Tipping the Scales Back in our Favor

May, 2022
René Agüero MSBA, CISSP
Global Director Security Strategists
Overview

• Why is it so damn expensive?
• Organized operationalized attacks!
• My data for sale
• What we can do?
How much pain?
What’s going on???

Espionage
Insider Threat
APT

SOC
Proactive Monitoring

125 lines

Millions of lines
Malware with SLA
Who?
Attackers know

- Learn victim environments
- Test new attacks in their labs
- Get stolen keys from black market
- Test different rules – evade, evade, evade
Attacker Techniques

- Metasploit – Runs on raspberry Pi pwnyExpress
- Malware Kits – SLA with support
- Phishing – almost always works
- Proxy attacks – B2B connections, Priv Account monitoring
- Poorly secured systems - cloud and boundary
- Watering hole attacks
Terminal

= metasploit v4.4.0-dev [core:4.4 api:1.0]
+-- --= 898 exploits - 486 auxiliary - 150 post
+-- --= 251 payloads - 28 encoders - 8 nops

msf >

KALI LINUX

splunk > turn data into doing
Figure 28: The inevitability of the click

Probability of at least one click

E-mails per campaign
What?

- Healthcare data - $363 per record
- Counterfeit social security cards - $250 to $400
- Forged driver's license - $100 to $150
- European Union, AsiaPac credit card with track data - $28
- U.S. credit card with track data - $1
P@$$$w0rd5

- NIST 800-63 – Move Past passwords
- Compromised Creds
- MFA and 2FA - not panacea
- Browsers
- Password Managers
- PAM - IAM
Advanced Threats Are Hard to Find

Cyber Criminals
“Another Day, Another Retailer in a Massive Breach”

Nation States
“Banks Seek U.S. Help on Supply Chain attacks”

Insider Threats
“Edward Snowden Tells SXSW He'd Leak Those Secrets Again”

100% Valid credentials were used

40 Average # of systems accessed

28 Median # of days before detection

67% Of victims were notified by external entity
APTs are Essentially Attack Transactions – but the **attacker** is trying to hide

**Technolog**

- **Threat Intelligence**
- **Network Access/Security**
- **Endpoint Access/Security**

**Transaction**

- Attacker hacks website
  - Steals .pdf files

**Gain Access to system**

- Web Portal

**Create additional environment**

- Remote control
  - Steal data
  - Persist in company
  - Rent as botnet

**Conduct Business**

- http (web) session to command & control server

**Technolog**

- **pdf** executes & unpacks malware
  - Overwriting and running “allowed” programs

**Transaction**

- Attacker creates malware, embed in .pdf
- emails to the target

**Conduct Business**

- .pdf creates additional environment
  - Gain Access to system
  - Conduct Business

**Technolog**

- .pdf executes & unpacks malware
  - Overwriting and running “allowed” programs

**Transaction**

- .pdf creates additional environment
  - Gain Access to system
  - Conduct Business

**Technolog**

- .pdf executes & unpacks malware
  - Overwriting and running “allowed” programs

**Transaction**

- .pdf creates additional environment
  - Gain Access to system
  - Conduct Business

**Technolog**

- .pdf executes & unpacks malware
  - Overwriting and running “allowed” programs

**Transaction**

- .pdf creates additional environment
  - Gain Access to system
  - Conduct Business

**Technolog**

- .pdf executes & unpacks malware
  - Overwriting and running “allowed” programs

**Transaction**

- .pdf creates additional environment
  - Gain Access to system
  - Conduct Business

**Technolog**

- .pdf executes & unpacks malware
  - Overwriting and running “allowed” programs

**Transaction**

- .pdf creates additional environment
  - Gain Access to system
  - Conduct Business

**Technolog**

- .pdf executes & unpacks malware
  - Overwriting and running “allowed” programs

**Transaction**

- .pdf creates additional environment
  - Gain Access to system
  - Conduct Business

**Technolog**

- .pdf executes & unpacks malware
  - Overwriting and running “allowed” programs
APTs are Essentially Attack Transactions – but the attacker is trying to hide
APT Defense using the Kill Chain Method

- Phishing or download from infected site
- Attacker communicates with system & installs tools
- Attacker escalates privileges, obtains credentials to key systems
- Data is acquired and staged for exfiltration
- Data sent to attacker system hidden in allowed outgoing traffic
- Any and all of the previous and more...

- Multiple activities, multiples phases
- Adversary (attacker) orientation
- Rationalize attribution (who), intent (why), tactics (how)
### Need to Connect the “Data-dots” to See the Whole Story

<table>
<thead>
<tr>
<th>Threat intelligence</th>
<th>Network Activity/Security</th>
<th>Host Activity/Security</th>
<th>Auth - User Roles, Corp Context</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delivery, exploit installation</td>
<td>Gain trusted access</td>
<td>Upgrade (escalate) Lateral movement</td>
<td>Data Gathering</td>
</tr>
<tr>
<td>Attacker, know relay/C2 sites, infected sites, IOC, attack/campaign intent and attribution</td>
<td>Where they went to, who talked to whom, attack transmitted, abnormal traffic, malware download</td>
<td>What process is running (malicious, abnormal, etc.) Process owner, registry mods, attack/malware artifacts, patching level, attack susceptibility</td>
<td>Access level, privileged users, likelihood of infection, where they might be in kill chain</td>
</tr>
</tbody>
</table>

**Exfiltration**
- Subscription feeds
- Open source
- Intelligence Sharing
- Firewalls
- Email, Web, DNS
- Malware analysis
- IDS/IPS
- Infrastructure
- Net flow
- Endpoint Threat Detection and Response (ETDR)
- Malware analysis
- Vulnerability Assessment
- Endpoint Security
- OS, App, database logs
- Patching
- LDAP, Active Directory, Authentication, SSO
- Asset databases CMBD, inventory
Connecting the “data-dots” via Relationships

- **Delivery, exploit installation**
- **Gain trusted access**
- **Upgrade (escalate) Lateral movement**
- **Data Gathering**
- **Exfiltration**

**Threat intelligence**
- Malware download

**Network Activity/Security**
- Unknown program install
- Process running

**Host Activity/Security**
- Same node/user with support indicators
- Multiple attributes link the 3 events
- Attributes are dynamic (since attackers are constantly changing techniques and tactics)

**Auth - User Roles**

**Data Gathering**
- Traffic to C2 from malware analysis

**High confidence event**
- Machine data

**Med confidence event**
- Traffic data

**Low confidence event**
- Abnormal behavior

**Authentication**
- User Roles

**Host**
- Activity/Security

**Network**
- Activity/Security

**Delivery, exploit installation**
- Malware download

**Gain trusted access**
- Unknown program install
- Process running

**Upgrade (escalate) Lateral movement**
- Traffic to C2 from malware analysis

**Data Gathering**
- Traffic data

**Exfiltration**
- Abnormal behavior
Connecting the “data-dots” via Relationships

- Threat intelligence
- Network Activity/Security
- Host Activity/Security
- Auth - User Roles

Delivery, exploit installation
Gain trusted access
Upgrade (escalate) Lateral movement
Data Gathering
Exfiltration

Malware download
Program installation
User on machine
Link to program
And process
Malware install

Blacklisted IP
Continued sessions during abnormal hours, periodicity, patterns, etc.

High confidence event
Med confidence event
Low confidence event
Abnormal behavior

Machine data
Traffic data
Insider Threat

Non-tech indicators

- SAP
- HR
- Dunn & Bradstreet
- HDFS
- Lexus Nexus
- Time Management
- Asset DB

Traditional Data

- Network & malware
- Threat Intelligence
- User & Identity
- Host & Application

The CERT Top 10 List for Winning the Battle Against Insider Threats
Dawn Cappelli, Software Engineering Institute, Carnegie Mellon University
Alert Fatigue!

- Incidents based on narrowly defined detections lead to majority noise within the SOC
- Adding more sources and detection mechanisms continue to overburden the SOC Analysts with more alerts
- Whitelisting as a reaction to the above results in a situational numbness
A Change of Perspective

- Efficient use of existing toolchain
- Scale and retain HAPPY analysts

People
Tech
Process
Now Broken

How we (myself included) have been working
Risk Attributions

Analytics
RBA Using a SIEM/Framework of Your Choice

Risk Scoring Macros

Risk Rules

Risk Attributions

Risk Notables

ES Threat intel Framework
ES Datamodels
ES Correlation Rule Framework
ATT&CK™

Risk Incident Rules

ES Asset Framework
ES Identity Framework
ES Correlation Rule Framework
ES Risk Framework

Risk Notables
ES Notable Framework
ES Incident Management framework
Benefits of using a Rick Based Approach

- **Reduce Alerts**
  Leverage risk as a layer of abstraction

- **Improved Detections**
  Dramatic increase in the true positive rate

- **Quantified Maturity**
  Easier to align with a framework like MITRE ATT&CK for data sources, detections, and purple teaming

- **Analyst Scale**
  Decouple # detections and data sources from the linear scaling of the SOC analysts

- **Increased Analytics Window**
  Ability to look across much larger windows for low and slow. Red team’s job is MUCH harder

- **Easy to Deploy**
  Easier to map against an industry framework than general use cases. Easy to integrate with SSE and ESCU
OLD PARADIGM

- TRADITIONAL TRIAGE
- RULES
- CONSTANT TUNING
NEW PARADIGM: RISK BASED ALERTING

USER FOCUS

MACHINE FOCUS

LESS TUNING
How does this look in practice?

With risk-based alerting, what were individual alerts become context that informs high-fidelity alerts.

6:55 AM
- Potential spearphishing observed - 10pts

6:58 AM
- Suspicious command disabling controls - 15pts

7:03 AM
- Suspicious Powershell observed - 20pts

7:07 AM
- AWS ACLs opened up all access - 10pts

7:13 AM
- AWS user provisioning observed - 15pts

7:16 AM
- AWS buckets created - 15pts

7:22 AM
- AWS permanent creation observed - 20pts

Risk Incident Rule:
Generate alert for any user or system that exceeds a risk score of 100 in a 24 hr period.

With one click, view all of the risk events that contribute to the alert.

Aggregated user risk score > 100
Hack Thyself

- Scan everything
- Pen tests
- Phish employees
- Provide training
- USB drops
- Social engineering
Sharing is caring

- ISACs
- Soltra Edge
- Other industries - Healthcare
- More meetings like this one
- VDBIR
- Sharing Enclaves
Listen to your data

• Know where you are
• Know how to get better
• All data is security relevant
• More meetings like this one
• VDBIR
Takeaways

• They’re coming for us
• Modern attacks require a modern approach
• Hack Thyself
• Share and use
• Know where you are and how to improve
THANK YOU