Modern Security for Modern Threats
Defending Today’s Hybrid IT Environment

Eldon Sprickerhoff
Founder and Chief Innovation Officer

July 29 - 31, 2019 | Dallas, Texas
eSentire at a Glance

Created the Managed Detection and Response (MDR) category

Proprietary platform driven by data analytics and AI/ML drives scalable margins, SOC efficiencies and extensible platform potential

- 450+ employees
- 650+ mid-market customers across 40+ countries
- 5 facilities with new Waterloo HQ

AI Awards:
- 2017
- 2018
Digital Evolution, Dynamic Threats
Expanding attack surface
- Endpoint
- Network
- Cloud and SaaS
- Users
- Mobile Devices
- IoT

Motivated and well-funded threat actors
- Malicious Insiders
- Terrorists
- Organized Crime
- Hacktvists
- Nation States

Creative and sophisticated attacks
- Spear-phishing
- Custom Malware
- Zero-Day Exploits
- Social Engineering
- Physical Compromise

Well-established cybercrime economy
- Credit Card Number, Email Accounts (per 1000)
  - 50¢ to $20
- Cloud Accounts
  - $7 to $8
- Custom Malware
  - Up to $3,500
- Nation States
  - Up to $50 per Healthcare Record
- Social Engineering
  - Up to $50
- Physical Compromise
  - Up to $1,000/day
- DDoS Attack
The Anatomy of a Cyberattack

**Attacker**

- **Infiltration**
  - **Spearphishing**
    - Email Attachment | Malicious URL
  - **External scans**
    - Vulnerabilities | Weak Credentials | SQLi
  - **Physical**
    - USB Drive | CDR | Laptop | Mobile | WIFI
  - **Opportunistic**
    - Drive-by Download

- **Establish Beach Head**
  - **Establish C2 Channel**
  - **Updates and Instructions**

- **Escalation/Extension/Expansion/Penetration**

- **Lateral Analysis**
  - To ‘Learn About You’

- **Lateral Access**
  - To ‘Secret Sauce’

**Local Methods**
- Key Logging
- DOC/Mailbox/Text Search
- Password Cracking/SAM
- User/Group Accounts
- Poorly Protected Shares
- ARP Hijack/MITM
- Poorly Patched Systems
- Broad Scanning

**Network Methods**

**Data Exfiltration**

**Ongoing education**

- **Establish Beach Head**
- **Spearphishing**
- **External scans**
- **Physical**
- **Opportunistic**

- **Lateral Analysis**
  - To ‘Learn About You’

- **Lateral Access**
  - To ‘Secret Sauce’

**Local Methods**
- Key Logging
- DOC/Mailbox/Text Search
- Password Cracking/SAM
- User/Group Accounts
- Poorly Protected Shares
- ARP Hijack/MITM
- Poorly Patched Systems
- Broad Scanning

**Network Methods**

**Data Exfiltration**

**Ongoing education**
Adversaries Hunt Their Prey

Oppportunistic  Industry Focused  Targeted
Rapid Detection Limits Costs
Operational Disruption | Reputational Damage | Lost Business | Share Price Decline | Executive Lost Jobs

- $750 compromised user account
- $25K compromised business system
- $122K compromised data / breach

- 10% share price decline 100+ days to recover
- $500K lost billable hours
- $1.9M stolen 24 hours after VC funding
- $24M regulatory fines HIPAA / OCR
The Reality of Current Security Approaches

What many think is happening

What is actually happening
What you can see is only a small part of the picture

It’s the things you can’t see that pose the greatest risk
Partial Visibility, Limited Response

10,000 Daily Alerts

500 Alerts Managed
Full Spectrum Detection, Immediate Response

Distributed IT Environment

Full Threat Visibility

Integrated Response

MACHINE LEARNING
SYSTEM LOGS
CLOUD SERVICES
ENDPOINTS
NETWORK
Living Off the Land: Finding the Signal in the Noise

Attackers use your own tools like PowerShell against you. This practice blends adversary activities with common administrative work, leaving fewer detectable artifacts—it’s the perfect camouflage.

The Cyber Kill Chain

- Planning
- Access
- Recon
- Collection
- Exfiltration

Detectable patterns to distinguish legitimate from malicious
### Reduce 1,000s of Signals to a Few Threats for Human Investigation

<table>
<thead>
<tr>
<th>HOSTS</th>
<th>BEHAVIORS</th>
<th>LIFECYCLE STAGES</th>
<th>THREAT CASES</th>
<th>ANALYST INVESTIGATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>10-1,000 of hosts in distributed environment</td>
<td>Models normal for each core adversary behavior to look for unusual activity</td>
<td>Blend behaviors into campaign stages to find hosts that exhibit high-levels of renaissance, collection or data exfiltration</td>
<td>Look for connections between high-risk activities</td>
<td></td>
</tr>
</tbody>
</table>

- **Models normal for each core adversary behavior to look for unusual activity.**
- **Blend behaviors into campaign stages to find hosts that exhibit high-levels of renaissance, collection or data exfiltration.**
- **Look for connections between high-risk activities.**
Artificial Intelligence: Extensible Platform and Approach to Hunting

- **Endpoints** (EDR+NGAV)
- **Network** (NGFW+IDS/IPS)
- **Cloud + SIEM Log Aggregation**

**Behavior Discovery**
- Build RESULTS
- Model Evaluation
- Data Exploration
- Add CONTEXT
- Iterate MODELS
- Aggregate DATA

**Security Operations**

Human experts who evaluate forensics evidence and provide true positive/false positive feedback.
Leveraging Machine Learning

```powershell
"(("bHqX7MnbNq+bNqsbNq+bN'+'gabNq+bNq0abNq+bNqsd bNq+bNq=
&'+'ZxpzbNq+bNqsbNq+bNq+bNq+ZxbNq+bNq'+"bNq+bNqgbNq+bN'+'Nq2xpNq+bNq+bNq2xpNq+bNqw'+'-obbNq+bNqjocZxpNb'+
'q+bNq+ZxpzZxp) bNq+bNqandbNq+bNqkbNq+bNqN!'+'X7MvKqN!'+'bNqYubNq+bNq bNq+bNq=
LbNq+bNq+NqgbNq+bNqnbNq+bNqzNk!b'+'Nq+bNq+ZxpzZxp+bNq'+'bNq2bNq+bNqxpNq+bNq
-ojbNq+bNqetbNq+bNq2bNq+bNqgbNq+bNqgbNq+bNq)
```

Leveraging Machine Learning

Rules were either too specific or easily bypassed using a number of methods including:

- Encoding
Leveraging Machine Learning

Rules were either too specific or easily bypassed using a number of methods including:

- Encoding
- Obfuscation

```cpp
InvoKE-eXPresSiOn ( ( (24 , 50, 53 , 56, 65 , 72, 73, 69 ,'6f' , '6e', 54 ,61,62 , '6c', 65 ,'2e' , 50,53,56, 65 ,72,73 , 69 , '6f' ,'6e ' )|% {{[char]([cOnVeRt]::toINT16(( [StrING]$_),16 )) }}-JOIN ''
```
Leveraging Machine Learning

Rules were either too specific or easily bypassed using a number of methods including:

- Encoding
- Obfuscation
- Encryption
Leveraging Machine Learning

Rules were either too specific or easily bypassed using a number of methods including:

- Encoding
- Obfuscation
- Encryption
- Compression
Leveraging Machine Learning

Rules were either too specific or easily bypassed using a number of methods including:

- Encoding
- Obfuscation
- Encryption
- Compression

- Most of these events are easily identified manually but do not work well being detected by rules
- There has to be a better way. It started with a very specific requirement (don’t boil the ocean)
Leveraging Machine Learning

- High level properties such as length, type of characters and presence of certain terms in the event is used to identify malicious from benign

- Here is a module commonly used in attacks but by itself it isn’t malicious

InvoKE-eXPResSiOn ( ( (24 , 50, 53 , 56 , 65 , 72, 73, 69,'6f' , '6e' , 54 ,61,62 , '6c' , 65 , '2e' , 50,53,56, 65 ,72,73 , 69 , '6f' , '6e' )|% {([char]([cOnVeRt]:toINT16{ [StrINg]$ _),16 ))})))-JOIN '' )
Leveraging Machine Learning

• High level properties such as length, type of characters and presence of certain terms in the event is used to identify malicious from benign

• Here is a module commonly used in attacks but by itself it isn’t malicious

• A large quantity of numbers which is not typical

```java
InvoKE-eXPresSiOn ( \{(24, 50, 53, 56, 65, 72, 73, 69, '6f', '6e', 54, 61, 62, '6c', 65, '2e', 50, 53, 56, 65, 72, 73, 69, '6f', '6e')\} % {{[char]([cOnVeRt]::toIN16([ [StrING]%_),16 ) )} ))--JOIN '' )
```
Probably bad:

wnsamaneh.iGhz+Ghzr/xq4IW+4I''+wn/ , h4IW+4Iwt4IW+4Iwt4IGhz+Ghzw4Iwp:4'+'Iw+4IW//
r4IW+4Iwhis4IW+4IW'+i'rsC4IW+4I''+wGhz+Ghzlasses4IWw4IW, 4IW+4Iwcom4IW''+4IW/q [...]"

Probably not bad:

"C:\windows\System32\WindowsPowerShell\v1.0\powershell.exe" "-Command" "if((Get- ExecutionPolicy ) -ne 'AllSigned') { Set-ExecutionPolicy -Scope Process Bypass }; & 'D:\srroberts2-Backup-11-13-2017\restore_from_home_drive.ps1'"
Leveraging Machine Learning

- Enlist experts to train a machine learning model with the hopes of encoding domain expertise:
  - Locked them in a room
  - Label thousands of PowerShell event samples as “suspicious” or “benign”
  - They calculated the features of each event such as the length, a score that describes character frequency analysis and similarity of known good samples, and developed a term
  - Fed the labeled samples into a machine learning algorithm
  - Used the algorithm to predict the labels of previously unseen samples
  - Discovered a very high accuracy score in the untrained test set of data
  - Applied the algorithm to PowerShell activity on the command line with a similar level of accuracy
Applying machine learning is an efficient and effective way to generalize the brittle rule sets we were using.

Utilizing ML allows us to leverage data from all customers and internally generated samples in order to train a global model used for prediction.

Version 1 was in place early 2017 and continually updated and enhanced throughout the year.
Maximize security analyst efficiency through automated event suppression

Augment detection efficacy over out-of-box vendor capabilities

1. Record all executions of PowerShell using endpoint telemetry
2. Upload telemetry data to cloud database for analysis
3. Advanced analytics used to identify signs of unusual activity, including machine learning to identify signs of obfuscation

Detection Efficacy

+28%
True Positive Detection

Orchestration Efficiency

99.97%
False Positive Reduction

Maximize security analyst efficiency through automated event suppression

Blue Steel Statistics

Augment detection efficacy over out-of-box vendor capabilities
Investigation reveals PsExec connection back to another compromised endpoint used as a staging point to conduct reconnaissance and launch attacks inside the network.

75% of compromised accounts and systems identified and contained

Investigation reveals modified OWA script to siphon user credentials, exfiltrated OWA accounts identified

Nearly all compromised systems discovered

Investigation reveals primary target was specific employee using zero-day malware, persistent mechanisms discovered

Investigators work with client providing forensic materials, removing persistent mechanisms, remediation concludes

0:00 Discovers compromised workstation using PsExec to deploy malware. Alert sent, host isolated

7:00 Investigation reveals PsExec connection back to another compromised endpoint used as a staging point to conduct reconnaissance and launch attacks inside the network.

11:00 12:00

Investigation reveals modified OWA script to siphon user credentials, exfiltrated OWA accounts identified

24:00

Investigation reveals primary target was specific employee using zero-day malware, persistent mechanisms discovered

72:00

Law Firm | eSentire Incident Investigation Timeline

Case Study: Detecting a Nation State Attack
Threat Intelligence and Advanced Threat Analytics Teams

• Responsible for combing through the billions of signals ingested by Security Operations Center (SOC) each year and investigating emergent threats

• Research manifests in two ways:
  • Feeds directly into SOC and engineering pipelines to help proactively protect customers against the latest threats
  • Knowledge sharing with the security community via security advisories, blog posts and threat reports
### Emotet Lures

#### Maldoc Timecourse

<table>
<thead>
<tr>
<th>Doc Type</th>
<th>Jan 1</th>
<th>Feb 1</th>
<th>Mar 1</th>
<th>Apr 1</th>
<th>May 1</th>
<th>Jun 1</th>
<th>Jul 1</th>
<th>Aug 1</th>
<th>Sep 1</th>
<th>Oct 1</th>
<th>Nov 1</th>
<th>Dec 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fax</td>
<td></td>
<td></td>
<td>1</td>
<td>5</td>
<td>8</td>
<td>7</td>
<td>7</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>IRS Form</td>
<td>2</td>
<td>2</td>
<td>3</td>
<td>5</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Shipping</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

- Independence Day
- Greeting Card
- Christmas Card
- Wire Request
- Bank Form
- Excel File
- Executable
- Invoice
- Unspecified
- Word Doc
Resources

Custom Risk Index Report: riskindex.esentire.com
Resource Library: www.esentire.com/resource-library
  • Includes on-demand webinars and podcasts
Blogs: www.esentire.com/blog
  • Reddit's r/tennis Serves up a RIG'd Wimbledon Stream: streaming the big game can bring big pain to your organization
Reddit Serving Up Exploit Kits

• An employee at a customer went looking for a stream to watch Wimbledon at their desk
• The r/Tennis subreddit (and top Google search result) linked to a site that served up a RIG exploit kit
• Desire to not miss the “big game” can override common sense security practices
  • Be prepared for major events like the World Cup and Olympic
Thank You

eldon.sprickerhoff@esentire.com
Twitter: @TheEldon