BLUE COAT

Security Empowers Business

FRESH FROM THE WAR ROOM

WHERE EXISTING SECURITY MEASURES FAIL

Dr. Felix Leder <felix.leder@bluecoat.com>

André Engel <andre.engel@bluecoat.com>

BUSINESS ASSURANCE TECHNOLOGY

Security and Policy Enforcement Center

SG & SG-VA
Web Security Service
WebFilter
SSL Visibility
Content Analysis
Malware Analysis
DLP
FW/IDS on X-Series

Mobility Empowerment Center

Mobile Device Security Service

Trusted Applications Center

Web App Reverse Proxy

Performance Center

MACH5
CacheFlow
PacketShaper

Resolution Center

Reporter SW
Hosted Reporting
Intelligence Center
Security Analytics Appliance with Threat Blades

BUSINESS ASSURANCE PLATFORM

- **Open Environment for Best-of-Breed Solutions**
- **Proxy-Based Architecture**
- **Global Cloud Infrastructure**
- **Threat, Web & Application Intelligence**
- **Scalable Virtualization Platform**
- **Rich Security Analytics**

BLUE COAT

LEADING CUSTOMER FRANCHISE

86% of FORTUNE Global 500 Companies

JPMorganChase
SAMSUNG
SONY
Abbott
A Promise for Life
Coca-Cola
P&G
BNP PARIBAS

Over 30% of FORTUNE Global 10K Companies

THOMSON REUTERS
RadioShack.
WIPRO
SWATCH GROUP
NYSE Euronext
Carlsberg
KGK
adidas
Kanematsu KGK
TIFFANY & CO.

16 Largest Service Providers in the World

at&t
france telecom
Telstra
中国移动通信
CHINA MOBILE
américa móvil
TELECOM ITALIA
verizon
Deutsche Telekom

Worldwide Government Organizations

HM TREASURY
Government of Canada

Over 15,000 highly satisfied customers spanning major enterprises worldwide

ADVANCED PERSISTENT THREAT

“Let me think who is the target?”

Firewalls

“Well its YOU ….still YOU”

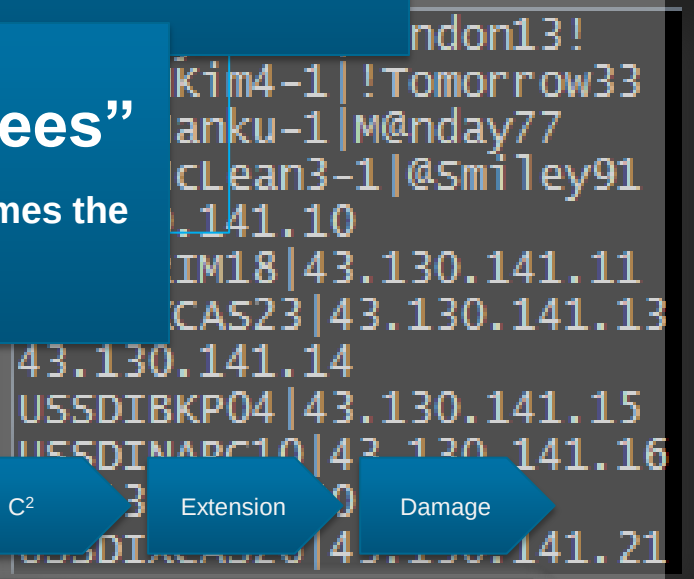
“Your company assets”

“YOUR Employees”

“social engineering becomes the easy way “

“YOUR Customers”

“breach you as the weakest Link”



Recon | We | nce | C² | Extension | Damage

SOCIAL NETWORK

- **Most popular hash tag ever**
  - 6500 time tweeted in 1 minute
  - 3.4 million tweet in just one 24 hour period

- **Miscreant say “Jesus Charlie too”**
  - Exploited #JesuisCharlie hash tag
  - Used RAT Dark Comet

PRINTERS

- Internally a computer:
  - CPU, RAM (you can buy more)
  - Ethernet ports / WiFi
  - Hard disk
- Hard disk
  - Often stores the full print history
    - Public announcements
    - Contracts
    - Financial numbers
    - Strictly confidential documents
  - "Smart printers" may contain original document type

- **Do you have anti-virus on your printer?**
- **When did you last update your printer's firmware?**

MOBILE DEVICES

- **BYOD <u>is</u> happening**
  - Are you sure there no private wifi hotspots on your premises?

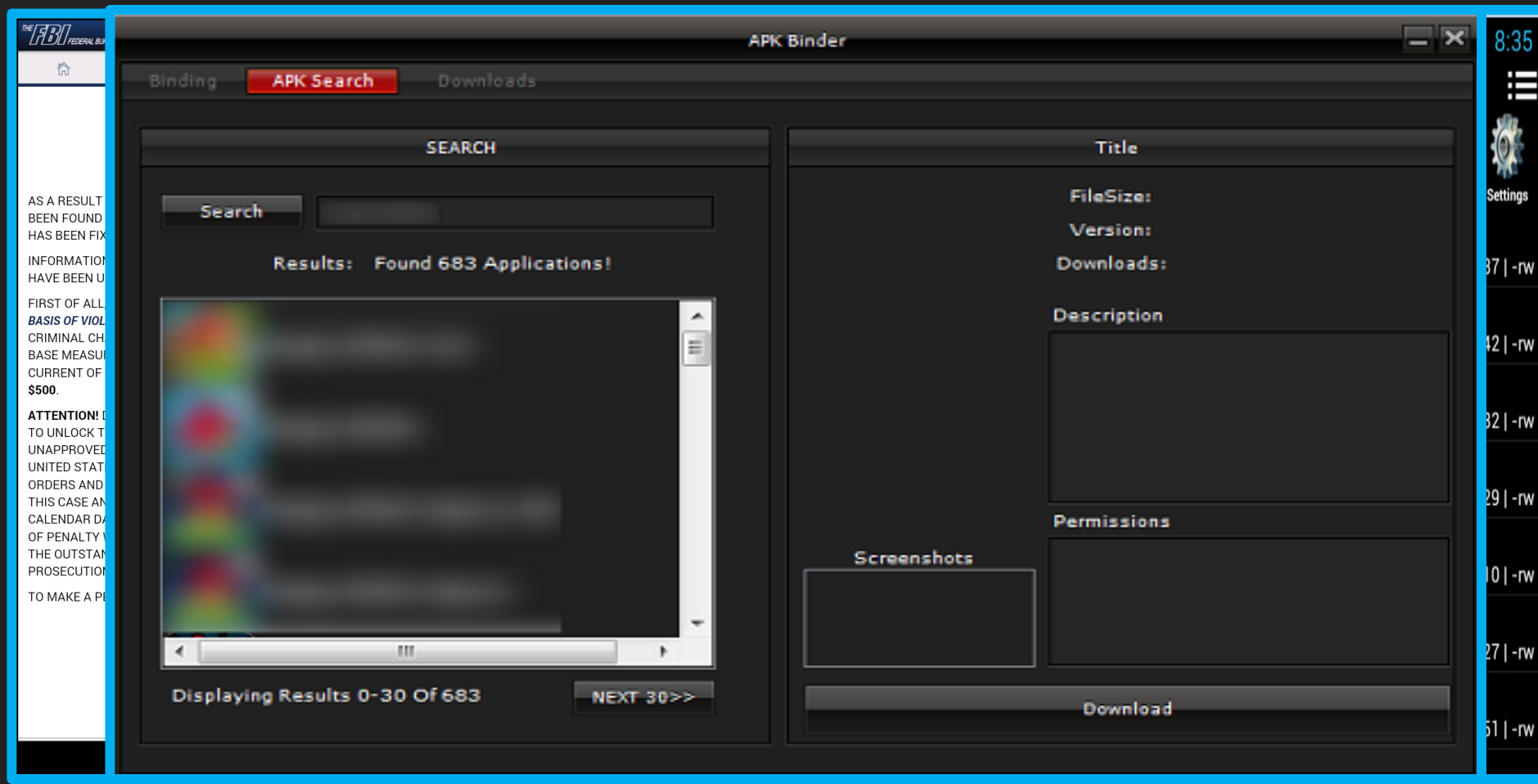
Access to emails, documents, contacts

- **Device has sensors**
  - Microphone
  - Camera
  - GPS
  - Light sensor
  - Accelerometer

“I HAVE NOTHING TO HIDE”

… but maybe something to lose

AS EASY AS 1, 2, 3



ANDROID “DEVICES”

- Android is not limited to phones/tablets

- Fridges
- Watches/ goggles / wearable’
- …
- Full Internet Connectivity
- Known bugs/vulnerabilities

- Every product has bugs:
  - Depends on 3rd party?
  - Google is not always patching (Webview vulnerability < Kitkat

HOW TO PROTECT?

Antivirus exists for mobile devices

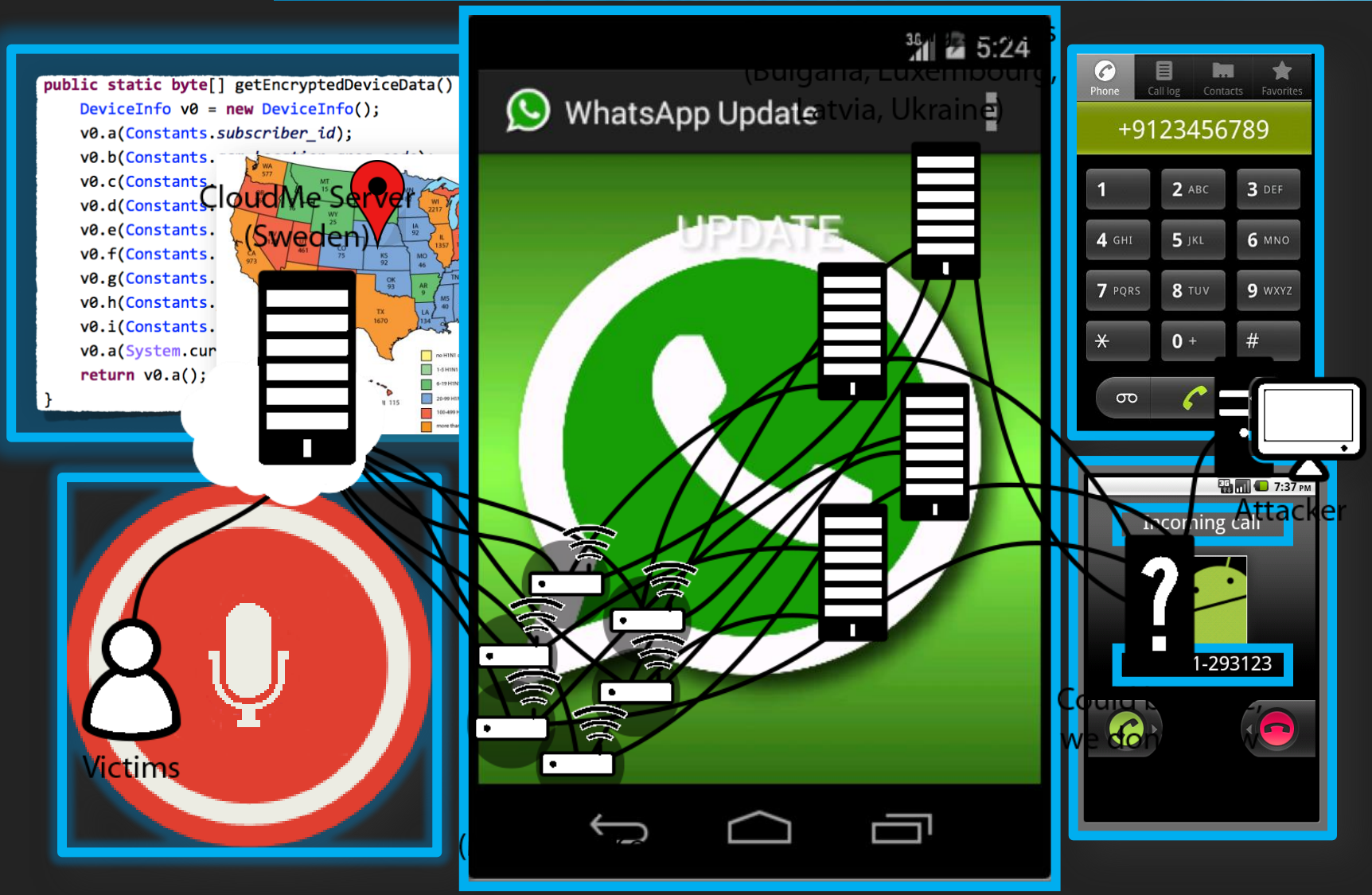
- Impossible for deep analysis without jail-breaking the phone (same security for everybody is a good concept)
- Only sees threats on the surface
- Usually limited to **known** threats

Attackers can use exploits and undermine security

➔ **Asymmetric scenario**

Old devices are usually not updated by the vendor

WAR STORY – TARGETTING EXECUTIVES, POLITICIANS, MILITARY



ROUTERS

"Yeah we have ANTIVIRUS"

Hey what's about your egress points themselves?

"Yeah we have Firewalls"

The Honeynet PROJECT®

BLUE COAT

POINT OF SALES

Restaurant: Ordering, bookkeeping, billing

Sho

Lar

Hov

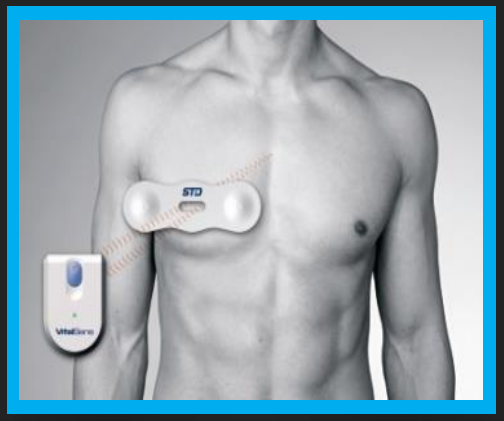
sec

```
aCorruptedRegex db 'corrupted regex pattern',0 ; DATA XREF: .text:00406B5B↑o
aCompliant_dat  db 'compliant.dat',0     ; DATA XREF: sub_40747F+135↑o
                                         ; sub_4079EB+EA↑o
                align 4
a?391091219DU00 db '\;?[3-9]{1}[0-9]{12,19}[D=\u0061][0-9]{10,30}\??',0
                                         ; DATA XREF: sub_40747F+D3↑o
                align 4
; char aExplorer_exe[]
aExplorer_exe   db 'explorer.exe',0      ; DATA XREF: sub_40773D+172↑o
                align 4
```

```
'\;?[3-9]{1}[0-9]{12,19}[D=\u0061][0-9]{10,30}\??',0
```

```
; char aMscorsvw_exe[]
aMscorsvw_exe   db 'mscorsvw.exe',0      ; DATA XREF: sub_40773D+144↑o
                align 4
; char aAlg_exe[]
aAlg_exe        db 'alg.exe',0           ; DATA XREF: sub_40773D+12D↑o
; char aWscntfy_exe[]
aWscntfy_exe    db 'wscntfy.exe',0       ; DATA XREF: sub_40773D+116↑o
; char aSpoolsv_exe[]
aSpoolsv_exe    db 'spoolsv.exe',0       ; DATA XREF: sub_40773D+FB↑o
; char aLsass_exe[]
aLsass_exe      db 'lsass.exe',0         ; DATA XREF: sub_40773D+C5↑o
```

ICS/ SCADA, MEDICAL, TELCO



PREVENTION

- **Prevention is required to remove the noise:**

- **Host antivirus**
  - Removes mass malware
  - As soon as something is on the endpoint, it is too late
  - Printers, fridges, mobile devices?

- **Network content analysis**
  - Stops before reaching endpoint
  - Can react on outgoing data
  - **What about SSL?**

PREVENTION TECHNOLOGIES

Whitelists:

- Works (if not compromised)
- Try once and never try again

Reputation / Big-data / Crowd

- You benefit from other incidents seen across the world in real-time
- Machine learning about “dirty” machines
- Blue Coat processes
  - ~300.000 files / 24h
  - ~6.000.000.000 URL ratings / 24h

BURNING QUESTION TODAY

~~How To Prevent A[illegible]ganisation From Suff[illegible]ecurity Breaches?~~

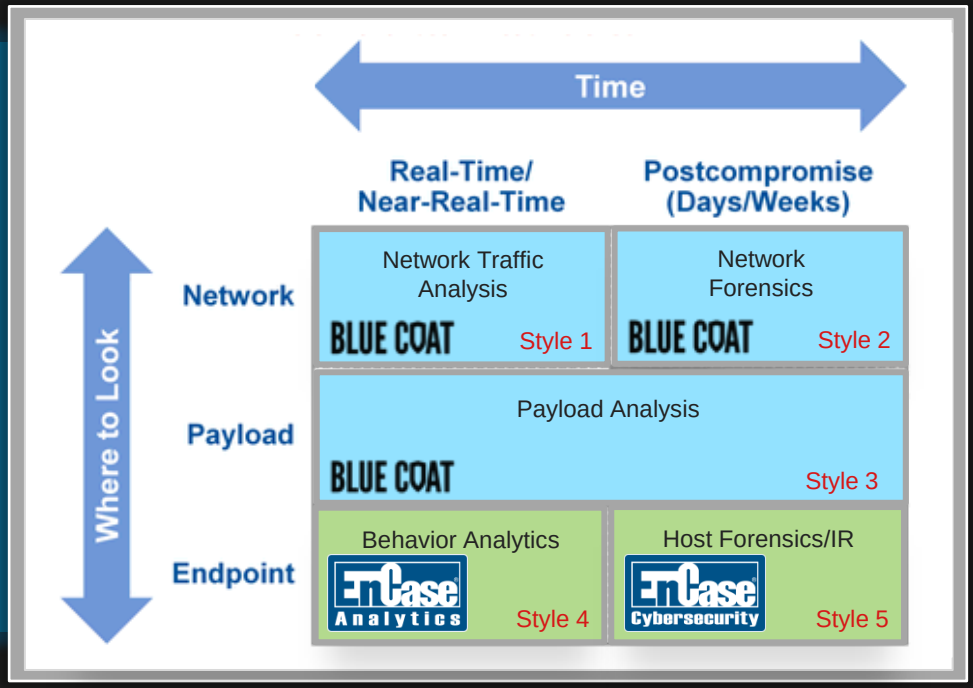
Security Breach will Happen !

Am I Ready To Respond?

NETWORK TO ENDPOINT VISIBILITY AND DEFENSE

Five Styles of Advanced Threat Defense

Built Upon
Full Network Visibility
+
Full Endpoint Visibility



CONT. RESPONSE – IN PRACTICE

Detect and react quickly, and learn

Big-data inside your organization?

- Data collection
- Correlation
- Are you able to track every step of intruders in your network?

Detection capabilities for unknown events – Sandboxing

- What about mobile?
- Really targeted malware is environment specific
- “Gold images” – customize to look like one of your real systems
- Really targeted can evade “generic behavioral detection”

LIFECYCLE DEFENSE

ASYMMETRY

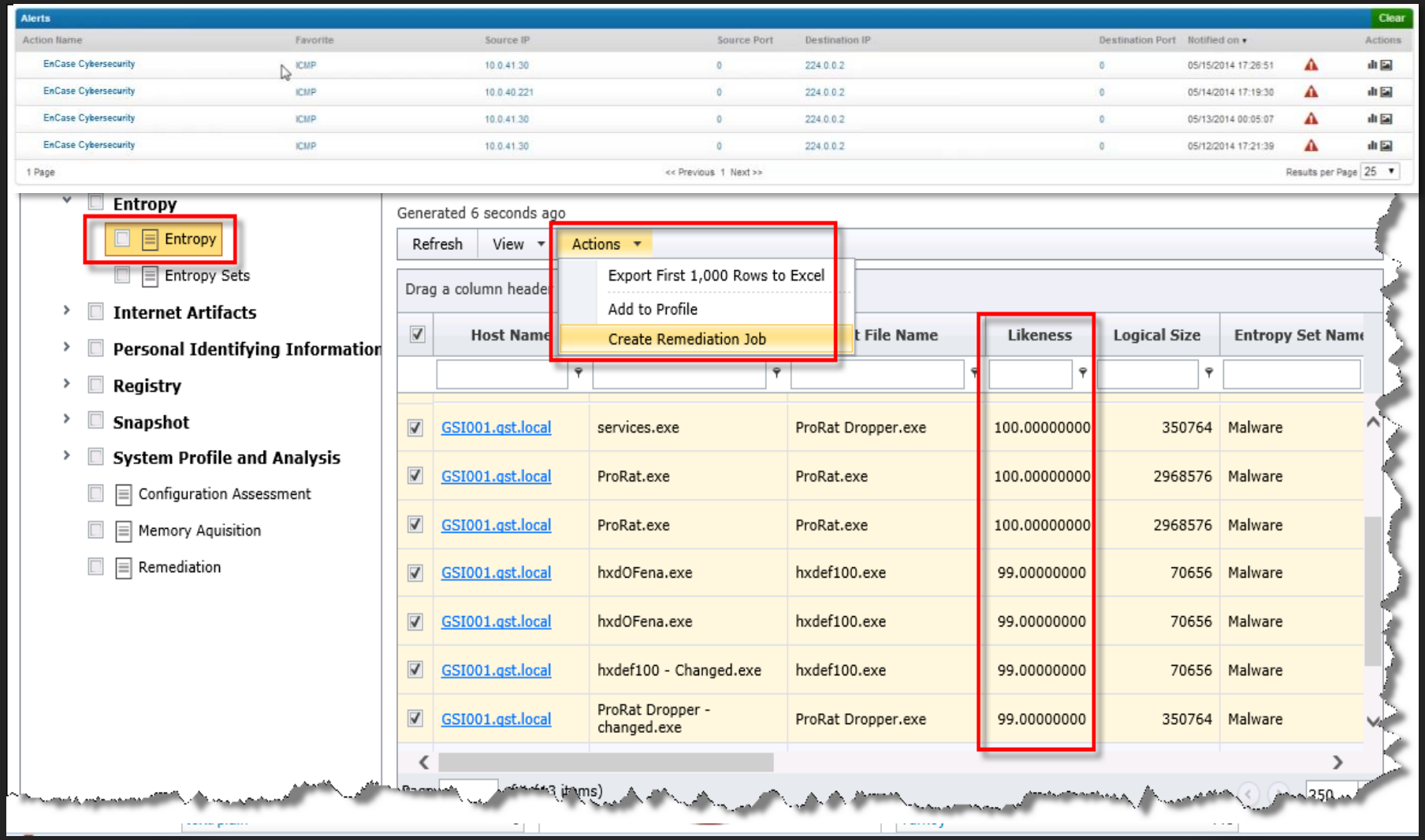
Attacker asymmetry:

Targeted to bypass general-purpose detections

Tripwires to turn tables:

- Spot irregular movements in network
- Custom patterns in sandboxes
- Bait files in sandboxes
- Set up “honeypots”

DON'T BE THE VICTIM



MESSAGE

APTs are Omni-present

You don’t control your infrastructure any longer

Continuous response (tools)

- Collect the right data
- Ability to correlate
- Learn

Tripwires are essential

BLUE COAT

Security Empowers Business

QUESTIONS?!

Felix Leder <felix.leder@bluecoat.com>
André Engel <andre.engel@bluecoat.com>