Attack Chain Lessons
Bolster Your IR Program

Eric Sun, Solutions Mgr,
Incident Detection & Response

@exalted
What is the Attack Chain, and why map to it?

Today’s state of Incident Detection & Response

Rapid7 approach to Investigations
Who is Eric?

• Solutions Manager – Incident Detection & Response @Rapid7
• Behavior analytics / risk management background
• Custom enterprise mobile app development – Zco Corporation
trusted by

5,600+
organizations

100+
countries

View All Customers
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 sized orgs
Steps in the Attack Chain

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

**Explore Network**
- 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
- Use leaked credentials
- Connect to network
- Anonymize access
- Deploy backdoors

**Mission Target**
- Access critical data
- Upload data to external location
Top Gaps Across the Attack Chain

Unified Network Coverage (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 IDR Survey

2. 24 Questions, 10-15 mins to complete – 86% completion
3. LinkedIn, Twitter, R7 Community, Rapid7 Staff
4. Findings 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%)

49% 26% 26%
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**: 10%
Top 3 Security Initiatives

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

2. Reducing Attack Surface: 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?
How many daily alerts do you receive from your SIEM?

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

How many security alerts can your team investigate per day?

- 201+
- 75-200
- 26-74
- 11-25
- 1-10
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
  - Limited resources; gaps in coverage

- Too many alerts
  - 62% orgs receiving more alerts than they can investigate

- Investigations take too long
  - Time-consuming to validate; jumping between multiple tools
Where are we going?
Combine SIEM, UBA, and EDR to leave attackers with nowhere to hide.

Find unknown threats with User Behavior Analytics and Deception Technology.

Know exactly where to search with Security Analytics.
Speeding up Investigations

**Is this alert real, or a false positive?**
Use experience and context to decide.

**Who was impacted?**
Retrace IP Addresses to the Users Behind Them

**What were the users doing?**
Review authentication logs; Query endpoint; Run forensics on machine

**Did this happen to anyone else?**
Search across log data; Run a hunt

**Gather findings. Create & share Super Timeline.**
Combine data across log search, user activity, and endpoint artifacts

---

Log Files (e.g. Event, AntiVirus, Firewall, Proxy)
SIEM/Log Aggregator
Endpoint Agent
User Behavior Analytics

**insightIDR**
Brings together:
- Enriched Log Search
- User Behavior
- Endpoint Data
DETECTION AND INVESTIGATION WORKFLOW
Lateral Movement of Credentials: User Sarah Spark attempted to remotely access 2 new assets
Last Accessed: Jan 24, 2016 @ 3:12PM

Honeypot Detected Malicious Scan: User Martha Green attempted 532 connections to 4 honeypots
Last Accessed: Jan 23, 2016 @ 10:00AM

Privileges Escalation: User Michael Henderson Authenticated as administrator
Last Accessed: Jan 22, 2016 @ 9:00AM

Spear Phishing URL Detected: Multiple visits to suspect domain rapid7 properties
Last Accessed: Jan 18, 2016 @ 6:00PM

Harvested Credentials: 192.92.94.23 failed to access 3 distinct accounts in 1 instances
Last Accessed: Jan 22, 2016 @ 3:10PM

Ingress From Service Account: Service account awskeyserver@rapid7.com authenticated 2 times
Last Accessed: Jan 21, 2016 @ 10:13AM

Account Password Reset: Password reset for account sbames by helenes
Last Accessed: Jan 19, 2016 @ 9:12AM
Lateral Movement of Credentials: User Sarah Spark attempted to remotely access 2 new assets
Last Accessed: Jan 24, 2016 @ 3:12PM

Honeypot Detected Malicious Scan: User Martha Green attempted 532 connections to 4 honeypots
Last Accessed: Jan 23, 2016 @ 10:03AM

Privileges Escalation: User Michael Henderson Authenticated as administrator
Last Accessed: Jan 22, 2016 @ 9:03AM

Spear Phishing URL Detected: Multiple visits to suspect domain rapid7 properties
Last Accessed: Jan 18, 2016 @ 6:05PM

Harvested Credentials: 192.92.94.23 failed to access 3 distinct accounts in 1 instances
Last Accessed: Jan 21, 2016 @ 3:12PM

Ingress From Service Account: Service account awskeyservlet@rapid7.com authenticated 2 times
Last Accessed: Jan 16, 2016 @ 10:19AM

Account Password Reset: Password reset for account sbames by helenes
Last Accessed: Jan 19, 2016 @ 9:12AM
INVESTIGATION DETAILS

Honeypot Detected Malicious Scan

Event Details:
- **Timeframe:** 01/24/16 to 01/27/16
- **Incidents:**
  - **01/24/16 08:30 PM:** Firewall Anomaly Event
    - User Martha Green sent an unusual amount of data to China IP Address
  - **01/25/16 09:30 AM:** New Asset Accessed
    - User Martha Green logged into info-fs.terazor.com
  - **01/27/16 09:20 PM:** New Asset Accessed
    - User Martha Green logged into Finance-fs.terazor.com
  - **01/24/16 09:10 PM:** Honeypot Detected Malicious Scan
    - User Martha Green attempted SSH connections to 4 honeypots

Investigation Elements:
- **Users:**
  - Martha Green
- **Assets:**
  - t230a-6100.terazor.com
  - t567-6100.terazor.com
  - t812-6100.terazor.com
02:20PM
**FIREWALL ANOMOLY EVENT**
User Martha Green sent an unusual amount of data to China IP Address

09:23AM
**NEW ASSET ACCESSED**
User Martha Green logged into info-fs.tor.razor.com

JAN 25, 2015

04:20PM
**NEW ASSET ACCESSED**
User Martha Green logged into Finance-fs.tor.razor.com

JAN 24, 2015

02:20PM
**HONEYPOT DETECTED MALICIOUS SCAN**
User Martha Green attempted 532 connections to 4 honeypots
02:20PM  
**FIREWALL ANOMOLY EVENT**  
User Martha Green sent an unusual amount of data to China IP Address

03:23AM  
**NEW ASSET ACCESSED**  
User Martha Green logged into info-fs.torrazor.com

04:20PM  
**NEW ASSET ACCESSED**  
User Martha Green logged into Finance-fs.torrazor.com

02:20PM  
**HONEYPOT DETECTED MALICIOUS SCAN**  
User Martha Green attempted 532 connections to 4 honeypots
<table>
<thead>
<tr>
<th>Process Name</th>
<th>Commonality</th>
<th>Executable Path</th>
<th>User</th>
<th>Start Time</th>
<th>Command Line</th>
<th>PID</th>
<th>Parent PID</th>
<th>MD5 Hashes</th>
<th>SHA1 Hashes</th>
</tr>
</thead>
<tbody>
<tr>
<td>chrome.exe</td>
<td>Common</td>
<td>C:\Program Files (x86)\Google...</td>
<td>TORRustance</td>
<td>2015-07-19 18:19:54 GMT</td>
<td>C:\Program Files (x86)\Google...</td>
<td>6534</td>
<td>6328</td>
<td>a3e2a02f5e241f1s5b...</td>
<td>705234646419f...</td>
</tr>
<tr>
<td>chrome.exe</td>
<td>Common</td>
<td>C:\Program Files (x86)\Google...</td>
<td>TORRustance</td>
<td>2015-07-19 18:19:54 GMT</td>
<td>C:\Program Files (x86)\Google...</td>
<td>6534</td>
<td>6328</td>
<td>a3e2a02f5e241f1s5b...</td>
<td>705234646419f...</td>
</tr>
<tr>
<td>chrome.exe</td>
<td>Common</td>
<td>C:\Program Files (x86)\Google...</td>
<td>TORRustance</td>
<td>2015-07-19 18:19:54 GMT</td>
<td>C:\Program Files (x86)\Google...</td>
<td>6534</td>
<td>6328</td>
<td>a3e2a02f5e241f1s5b...</td>
<td>705234646419f...</td>
</tr>
<tr>
<td>chrome.exe</td>
<td>Common</td>
<td>C:\Program Files (x86)\Google...</td>
<td>TORRustance</td>
<td>2015-07-19 18:19:54 GMT</td>
<td>C:\Program Files (x86)\Google...</td>
<td>6534</td>
<td>6328</td>
<td>a3e2a02f5e241f1s5b...</td>
<td>705234646419f...</td>
</tr>
<tr>
<td>chrome.exe</td>
<td>Common</td>
<td>C:\Program Files (x86)\Google...</td>
<td>TORRustance</td>
<td>2015-07-19 18:19:54 GMT</td>
<td>C:\Program Files (x86)\Google...</td>
<td>6534</td>
<td>6328</td>
<td>a3e2a02f5e241f1s5b...</td>
<td>705234646419f...</td>
</tr>
<tr>
<td>chrome.exe</td>
<td>Common</td>
<td>C:\Program Files (x86)\Google...</td>
<td>TORRustance</td>
<td>2015-07-19 18:19:54 GMT</td>
<td>C:\Program Files (x86)\Google...</td>
<td>6534</td>
<td>6328</td>
<td>a3e2a02f5e241f1s5b...</td>
<td>705234646419f...</td>
</tr>
<tr>
<td>chrome.exe</td>
<td>Common</td>
<td>C:\Program Files (x86)\Google...</td>
<td>TORRustance</td>
<td>2015-07-19 18:19:54 GMT</td>
<td>C:\Program Files (x86)\Google...</td>
<td>6534</td>
<td>6328</td>
<td>a3e2a02f5e241f1s5b...</td>
<td>705234646419f...</td>
</tr>
<tr>
<td>chrome.exe</td>
<td>Common</td>
<td>C:\Program Files (x86)\Google...</td>
<td>TORRustance</td>
<td>2015-07-19 18:19:54 GMT</td>
<td>C:\Program Files (x86)\Google...</td>
<td>6534</td>
<td>6328</td>
<td>a3e2a02f5e241f1s5b...</td>
<td>705234646419f...</td>
</tr>
</tbody>
</table>
Honeypot Detected Malicious Scan

- 3 Unique Processes
- 10 Rare Processes
- 100 Common Processes
- 75 Very Common Processes
Endpoint bos-t431s-2053.tor.rapid7.com ran malicious processs dropper.exe

Time: 2:20 PM 01/25/16 to 2:36 PM 01/25/16
User: Flora Page
Asset: bos-t567-6100.tor.razor.com
IP: 203.115.183.40
Results for 203.115.183.40 across all available endpoints

<table>
<thead>
<tr>
<th>timestamp</th>
<th>process name</th>
<th>common name</th>
<th>path</th>
<th>host name</th>
<th>host</th>
<th>fwd IP address</th>
<th>service ID</th>
<th>User ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015-10-30 22:24:22</td>
<td>svchost.exe</td>
<td>trojan virus</td>
<td>C:\WINNT\system32\svchost.exe</td>
<td>box-77-698.torazor.com</td>
<td>aas.heroeapp.com</td>
<td>203.115.183.40</td>
<td>2356</td>
<td>brodon</td>
</tr>
<tr>
<td>2015-10-30 22:24:22</td>
<td>svchost.exe</td>
<td>trojan virus</td>
<td>C:\WINNT\system32\svchost.exe</td>
<td>box-02-4215.torazor.com</td>
<td>aas.heroeapp.com</td>
<td>203.115.183.40</td>
<td>2356</td>
<td>lcortes</td>
</tr>
<tr>
<td>2015-10-30 22:24:22</td>
<td>svchost.exe</td>
<td>trojan virus</td>
<td>C:\WINNT\system32\svchost.exe</td>
<td>box-02-4215.torazor.com</td>
<td>aas.heroeapp.com</td>
<td>203.115.183.40</td>
<td>2356</td>
<td>mfrost</td>
</tr>
<tr>
<td>2015-10-30 22:24:22</td>
<td>svchost.exe</td>
<td>trojan virus</td>
<td>C:\WINNT\system32\svchost.exe</td>
<td>box-02-4215.torazor.com</td>
<td>aas.heroeapp.com</td>
<td>203.115.183.40</td>
<td>2356</td>
<td>lcortes</td>
</tr>
<tr>
<td>2015-10-30 22:24:22</td>
<td>svchost.exe</td>
<td>trojan virus</td>
<td>C:\WINNT\system32\svchost.exe</td>
<td>box-02-4215.torazor.com</td>
<td>aas.heroeapp.com</td>
<td>203.115.183.40</td>
<td>2356</td>
<td>mfrost</td>
</tr>
<tr>
<td>2015-10-30 22:24:22</td>
<td>svchost.exe</td>
<td>trojan virus</td>
<td>C:\WINNT\system32\svchost.exe</td>
<td>box-02-4215.torazor.com</td>
<td>aas.heroeapp.com</td>
<td>203.115.183.40</td>
<td>2356</td>
<td>lcortes</td>
</tr>
<tr>
<td>2015-10-30 22:24:22</td>
<td>svchost.exe</td>
<td>trojan virus</td>
<td>C:\WINNT\system32\svchost.exe</td>
<td>box-02-4215.torazor.com</td>
<td>aas.heroeapp.com</td>
<td>203.115.183.40</td>
<td>2356</td>
<td>mfrost</td>
</tr>
<tr>
<td>2015-10-30 22:24:22</td>
<td>svchost.exe</td>
<td>trojan virus</td>
<td>C:\WINNT\system32\svchost.exe</td>
<td>box-02-4215.torazor.com</td>
<td>aas.heroeapp.com</td>
<td>203.115.183.40</td>
<td>2356</td>
<td>lcortes</td>
</tr>
<tr>
<td>2015-10-30 22:24:22</td>
<td>svchost.exe</td>
<td>trojan virus</td>
<td>C:\WINNT\system32\svchost.exe</td>
<td>box-02-4215.torazor.com</td>
<td>aas.heroeapp.com</td>
<td>203.115.183.40</td>
<td>2356</td>
<td>mfrost</td>
</tr>
<tr>
<td>2015-10-30 22:24:22</td>
<td>svchost.exe</td>
<td>trojan virus</td>
<td>C:\WINNT\system32\svchost.exe</td>
<td>box-02-4215.torazor.com</td>
<td>aas.heroeapp.com</td>
<td>203.115.183.40</td>
<td>2356</td>
<td>lcortes</td>
</tr>
</tbody>
</table>
Honeypot Detected Malicious Scan

- **02:02PM**
  - Malware detected: dropper.exe
  - Outbound Network Connection to China
  - User: Martha Green
  - IP: 1976-2461.tor.razor.com

- **02:20PM**
  - Honeypot detected malicious scan
  - User: Martha Green attempted 032 connections to 4 honeypots

- **03:55AM**
  - Malware detected: dropper.exe
  - Outbound Network Connection to China
  - User: Flora Page
  - IP: 1234-4617.tor.razor.com

- **04:22PM**
  - New asset accessed
  - User: Martha Green
  - IP: 1234-6100.tor.razor.com

- **04:30PM**
  - Malware detected: dropper.exe
  - Outbound Network Connection to China
  - User: Marion Fox
  - IP: 1812-6100.tor.razor.com

- **05:23AM**
  - New asset accessed
  - User: Martha Green
  - IP: 1234-6100.tor.razor.com

- **05:58PM**
  - Malware detected: dropper.exe
  - Outbound Network Connection to China
  - User: Lance Castro
  - IP: 1976-2461.tor.razor.com

- **04:18PM**
  - New asset accessed
  - User: Bob Robson
  - IP: 1234-6100.tor.razor.com
Customer Success with InsightIDR

Pioneer

“I like the log search and the ability to bring in logs from anywhere. Not just from supported sources, but any source.”

Chad Kliewer
Information Security Officer

BLACKLINE

“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

VISIER

“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

LIBERTY WINES

“InsightIDR is a great system. It gives you that warm feeling inside by catching any suspicious behavior on the network months before you’d otherwise discover it…”

Tom Brown
IT Manager

“InsightIDR arms my team of incident investigators with the exact information they need to make smarter decisions.”

Fortune 500 Real Estate Investment Trust
Correlating it all Together

1. Focus on earlier detection in the chain
2. Avoid duplications per step to maximize investments
3. Identify current gaps in your program
4. Prioritize high-probability attacks (e.g. creds)
THANK YOU!

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

- Network Events
- Real-Time Endpoint Events
- Intruder Traps
- Applications
- Existing Security Solutions, Alerts, and Events
- Remote Endpoints
- On-Premise Insight Collectors
- SSL
- Enterprise Cloud Apps
- Mobile Devices
- Security Team

InsightIDR Attacker Analytics Platform

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

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

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
Metasploït
Nexpose
Sophos Enduser Protection
Symantec Endpoint Protection

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

Insight Platform Event Sources Cont.