ATTACK CHAIN LESSONS

Bolster Your IR Program

Eric Sun, Solutions Mktg, Rapid7
@exalted
Today’s Topics

Why is the Attack Chain important?  
Today’s state of security  
Common gaps & Rapid7 best practices
Who is Eric?

- PMM – Incident Detection & Response @Rapid7
- Behavior analytics / risk management background
- Custom enterprise mobile app development – Zco Corporation
Delivering Security Data & Analytics that revolutionize the practice of cyber security

5,300+ Customers  36% Fortune 1000  99 Countries  900+ Employees

NASDAQ: RPD
What is the Attack Chain?

• Graphical representation of steps required to breach a company

• Applies across entire range of attacks
  – Credential-based attacks
  – Malware
  – Vulnerability exploitation

• Detecting earlier in the chain = no chance for data exfiltration
Why is the Attack Chain Important?

• Poker story: “How much you bluff?”

• Sharks:
  – Attack the right target
  – Analyze behavior to find weakness

• Attackers:
  – Monetizable data + immature
  – What’s worked before?

• IR Program: compare against attacker maturity, not similar organizations
Steps in the Attack Chain

Infiltration and Persistence
- Phish users
- Use leaked credentials
- Connect to network
- Anonymize access
- Deploy backdoors

Reconnaissance
- Get user list
- Scout targets
- Find vulnerabilities

Lateral Movement
- Access machines with credentials
- Collect more passwords
- Increase privileges

Mission Target
- Access critical data
- Upload data to external location

Maintain Presence
- Deploy backdoors
- Continued check-ins for future use
Variations in the Attack Chain

Infiltration and Persistence
- Phish users with fake log-in page
- Use compromised credentials to gain access
- Exploit vulnerability

Mission Target
- Access critical data
- Upload data to external location
Modeling Your Security Program to the Attack Chain

1. Detecting earlier in the chain is better
2. Avoid duplications per step to reduce overspending
3. Identify gaps in your security program
4. Focus on high-probability attacks first
Top Attack Vectors Behind Breaches

Significant Threat Actions Over Time

- Credentials
- RAM Scraper
- Spyware/Keylogger
- Phishing

60%
Challenges Implementing the Attack Chain Approach

• So *many* security monitoring solutions
• Your security stack may be siloed, or have significant overlap
• Difficult to measure individual or combined effectiveness
• Implementation often is a scattershot approach or in response to pain
Top Gaps Across the Attack Chain

Coverage Across Network (Step 1)
- Cloud services
- Remote workers

Attacker Recon (Step 2)
- Network scans
- Password guessing attempts

Compromised Creds (Step 3)
- Cannot detect with threat intel
- Present in 63% of confirmed data breaches*

*2016 Verizon Data Breach Investigations Report
WHAT ARE WE DOING TODAY?
The Survey

2. 24 Questions, 10-15 mins to complete – 86% completion
3. LinkedIn, Twitter, R7 Community, Rapid7 Staff
4. Report & Apple Watch
Security Team Size

Figure 4: What size is your security team?

1-1000 Employees
Answered: 152 (56%)  Skipped: 0

1001-5000 Employees
Answered: 49 (18%)  Skipped: 1 (~1%)

5001+ Employees
Answered: 68 (25%)  Skipped: 1 (~1%)
What security products do you use for Incident Detection and Response?

- IPS: 60%
- Endpoint Agent: 60%
- SIEM: 50%
- Malware/Sandboxing Solution: 40%
- Forensics: 30%
- Netflow: 20%
- User Behavior Analytics: 0%
Top 3 Security Initiatives

1. Security Information & Event Management: Deploying and maintaining SIEM

2. Threat Exposure Management: Pen testing, vuln management, web app scanning

3. Firewall: Tuning, replacing, and deploying next-gen solutions
SIEMs: How are they being used?

• Do you use one? (poll)
• Primary drivers:
  – Incident Detection
  – Compliance
  – Log Search
• How are they useful?
• What is being monitored?

Figure 8: Does your organization use a SIEM?

Answered: 264 (97%)  Skipped: 7 (3%)

No, we don’t have plans to buy a SIEM
26.14% (69)

Yes
52.27%

No, but we are looking to purchase
21.59% (57)
How many daily alerts do you receive from your SIEM?

- 75-200
- 26-74
- 11-25
- 1-10
- 201+

How many security alerts can your team investigate per day?

- 75-200
- 26-74
- 11-25
- 1-10
- 201+
79% of companies allow the use of approved cloud services. 67% of companies don’t have security visibility into those cloud services.

Office 365, Google Apps, and Salesforce are the top 3 cloud services used by businesses.
Top Security Team Pain Points

Security teams are strained

Strained sec team; incomplete ecosystem coverage

SIEMs: too many alerts

62% orgs receiving more alerts than they can investigate

Investigations take too long

False positives; retracing user activity; incident scoping
WHERE ARE WE GOING?
From Compromise to Containment — Fast!

Cut Through the Noise
Behavioral Analytics
Detection Traps
Alerting

Speed Investigations
Contextual Investigations
Endpoint Forensics
Enterprise Search

End Data Drudgery
Log, Machine and User Data
Attribution
Compliance Reporting
Malware Detected: Dropper.exe
Outbound Network Connection to China
Martha Green  978-2460 to razor.com

Firewall Anomaly Event
User Martha Green sent an unusual amount of data to China IP Address

New Asset Accessed
User Martha Green logged into intranet.razor.com

Malware Detected: Dropper.exe
Outbound Network Connection to China
Martha Green  9724-6100 to razor.com

New Asset Accessed
User Martha Green logged into Firewalls.razor.com

Malware Detected: Dropper.exe
Outbound Network Connection to China
Luisa Castro  5566-6100 to razor.com

Honeypot Detected Malicious Scan
User Martha Green attempted SSL connections in a honeypot.
Disrupting The Attack Chain

Infiltration and Persistence
- Detect phishing attempts
- Spot vulnerabilities and malware
- Alert on leaked credentials
- Monitor inbound connections

Reconnaissance
- Detect network scans

Lateral Movement
- Detect intruders switching identities
- Detect unusual authentications
- Spot vulnerabilities and malware
- Identify privilege escalation

Mission Target
- Detect suspicious access to critical data
- Monitor data traffic and cloud usage

Maintain Presence
- Detect malicious processes
Honey Pots

What is a honey pot?
• Virtual machine that appears as legitimate asset.

Why?
• Identify early attacker reconnaissance

Honey Users

“a.k.a. Fake users”

What is a honey user?
• Fake accounts to lure attackers to try authentications.
• Rapid7 Heisenberg Research

Why?
• Identify AD/LDAP enumeration & password guessing attempts.

Honey Credentials

What is a honey credential?
• Fake credentials onto your endpoints – alerts if used

Why?
• Detect pass-the-hash & other techniques earlier in the attack chain.
Customer Success with InsightIDR & InsightUBA

“Cuts incident investigation and reaction time by 20x.”
Cameron Chavers
Manager of Enterprise Security
Full Story

Incident detection and investigation has always been a cumbersome, manual process. With InsightIDR all the information I need to understand and solve a problem is at my fingertips.

Jordan Schroeder
Security Architect

Without InsightUBA, correlating user behavior would be time consuming – roughly two to three business days per incident. With InsightUBA, it’s 60 seconds.

When you compare it to our previous method of manually going through logs, it’s reduced investigation time by roughly 85 percent.
Russ Swift
Information Security Manager

“If someone [logged] in twice across 200 machines… would I catch that? Without InsightUBA, the answer is no.”
Nick Hidalgo
Director of IT
Full Story
Key Takeaways

1. Prioritize early attack chain detection
2. Have coverage on each of the steps appropriate to your security bandwidth
3. Identify gaps in your security program (e.g. compromised credentials?)
Full Range for Incident Detection & Response

People
IDR Services
ANALYTIC RESPONSE
INCIDENT RESPONSE SERVICES

Process
IDR Program Development
IDR PROGRAM ASSESSMENT
IDR PROGRAM DEVELOPMENT

Technology
IDR Software
InsightIDR
InsightUBA
THANK YOU!

Eric Sun, eric_sun@rapid7.com, @exalted
www.rapid7.com/solutions/incident-detection
InsightIDR Solution Architecture

- Network Events
- Real-Time Endpoint Events
- Intruder Traps
- Applications
- Existing Security Solutions, Alerts, and Events

On-Premise Insight Collectors

Remote Endpoints

InsightIDR Attacker Analytics Platform

- User Behavior Analytics
- Machine Learning
- Fully Searchable Data Set

Enterprise Cloud Apps

Mobile Devices
Insight Platform Supported Event Sources

FOUNDATION EVENT SOURCES

LDAP
Microsoft Active Directory LDAP

Active Directory
Microsoft

DHCP
Alcatel-Lucent VitalQIP
Bluecat
Cisco iOS
Cisco Meraki
Infoblox Trinzic
ISC dhcpd
Microsoft
MicroTik
SophosUTM

VALUE-ADD EVENT SOURCES

› DNS
› VPN
› IDS / IPS
› Web Proxy
› Firewall
› E-mail Servers
› Security Console
› Enterprise Cloud Applications
› Intruder Traps
**DNS**
ISC Bind9
Infoblox Trinzc
Microsoft DNS
MikroTik
PowerDNS

**Data Exporters**
FireEye Threat Analytics Platform
HP ArcSight & ArcSight Logger
Splunk

**VPN**
Barracuda NG
Cisco ASA
Citrix NetScaler
F5 Networks FirePass
Fortinet FortiGate
Juniper SA
Microsoft IAS (RADIUS)
Microsoft Network Policy Server
Microsoft Remote Web Access
MobilityGuard OneGate
OpenVPN
SonicWALL
VMware Horizon
WatchGuard XTM

**Web Proxy**
Barracuda Web Filter
Blue Coat
Barracuda Web Filter
Cisco IronPort
Fortinet FortiGate
Intel Security (fka McAfee) Web Reporter
McAfee Web Reporter
Sophos Secure Web Gateway
Squid
TrendMicro Control Manager
Watchguard XTM
WebSense Web Security Gateway
Zscalar NSS

**E-mail & ActiveSync**
Microsoft Exchange Transport Agent (Email monitoring)
OWA/ActiveSync (Ingress monitoring, mobile device attribution)

**Firewall**
Barracuda NG
Cisco ASA & VPN
Cisco IOS
Cisco Meraki
Check Point
Clavister W20
Fortinet Fortigate
Juniper Junos OS
Juniper Netscreen
McAfee
Palo Alto Networks & VPN
pfSense
SonicWALL
Sophos
Stonesoft
Watchguard XTM

**IDS / IPS**
Cisco Sourcefire
Dell iSensor
Dell SonicWall
HP TippingPoint
McAfee IDS
Metaflows IDS
Security Onion
Snort

**Rapid7**
Windows Agentless Endpoint Monitor
Mac Agentless Endpoint Monitor
Honeypot & Honey Users
Metasploit
Nexpose
Sophos Enduser Protection
Symantec Endpoint Protection

**Cloud Services**
Microsoft Office 365
AWS Cloud Trails
Box.com
Duo Security

**Advanced Malware**
FireEye NX
Palo Alto Networks WildFire

**SIEMs/Log Aggregators**
HP ArcSight
IBM QRadar
Intel Security (fka McAfee)
NitroSecurity
LogRhythm
Splunk

**Virus Scanners**
Cylance Protect
Check Point AV
F-Secure
McAfee ePO
Sophos
Symantec Enduser Protection
TrendMicro OfficeScan
TrendMicro Control Manager

**Application Monitoring**
Atlassian Confluence
Microsoft SQL Server
## Mapping Security Solutions to the Attack Chain

<table>
<thead>
<tr>
<th>Infiltration and Persistence</th>
<th>Reconnaissance</th>
<th>Lateral Movement</th>
<th>Mission Target</th>
<th>Maintain Presence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Email Gateway</td>
<td>Intrusion Detection System</td>
<td>Network Behavior Analysis (Packet Capture)</td>
<td>SIEM</td>
<td>Endpoint Detection &amp; Protection Platform</td>
</tr>
<tr>
<td>Malware Protection System</td>
<td>Network Behavior Analysis (Packet Capture)</td>
<td>Security Information &amp; Event Management (SIEM)</td>
<td>Database Audit &amp; Protection</td>
<td>SIEM (via Hunting)</td>
</tr>
<tr>
<td>Intrusion Detection System</td>
<td>Honeypot Technology</td>
<td>File Activity Monitoring</td>
<td>Endpoint Detection &amp; Protection Platform</td>
<td></td>
</tr>
<tr>
<td>Web App Firewall</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Database Audit &amp; Protection</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Endpoint Detection &amp; Protection Platform</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>