Fact Tables: A Case Study in Reducing Reactive Time-to-Know by 95%

Jeff Boerio, Sr. Advanced Intrusion Analyst, Intel Corp.
Victor Colvard, Security Systems Engineer, Intel Corp.
Today’s Talk

• Our wake-up call
• What we had in terms of “SBI”
• Where we are today
• What is this “Order-1” or “Fact Table” concept
• How it fits in our workflow
• Other use cases
Where it Started – Operation Aurora

Operation “Aurora” Hit Google, Others

Highly resourced, coordinated attack campaign affecting dozens of US-based companies in the technology, finance, media, & chemical sectors

What Went Well
- Intel ahead of most peers in response
- Required expertise largely existed in-house

What Didn’t
- People, Process, Tool issues
  - New team unknown to some data owners
  - Accessibility/Availability of data
  - Geo challenges
  - No real time monitoring
- Challenges to sustaining response
  - Day jobs didn’t go away
  - If another APT event had occurred …

Intel notified, Prelim. investigation
Response team formed

Feb ‘10
10K Filing

Mar ‘10
Response team deactivated
Databases only held 45 days of data
Enter SBI

Netflow — Botnet — IDS — HIPS — AV — OSINT — DB
VPN — Proxy — Email — DNS — DHCP — Firewall — Account (and more)

Threat Management
- Malware escalation
- Anomalous activity escalation
- SBI/SIEM continuous improvement

Vuln Mgt

Incident Response
Responds to:
- Cyber Events
- Site, Corporate EOC
- System, App Outages
- Information Security

Types of Response:
- Proactive
- Reactive
- Need To Know

Incident Commander

SBI/SIEM

IIS Investigations
- Forensics
- Privacy
- Legal

Fellow Travelers
- LEO
- Prof Orgs
- Peer Companies

Advanced Threat Response (APT)

As needed:
- Cyber Intelligence
- Malware Analyst
- Forensic Investigations
- Communications (+PR)
- Patch/Remediate
- Data Center
- Disaster Recovery
- Business Apps
- Business Partners

1yr data for all event sources – but there’s a LOT of data
Order(1) Proxy Searches
IOC – Have You Seen It?

evil.com
IOCs – Have You Seen These?

APT1 IOCs
Requirements

- Have we seen attempts to *blah*?
- How many?
- What date range?
- Keep for a long time (2-5 yrs)
- Speed
Fact Table

```
select host, 
    min(timestamp) as "First Seen", 
    max(timestamp) as "Last Seen", 
    count* 
from proxyDB 
group by 1
```

<table>
<thead>
<tr>
<th>Host</th>
<th>First Seen</th>
<th>Last Seen</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>example.com</td>
<td>1974-01-12 18:32:08 UTC</td>
<td>1974-01-12 18:32:08 UTC</td>
<td>2</td>
</tr>
</tbody>
</table>

Take all the sites we saw on $day and add to O1db
# Uses

## Have we ever seen traffic to example.com or example2.com?

```sql
select Destination, min(MIN_TS) as "First Seen", max(MAX_TS) as "Last Seen", sum(Count) from proxyOLDB where Destination in "example.com,example2.com" and MIN_TS="01-01-1970 00:00:00" and MAX_TS="12-31-2008 23:59:59" group by 1
```

<table>
<thead>
<tr>
<th>Destination</th>
<th>First Seen</th>
<th>Last Seen</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>example.com</td>
<td>1970-01-01 09:15:31 UTC</td>
<td>1974-01-12 18:32:08 UTC</td>
<td>854</td>
</tr>
<tr>
<td>example2.com</td>
<td>1998-11-21 19:13:01 UTC</td>
<td>2008-12-02 04:12:01 UTC</td>
<td>20</td>
</tr>
</tbody>
</table>

## When did we see traffic to example.com?

```sql
select Destination, min(MIN_TS) as "First Seen", max(MAX_TS) as "Last Seen", sum(Count) from proxyOLDB where Destination = "example.com" and MIN_TS="01-01-1970 09:15:31" and MAX_TS="01-12-1974 18:32:08" group by 1
```

<table>
<thead>
<tr>
<th>Destination</th>
<th>First Seen</th>
<th>Last Seen</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>example.com</td>
<td>1974-01-12 03:00:01 UTC</td>
<td>1974-01-12 18:32:08 UTC</td>
<td>481</td>
</tr>
</tbody>
</table>
Now We Have Something to Pivot On

<table>
<thead>
<tr>
<th>Destination</th>
<th>First Seen</th>
<th>Last Seen</th>
<th>Count</th>
</tr>
</thead>
</table>

**Timestamp** | **Client_IP** | **Username** | **Destination**
--- | --- | --- | ---
1970-01-01 09:15:31 UTC | 10.1.1.1 | joe | example.com
1970-01-01 09:18:31 UTC | 10.1.1.1 | joe | example.com
1970-01-01 09:10:22 UTC | 10.1.1.3 | sue | example.com
1970-01-01 08:32:33 UTC | 10.1.1.3 | sue | example.com

**Client_IP** | **Hostname** | **Start** | **Stop**
--- | --- | --- | ---
10.1.1.1 | joe-laptop | 1970-01-01 07:02:11 UTC | 1970-01-03 15:22:00 UTC

O(1) Results

Detailed Searches

What used to take weeks now takes <1 day
DNS Use Case

Requirements essentially the same
• Have we seen attempts to *blah*?
• How many?
• What date range?
• Keep for a long time (2-5 yrs)
• Exclude Intel lookups
• Speed

Our O(1) DNS only stores non-intel.com queries
Improvements, Automation, Additional Work
Proxy/DNS “Firehose”

Current
• Provide IOCs to engine
• Engine queries on O(1) tables

Future
• Automatically open a case
• Engine automatically pulls proxy/DHCP
  • And employee entitlements/access

Do all the work an analyst currently does manually
Generate shareable threat intelligence
DNS Tunnel Detection

- Query O(1) DNS table
- Remove Alexa Top 1 Million
- Count primary domains
- High counts could indicate tunnels

Detected pen testing vendor
Other Use Cases

• User-Agent
  • Many malware uses specific U-A strings

• Observed Malware
  • How many times are you seeing a malware family

• Email
  • Phishing campaigns based on sender, subject, etc

• VPN
  • Identify geo-spatial issues or anomalies

Be mindful of privacy requirements
Acknowledgements

Steve Mancini  Idea development
Victor Colvard  Solution engineering
Stacy Purcell  SBI evangelist
Questions?

Jeff Boerio, Sr. Advanced Intrusion Analyst, Intel Corp.
Email: jeff.boerio@intel.com
Victor Colvard, Security Systems Engineer, Intel Corp.
See Jeff for Contact Details