique URI string
- Group by username
- Rule runs once each minute

Tuning for false positives

- List of domains to exclude

Results: Investigate 3 – 5 accounts per week



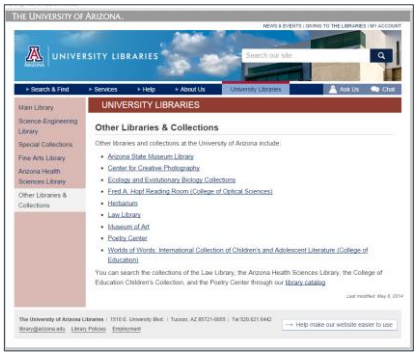
Example 4: Compromised accounts accessing Library resources

Needed to identify compromised accounts downloading material

Built off same technique as compromised VPN search

Leverage additional log sources

- WiFi authentication
- VPN authentication
- Web Single Sign On
- EZProxy authorization



Example 4: Compromised accounts accessing Library resources

Built custom parsing for EZProxy logs

- Similar to Apache but slight nuances

Used multiple searches with subsearch function

- Identifies accounts logging in from multiple GeoIP regions
- Filters to highlight EZProxy users tagged in broader search

Results: Investigate 2 – 5 compromised accounts/day

```
username:(class:[cisco_vpn,jasig_cas,shibboleth_sso,oclc_ezproxy]
AND has:srcipv4
AND has:srccountrycode
not srccountrycode:us
not srccountrycode:mx
not srccountrycode:ca
not action:"authentication_failed"
not action:"ticket_granting_ticket_not_created"
not msg:"authentication: rejected*")

AND ((class:[jasig_cas,cisco_vpn,shibboleth_sso,oclc_ezproxy]
AND (srccountrycode:us OR srcisp:"private ip address lan")
NOT (srcipv4:10.138.* OR srcipv4:150.135.114.* OR srcipv4:150.135.115.*)
not action:"authentication_failed"
not action:"ticket_granting_ticket_not_created"
not msg:"authentication: rejected*")

OR (class:cisco_acs AND callid:10.*))

AND class:oclc_ezproxy | groupby username 1000
```

Questions?

- Christian Schreiber
  schreiber@email.arizona.edu