

**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>



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

LEADING CUSTOMER FRANCHISE

86% of FORTUNE
Global 500 Companies



SONY



Over 30% of FORTUNE
Global 10K Companies



THOMSON REUTERS RadioShack.



WIPRO SWATCH GROUP



NYSE Euronext.



Kanematsu KGK

TIFFANY & CO.

16 Largest Service
Providers in the World



at&t



france telecom



中国移动通信
CHINA MOBILE



américa
móvil



Deutsche
Telekom

Worldwide Government
Organizations



Government
of Canada

Over 15,000 highly satisfied customers
spanning major enterprises worldwide

“Let me think who is the target?”

Firewalls

“Well its YOUstill YOU”
“Your company assets”

“YOUR Employees”
“social engineering becomes the easy way “

“YOUR Customers”
“breach you as the weakest Link”

Recon

We

ence

C²

Extension

Damage

mediate

```
London13!  
Kim4-1|!Tomorrow33  
anku-1|M@nday77  
cLean3-1|@Smiley91  
.141.10  
IM18|43.130.141.11  
CA523|43.130.141.13  
43.130.141.14  
USSDIBKP04|43.130.141.15  
USSDINARC10|43.130.141.16  
USSDIACB20|43.130.141.21
```

▪ 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



- 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?**

- **BYOD is happening**
 - Are you sure there are no private wifi hotspots on your premises?

Access to emails, documents, contacts

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



... AS EASY AS ~~AS~~ ^{Something} to lose

The screenshot displays the 'APK Binder' application window. The interface is dark-themed and includes a sidebar on the left with a home icon and a settings gear icon. The main content area is divided into two panels. The left panel, titled 'SEARCH', contains a search input field with a 'Search' button and a message: 'Results: Found 683 Applications!'. Below this is a scrollable list of application results, with the first few items visible as colorful icons. At the bottom of this panel, it says 'Displaying Results 0-30 Of 683' and has a 'NEXT 30>>' button. The right panel, titled 'Title', shows details for a selected application, including 'FileSize:', 'Version:', 'Downloads:', and 'Description'. Below these are sections for 'Permissions' and 'Screenshots'. At the bottom of the right panel is a 'Download' button. The top of the window has tabs for 'Binding', 'APK Search', and 'Downloads'. The system tray on the right shows the time as 8:35 and a settings icon.

- 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)



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





**“Yeah we have
ANTIVIRUS”**

**Hey what's about
your egress points
themselves?**

**“Yeah we have
Firewalls”**



The HoneyNet
P R O J E C T®

Restaurant: Ordering bookkeeping billing

Show

Large

```
aCorruptedRegex db 'corrupted regex pattern',0 ; DATA XREF: .text:00406B5Bfo
aCompliant_dat db 'compliant.dat',0 ; DATA XREF: sub_40747F+135fo
; sub_4079EB+EAfo
align 4
a?391091219DU00 db '\;?[3-9]{1}[0-9]{12,19}[D=\u0061][0-9]{10,30}\??',0
; DATA XREF: sub_40747F+D3fo
align 4
; char aExplorer_exe[]
aExplorer_exe db 'explorer.exe',0 ; DATA XREF: sub_40773D+172fo
align 4
```

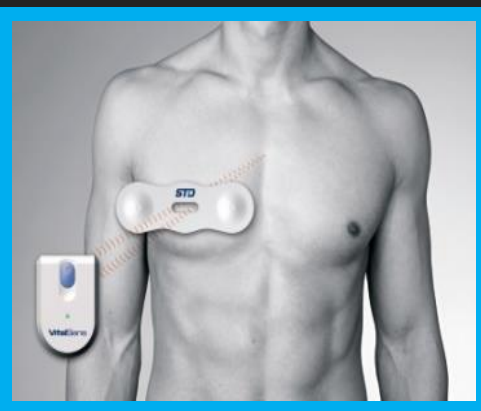
```
'\;?[3-9]{1}[0-9]{12,19}[D=\u0061][0-9]{10,30}\??',0
```

POC

How
sec

```
; char aMscorsvw_exe[]
aMscorsvw_exe db 'mscorsvw.exe',0 ; DATA XREF: sub_40773D+144fo
align 4
; char aAlg_exe[]
aAlg_exe db 'alg.exe',0 ; DATA XREF: sub_40773D+12Dfo
; char aWscntfy_exe[]
aWscntfy_exe db 'wscntfy.exe',0 ; DATA XREF: sub_40773D+116fo
; char aSpoolsv_exe[]
aSpoolsv_exe db 'spoolsv.exe',0 ; DATA XREF: sub_40773D+FBfo
; char aLsass_exe[]
aLsass_exe db 'lsass.exe',0 ; DATA XREF: sub_40773D+C5fo
```







- 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?**



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

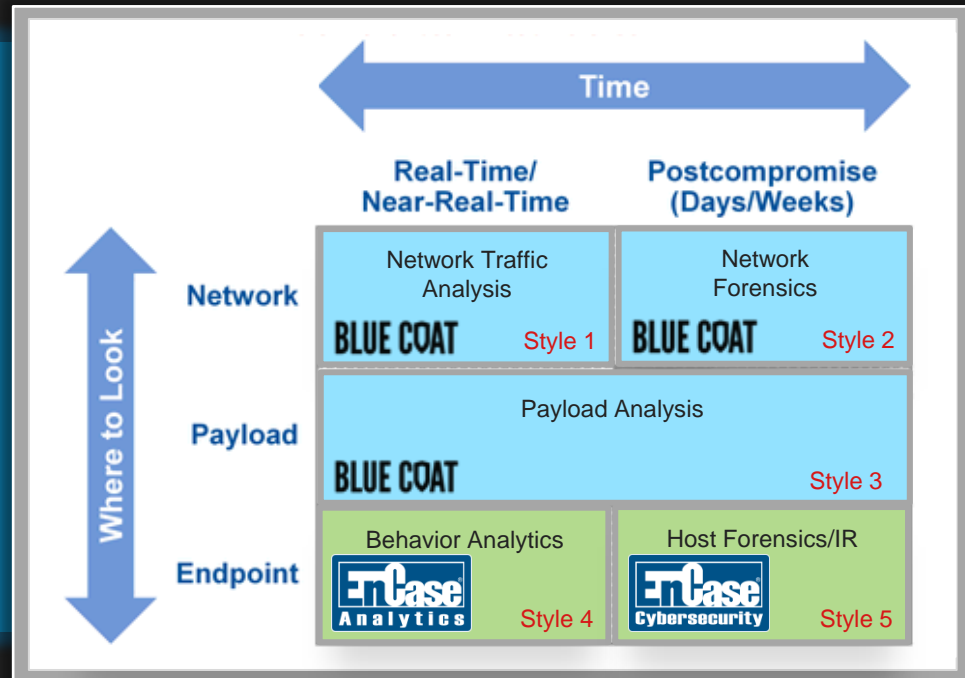
~~How To Prevent An Organisation
From Suffering Security Breaches?~~

Security Breach will Happen !

Am I Ready To Respond?

Five Styles of Advanced Threat Defense

Built Upon
Full Network Visibility
+
Full Endpoint Visibility



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”



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”

Alerts Clear

Action Name	Favorite	Source IP	Source Port	Destination IP	Destination Port	Notified on	Actions
EnCase Cybersecurity	ICMP	10.0.41.30	0	224.0.0.2	0	05/15/2014 17:26:51	
EnCase Cybersecurity	ICMP	10.0.40.221	0	224.0.0.2	0	05/14/2014 17:19:30	
EnCase Cybersecurity	ICMP	10.0.41.30	0	224.0.0.2	0	05/13/2014 00:05:07	
EnCase Cybersecurity	ICMP	10.0.41.30	0	224.0.0.2	0	05/12/2014 17:21:39	

1 Page << Previous 1 Next >> Results per Page 25

- ▼ Entropy
 - Entropy
 - Entropy Sets
- ▶ Internet Artifacts
- ▶ Personal Identifying Information
- ▶ Registry
- ▶ Snapshot
- ▶ System Profile and Analysis
 - Configuration Assessment
 - Memory Acquisition
 - Remediation

Generated 6 seconds ago

Refresh View **Actions**

Drag a column header

<input checked="" type="checkbox"/>	Host Name	File Name	Likeness	Logical Size	Entropy Set Name
<input checked="" type="checkbox"/>	GSI001.qst.local	services.exe	ProRat Dropper.exe	100.00000000	350764 Malware
<input checked="" type="checkbox"/>	GSI001.qst.local	ProRat.exe	ProRat.exe	100.00000000	2968576 Malware
<input checked="" type="checkbox"/>	GSI001.qst.local	ProRat.exe	ProRat.exe	100.00000000	2968576 Malware
<input checked="" type="checkbox"/>	GSI001.qst.local	hxdOfena.exe	hxdef100.exe	99.00000000	70656 Malware
<input checked="" type="checkbox"/>	GSI001.qst.local	hxdOfena.exe	hxdef100.exe	99.00000000	70656 Malware
<input checked="" type="checkbox"/>	GSI001.qst.local	hxdef100 - Changed.exe	hxdef100.exe	99.00000000	70656 Malware
<input checked="" type="checkbox"/>	GSI001.qst.local	ProRat Dropper - changed.exe	ProRat Dropper.exe	99.00000000	350764 Malware

250

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>