esentire®

INTECH

Ransomware: Its Impact On Your Business

Eldon Sprickerhoff, Chief Security Strategist
eldon.sprickerhoff@esentire.com
@TheEldon

March 9th 2017

FOUNDED
2001

CUSTOMERS
600+

EMPLOYEES
290

esentire®

PROVEN

CYBERSECURITY

FOR MID-SIZED ENTERPRISE

YOY GROWTH
60%

CUSTOMER RETENTION
97%

CLIENT AUM PROTECTED
$3.2T

CAMBRIDGE | NEW YORK | LONDON | CORK

CURRENT CYBER ATTACKS

Ransomware Failure Vectors: Technical, Process/Policy, Training

- The firm's upstream email (SMTP) provider did not scan attachments for malicious content.
- The firm's next-generation firewall did not identify the attachment as malicious (or questionable) content.
- The firm's local email system (e.g. Microsoft Exchange) did not scan attachments for malicious content.
- The end user was not sufficiently trained to identify a phishing email (with malicious content).
- The user's workstation (or mobile device) did not flag the malicious content (through anti-virus or other endpoint protection methodology).
- If the delivery vector was a macro hidden within an Office document (the most common delivery method), macros were enabled within Office (or the user was enticed to enable them manually).
- (Otherwise) The user's workstation had vulnerable software installed (a gap in patching/process).
- The user's workstation did not have restrictions placed on the execution of downloaded content.
- The firm's next-generation firewall and/or Intrusion Prevention system did not recognize and/or block the command-and-control traffic (including key generation) of the malicious code (particularly important if the remote IP addresses were previously known to be bad).
- The firm did not detect (through filesystem analysis) that a specific user was modifying a large number of files rapidly.
- Depending on how many files were affected by the infected endpoint, it is a possibility that the end user had more access than they necessarily needed to execute their job.
- During the restore process, some newer files might have been not backed up due to a gap in backup rigor.

esentire® MANAGED DETECTION & RESPONSE

Detection and **Prevention** Technology

- Real-time detection and prevention of known attacks
- Signal suspicious network behavior to detect unknown attacks

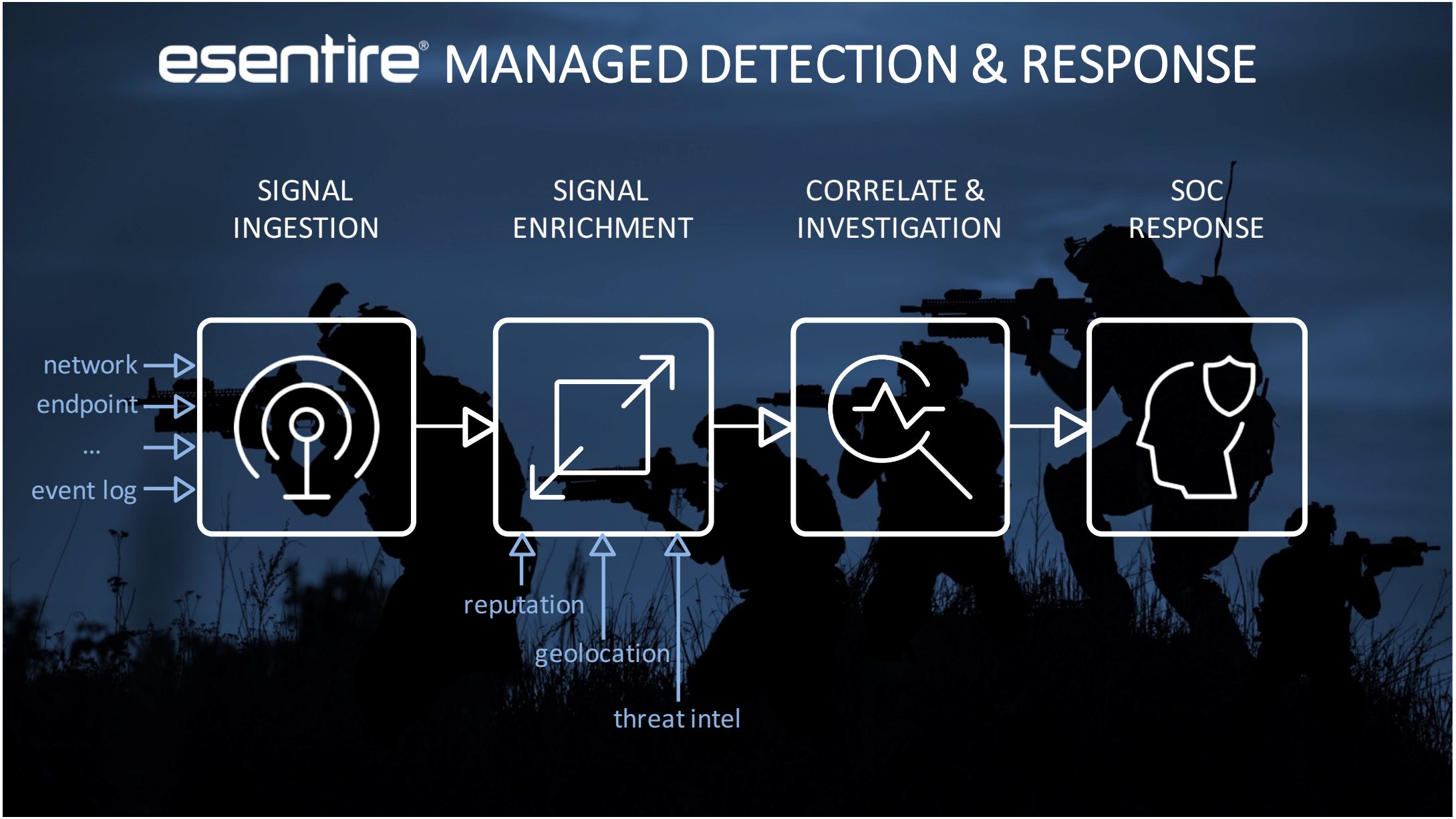
24X7 Human **Monitoring** and **Hunting**

- Real-time forensics via 24X7 Global SOCs
- Add insights to raw signals
- Quickly determine if weird normal or weird bad

Intervention & Response

- Contain Threat
- Escalate to customer
- Remediate

esentire® MANAGED DETECTION & RESPONSE



LAW FIRM

DENIAL
OF SERVICE
CASE FILE SHARE

RANSOMWARE

7:43AM
AMP BLOCKS 1st 87.exe
DOWNLOADED FROM 2ND IP

7:44AM
TESLACRYPT BEACONS
TO CNC SERVER

7:54AM
SOC ALERTS ON INFECTION
AND BLOCKS TRAFFIC

8:30AM
INFECTED HOST
ISOLATED/MITIGATED

“Am I doing enough to stop ransomware?”

eSentire Cybersecurity Response
Ransomware Defense Matrix

esentire®

Human (Wetware) Defense Mechanisms

Minimum	Intermediate	Advanced
✓ Staff training to aid in the proactive detection of malicious content (online, videos, posters). ✓ Annual phishing testing performed for employees. ✓ Create Incident Response plans to prepare for an eventual incident.	✓ Monthly phishing testing performed for employees. ✓ Quarterly review of Incident Response plans. ✓ Investigate a Continuous Monitoring/embedded Incident Response methodology.	✓ Regular micro-training (daily) to ensure ongoing mindshare in defending against malicious content.

Pragmatic Security Event Management - RANSOMWARE

esentire

PHASE 0 PREPARATION

Ensure all systems are up-to-date

- **Workstations, Servers (including internal and DMZ)**
  - *Patching, where possible.*
  - *Antivirus, Anti-Exploit (e.g. EMET), Application Whitelisting (e.g. AppLocker)*
  - *Restrict downloading of applications and payloads (Network Application Control)*
- **Mobile Devices**
  - *MDM (Patching, Restricting Applications, Downloads)*

Ensure backups of critical systems and data are successful and available

- **Test regularly for content accuracy**
- **Back up important data offline**

Restrict Access

- **Enforce "least-privilege" access throughout filesystems**
- **Segment network**
  - *Restrict workstation-to- workstation access*
  - *Utilize jump box for important and critical parts of network*
- **Log access attempts to shares that get denied (early signs of infestation)**

Reduce Susceptibility Footprint

- **Reduce inbound vectors (e.g. personal email)**
- **Disable macros within Microsoft Office if not needed**
- **Use Microsoft Viewer software if editing of Office documents is not needed for all tasks (especially when viewing suspect documents)**
- **Improve/Harden upstream SMTP attachment scanning and quarantine**
  - *Block .zip, .exe, .js, .html*
  - *PTR/SPF records for anti-spoofing protection*

Training

- **Inoculate skepticism in end-users**
  - *Security Awareness Training*
  - *Phishing test campaigns*
  - *Weekly reminders/ postings*

Alerting

- **Implement behavior-based alerting when a certain threshold of files are modified**
- **Implement a Continuous Monitoring/Embedded Incident Response methodology**

PHASE I DETECTION

Formal Initiation of Event

- **Note timestamp and method of discovery**
- **Identify "Patient(s) Zero"**
  - *External*
    - *FI*
  - *Workstation*
    - *Single or Multiple?*
  - *Server*
    - *Single or Multiple?*
  - *Mobile Device*
    - *Single or Multiple?*
  - *Accounts*
    - *Single or Multiple?*
  - *Blend of the above*

PHASE II CONFIRMATION / TRIAGE / ASSESSMENT

Initiate Event Data Cull if manpower permits, otherwise immediately move to PHASE III.

PHASE III MITIGATION / REMEDIATION / RESOLUTION

Contain

- **Is isolation possible?**
- **What is the impact of isolation?**
- **Is there a need for the BC/DR Plan to be put into effect?**
- **Method**
  - *Manual Disconnect*
    - *Cable*
    - *Wireless*
    - *Antenna Disable (mobile device)*
  - *Switch Port Disable*
  - *Wireless Controller Access Disable*

Identify

- **Breadth of the filesystem affected**
- **Impact and sensitivity of the files lost**

Analyze

- **Affected systems for possible multi-pronged/method attack**
- **Vestigial artifacts left on affected systems**
- **Network Indicators**
  - *Payload Transfer / Droppers*
  - *Command and Control Channels / Covert Channels*
  - *Data Loss/File Extrusion*

Eradicate

- **Implement IP blocks (on firewall) if deemed appropriate**
- **Alert staff to indicators derived from attack**

Recovery

- **Initiate file recovery**
- **Verify backups not affected**
  - *Check shadow copies (system restore)*
- **Wipe affected systems**
  - *if needed*
  - *when convenient*
  - *and analytics completed*

PHASE IV POST-INCIDENT

Confirm "All Clear" Event

- **Note timestamp for formal records**

Update and Secure Documentation

Root Cause Analysis

- **Present findings to management**

Enhance Response Capabilities

- **Present findings to management**

esentire®

DOWNLOAD from www.esentire.com:

1) Ransomware eBook
2) Ransomware Incident Response Framework
3) Managed Detection and Response Framework

Ann-Maree Maynard ann-maree.maynard@esentire.com +44 (0) 7718 258005
James Morgan james.morgan@esentire.com +44 (0) 7730 897846

WE DETECT THE CYBER THREATS THAT OTHER TECHNOLOGIES MISS