

# Unsecured Endpoints in the Hospital Environment Securing IOT and Medical Devices

Richard Staynings  
Cybersecurity Healthcare Leader

Craig Williams  
Talos Senior Technical Leader



## AGENDA

1. The Changing Face of Security
2. The IOT Medical Device Challenge
3. How to Secure the Un-Securable?
4. Intelligence: The Dangers of Unchecked IoT

# The Changing Face of ..... Security

A person wearing a blue hoodie is sitting at a wooden desk, looking at a laptop. The background is dark blue with vertical streaks of light and the word "PASSWORD" repeated in white and red. The word "PASSWORD" is also written in red on the laptop screen.

The Internet of  
**THINGS!**



**Healthcare is under attack!**





# Hollywood hospital becomes ransomware victim

The cyberattack prompted the centre to declare an "internal emergency," with access to IT systems left locked and held for ransom.



By Charlie Osborne for Zero Day | February 15, 2016 -- 12:23 GMT (04:23 PST) | Topic: Security



## RELATED STORIES



Security  
Ransomware: How much would you pay to get your files back?



Government  
Obama's gadgets: What tech does the president use?



CIO  
Online security? Just let me Google that, say puzzled bosses

# Ransomware Attackers Double-Bill Hospital

Kansas Heart Hospital Pays Ransom, Gets Told to Pay Again

Mathew J. Schwartz (@euroinfosec) • May 23, 2016

0 Comments



## Post-Examiner

### FBI investigating computer hack, possible ransom demand at MedStar Health

BY ANTHONY C. HAYES · MARCH 28, 2016 · 1 COMMENT



# MedStar Health

The FBI is investigating a computer hack and a possible ransom demand at Baltimore area MedStar hospital, according to sources familiar with the incident.

Because of this situation, staff at the affected locations cannot get into their computers, leaving personnel to conduct business with pen and paper.

**REUTERS**

**TECHNOLOGY**

Mon Mar 28, 2016 | 5:33 PM EDT

## Washington's MedStar Health shuts down computers after virus

### Canadian hospital's website hacked to serve up Teslacrypt ransomware



"The web portal is powered by the Joomla CMS, running version 2.5.6 (latest version is 3.4.8) according to a manifest file present on their server. Several vulnerabilities exist for this outdated installation, which could explain why the site has been hacked."



KDH operates an 86-bed hospital and physicians' office in Madison, Ind. – Hit by Locky Ransomware March 30<sup>th</sup> on a single computer but shut whole network down

March 18- two of Prime Healthcare's hospitals in California  
- Chino Valley Medical Center and Desert Valley Hospital  
shutdown because of ransomware attack

March 16<sup>th</sup>, Kentucky Methodist Hospital – forced to shutdown computer systems when hit with Locky Ransomware.

A screenshot of the Kentucky Methodist Hospital website. The browser address bar shows 'www.methodisthospital.net'. A prominent red banner at the top of the page contains the text: 'Internal State of Emergency due to a computer virus. [Click here for additional information.](#)'. Below this banner, the text reads: 'ethodist Hospital is currently working in an Internal State of Emergency due to a Computer Virus that has limited our use of ele'. The main content area has a light blue background. On the left, there is a logo for 'METHODIST HOSPITAL' with the tagline 'Our mission is your health.' On the right, there is a Google Custom Search bar with a 'Search' button. Further right, the address '1305 North Elm Street, Henderson, Kentucky 42420' and the phone number '270-827-7700' are displayed. At the bottom right, there are social media icons for Facebook and YouTube, and a logo for 'FAST COMMAND' with the text 'Original Disaster Response System'.



# Northern Lincolnshire and Goole NHS Foundation Trust cancels ALL operations after cyber attack



## MAJOR INCIDENT - UPDATE

### MAJOR INCIDENT – APPOINTMENTS CANCELLED

A virus infected our electronic systems on Sunday October 30 and we have taken the decision, following expert advice, to shut down the majority of our systems so we can isolate and destroy it.

All planned operations, outpatient appointments and diagnostic procedures have been cancelled for Wednesday November 2 with a small number of exceptions as follows:

- Audiology
- Physiological measurements
- Antenatal
- Community and therapy
- Chemotherapy
- Paediatrics

**Patients told not to turn up for appointments or for surgery**

[Privacy & Security](#)

## More than half of hospitals hit with ransomware in last 12 months

New research by Healthcare IT News and HIMSS Analytics found considerable uncertainty, questionable business continuity plans, and the need for more effective end-user education rampant in the industry.

By [Tom Sullivan](#) | April 07, 2016 | 07:52 AM

SHARE



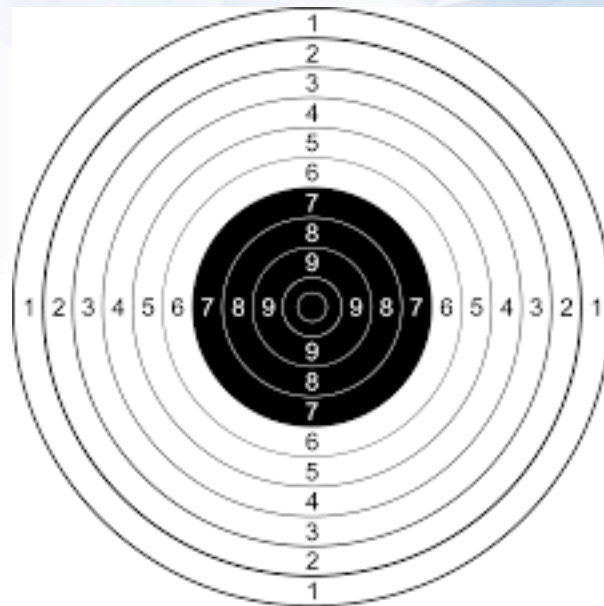
# Healthcare is Seen as an Easy Target

## Theft

- Theft of Medical Records - \$45~\$50 per
- Theft of full Identity – up to \$500
- Theft of clinical research / clinical trial data
- Theft of formulations / procedures

## Malicious Attack – DOS / Integrity /

- ICS systems – Critical hospital systems – water, air, heat, mechanicals
- Patient harm / assassination / poisoning





# The IoT / Medical Device Challenge

# The IoT / Medical Device Challenge

- 20% growth per annum in number of medical devices
- No common standards or security
- Windows Embedded 2009, (Windows XP)
- Dumb devices unable to support AV or End Point Protection
- Limited CPU and memory unable to sustain malware or DOS
- Easiest way to infiltrate a healthcare network is via a medical device / medical device network – 802.11 40 bit WEP or RJ45 port

# Legacy Medical Devices Aren't Going Away!

Half Life – Medical Devices last for up to 20 years

- 40 bit WEP anyone?
- Limited Network Stack







20% growth per annum in number of medical devices

# Converged Networks

# IoT Now Being Targeted at a Hospital Near You!

The next ransom attacks will likely be leveled directly against Hospital IOT systems and Medical Devices

# IoT Now Being Targeted

- IOT services we can't do without:
  - HVAC,
  - Elevators / Lifts,
  - Water Management,
  - Electrical supply,
  - etc.



**Imagine a man-made  
Hurricane Katrina....**



**.... A Cyber Attack  
against our  
Healthcare IOT  
Systems**

# The Next Level of Ransoms...won't be against data

- Could Patient lives be held to ransom by compromised Medical Device?



In 2014, the Federal Bureau of Investigation issued a report that predicted hackers could assail medical devices


In 2015 they issued an alert warning companies and the public about cybersecurity risks to networked medical devices and wearable sensors

# Cyber Assassin

You don't need James Bond to carry out assassinations when you own the medical device targets are attached to





A man is lying in a hospital bed, appearing to be asleep. He is wearing a light blue hospital gown with a small cross pattern. He has a nasal cannula in his nose and several IV lines in his arms. The bed is covered with a yellow blanket. To the left of the bed, there is a medical monitor on a stand. To the right, there are various medical tubes and equipment. The background shows a typical hospital room setting with wooden paneling.

Russian Oligarch,  
Mafia Boss or  
innocent victim?

**How Secure is your ICU?  
How confident are you  
about  
the security of your medical  
devices?**

What if the NICU was compromised ?





# The Weakest Link

So how can we go about protecting these simple networked devices in our healthcare environment?

How can we protect patients from malicious or unintentional harm?

# The Weakest Link

You **COULD** perform an assessment and configuration review of every IOT and medical device in each of your hospitals

- It would need to be ongoing!
- You would need an army!

Far easier to just assume the whole lot are a hopeless case and will be for the foreseeable future AT LEAST.. inherently INSECURE

# The Weakest Link

We need to SEGMENT them but in such a way that it doesn't impede patient care.

## Options:

1. Proxy traffic – simple, cheap, but doesn't scale
2. Infrastructure Enclaving (firewall & switch ACLs, VRF, MPLS, etc.) – inflexible, expensive to run & maintain and impedes the business
3. Dynamic policy-based segmentation – define once, apply globally

# Dynamic Policy Based Segmentation

- Easy to manage .... from one console across all sites
- Inclusive of all endpoints regardless
- Does not get in the way of the business of treating patients
- Enterprise Policy .... written once ... enforced globally
- Uses much of what you already own
- Uses your network to enforce your Policy via TrustSec and ISE

# TrustSec and ISE

- **TrustSec** is a feature of all recent Cisco switches and routers
  - You own it already! Its already in most of your hospitals! The footprint is expanded all the time!
- **ISE (Identity Services Engine)** – is probably used to manage your Guest Wireless Network or for NAC & Quarantine
  - Expand to the wired network and enable profiling feature
  - Enterprise ISE Domain across all sites
  - Global Management Console



# TrustSec Software-Defined Segmentation

Leverage the Intelligence Built into Cisco Network Hardware

## Desired Policy

- Who can talk to whom
- Who can talk to which systems
- Which systems can talk to other systems



|                 | Patient Records | Employee Intranet | Internet |
|-----------------|-----------------|-------------------|----------|
| Doctor / Laptop | ✓               | ✓                 | ✓        |
| Doctor / iPad   | ✗               | ✓                 | ✓        |
| Guest / Laptop  | ✗               | ✗                 | ✓        |
| Guest / iPad    | ✗               | ✗                 | ✓        |

Simplifies Policy with Security Group Tagging

Reduces ACL and Firewall Rule Complexity

Allows for Segmentation without VLANs



Switch



Router



VPN &  
Firewall



DC  
Switch



Wireless  
Controller

**Flexible and Scalable Policy Enforcement**

## Cisco Medical NAC

Identifying, Classifying, and Segmenting Clinical Healthcare Devices



# Intelligence : The Dangers of Unchecked IoT

# Why is IoT Dangerous? Let's ask a pro



USENIX Enigma 2016 - NSA TAO Chief on Disrupting Nation State Hackers



USENIX Enigma Conference

Subscribe 2,661

+ Add to Share ... More

91,878 views

682 19

# Dangers of Unchecked IoT

- Rob Joyce Chief, Tailored Access Operators NSA
  - “..there’s even the heating and cooling systems”
- Talos identified several flaws in Trane ComfortLink II thermostats and alerted Trane to them in April 2014.





# Vulnerability Details

- CVE-2015-2867 - Hardcoded credential vulnerability
- CVE-2015-2868 - Buffer overflow flaws leading to remote code execution

```
def exploit
  lop = [
    0xeaffffffe
  ].pack('V')

  xor = [
    0xe28f7018, # add    r7, pc, #24
    0xe3a06078, # mov    r6, #120 ; 0x78
    0xe3a04088, # mov    r4, #136 ; 0x88
    0xe7d73006, # ldrb   r3, [r7, r6]
    0xe0233004, # eor    r3, r3, r4
    0xe7c73006, # strb   r3, [r7, r6]
    0xe2566001, # subs   r6, r6, #1
    0x5afffffa # bpl    c < .text+0xc>
  ].pack('V*')
```

# Why pop IoT?

- Where are the advisories?
- download the update - <https://www.trane.com/residential/en/resources/smart-home-automation/installing-upgrading.html>

# Advisories?

```
.o0( craiwill@CRAIWILL-M-G0D3 temp ) tar zxvf rsup_145007844901.tar.gz  
x a_145007844901  
x b_145007844901  
x c_145007844901  
x d_145007844901  
x e_145007844901  
x f_145007844901  
x g_145007844901  
x v_145007844901  
x m_145007844901
```

# Advisories

```
.o0( craiwill@CRAIWILL-M-G0D3 temp ) file *
a_145007844901:      u-boot legacy uImage, Linux-2.6.26-466-ga04670e, Linux/ARM, OS Kernel Image (Not compressed), 2002624 bytes, Tue Apr 21 02:54:04 2015,
x2E948E86
b_145007844901:      gzip compressed data, was "rootfs.ext2", from Unix, last modified: Tue Apr 21 03:07:48 2015
c_145007844901:      Linux jffs2 filesystem data little endian
d_145007844901:      u-boot legacy uImage, Linux-2.6.26-466-ga04670e, Linux/ARM, OS Kernel Image (Not compressed), 1854792 bytes, Mon Dec 14 02:32:42 2015,
xA5F612F1
e_145007844901:      data
f_145007844901:      data
g_145007844901:      Linux jffs2 filesystem data little endian
m_145007844901:      ASCII text ←
rsup_145007844901.tar.gz: gzip compressed data, from Unix, last modified: Mon Dec 14 08:43:59 2015
v_145007844901:      ASCII text
```

# Advisories

```
.o0( craiwill@CRAIWILL-M-G0D3 temp ) head m_145007844901
<version_info>
<product build='145007844901' release='4.0.3' date='14-Dec-2015' downloadSize='90922' installationSize='95468'>
<features>
<feature notes='Improved WiFi management, Comm Bus improvements'/>
</features>
<fixes>
<fix info='Security fixes, courtesy: Cisco Talos'/> ←
<fix info=' Improved comm link reporting with 940'/>
</fixes>
<checksum></checksum>
.o0( craiwill@CRAIWILL-M-G0D3 temp )
```



# Implications

- Where is the advisory??
- A fully functional, unrestricted BusyBox environment in an IoT device means it's useful for other “things”
- No one thinks about patching their IoT devices
- *Mr. Robot*, anyone?



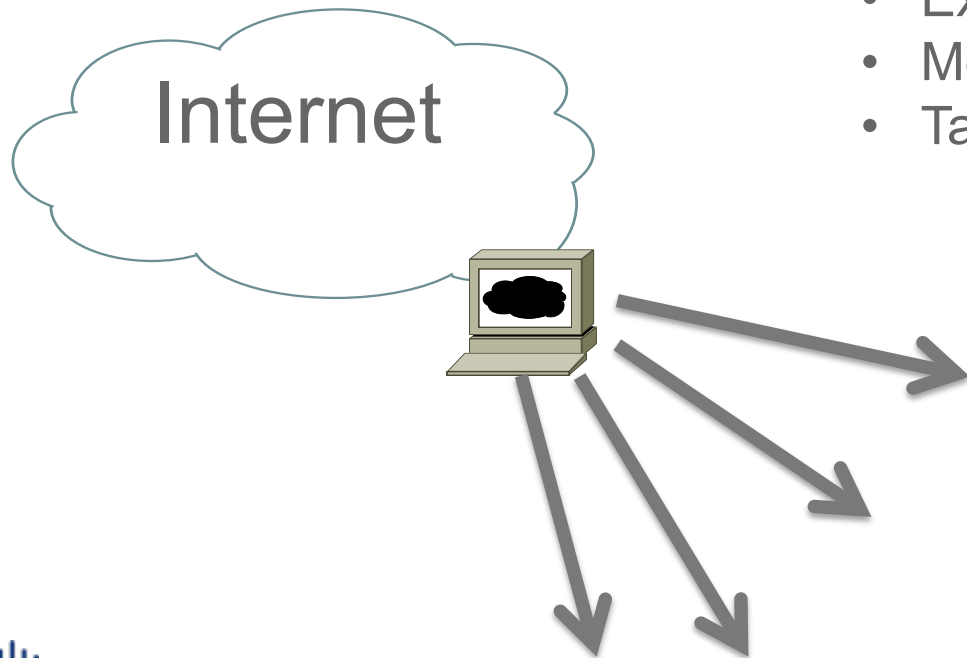
# Conclusion

- IoT presents an enormous opportunity to connect, share, and simplify our lives
- Security cannot be afterthought
- Pick vendors who will be around to maintain and secure the device for its life span
- Talos is committed to making the internet safer and more secure for all users



# Ransomware Distribution: Network Vectors

# SAMSAM



- Exploits Jboss Vulnerability
- Moves Laterally
- Targeted Across Organization

# Two Critical JBoss CVEs

## CVE-2007-1036

“...JBoss does not restrict access to the console and web management interfaces...”

## CVE-2010-0738

“The JMX-Console web application ... performs access control only for the GET and POST methods...”

# Communicating with Threat Actors

Browser address bar: roe53[redacted]on/fatman/

| Your comments  | Our Answer  |
|--|---|
| Leave a comment here with your "Computer name" to receive decryption software. |   |
| 22.03.2016 18:40 -- [redacted]@gmail.com<br>For All Affected PCs               | Test decryption for [redacted] PC, check help, <a href="http://s000.tinyupload.com/index.php?file_id=727012669578">http://s000.tinyupload.com/index.php?file_id=727012669578</a> [redacted] |
|  | Sorry for delay, here you are: allKeys <a href="http://s000.tinyupload.com/index.php?file_id=50019761328">http://s000.tinyupload.com/index.php?file_id=50019761328</a> [redacted]           |

**Leave a comment**

Your Email:



# Payment Increases..

## #What happened to your files?

All of your important files encrypted with RSA-2048, RSA-2048 is a powerful cryptography algorithm  
For more information you can use Wikipedia  
\*attention: Don't rename or edit encrypted files because it will be impossible to decrypt your files

## #How to recover files?

RSA is a asymmetric cryptographic algorithm, You need two key

- 1-Public key: you need it for encryption
- 2-Private Key: you need it for decryption

So you need Private key to recover your files.  
It's not possible to recover your files without private key

## #How to get private key?

You can receive your Private Key in 3 easy steps:

**Step1:** You must send us One Bitcoin for each affected PC to receive Private Key.

**Step2:** After you send us one Bitcoin, Leave a comment on our blog with these detail: Your Bitcoin transaction reference + Your Computer name

\*Your Computer name is: COMPUTERNAME VARIABLE

**Step3:** We will reply to your comment with a decryption software, You should run it on your affected PC and all encrypted files will be recovered

\*Our blog address:

```
</html>
<pre>
<font color="Maroon"><center><h3>#What happened to your files?</h3></center></font>

All of your important files encrypted with RSA-2048, RSA-2048 is a powerful cryptography algorithm
For more information you can use Wikipedia
<font color="DrakRed">*</font>attention: Don't rename or edit encrypted files because it will be impossible to decrypt your files

<font color="Maroon"><center><h3>#How to recover files?</h3></center></font>

RSA is a asymmetric cryptographic algorithm, You need two key

1-Public key: you need it for encryption
2-Private Key: you need it for decryption

So you need Private key to recover your files.
It's not possible to recover your files without private key

<font color="Maroon"><center><h3>#How to get private key?</h3></center></font>

You can receive your Private Key in 3 easy steps:

<font color="red">Step1:</font> You must send us <font color="red">1.5 Bitcoin</font> for each affected PC OR <font color="red">22 Bitocin</font> to receive ALL
Private Key for ALL affected PC.

<font color="red">Step2:</font> After you send us <font color="red">1.5 Bitcoin</font>, Leave a comment on our blog with this detail: Just write Your "Computer
name" in your comment

<font color="DrakRed">*</font>Your Computer name is:PC<br><br>
<font color="red">Step3:</font> We will reply to your comment with a decryption software, You should run it on your affected PC and all encrypted files will be
recovered

<font color="DrakRed">*</font>Our blog address: <a href="https://followsec7.wordpress.com">https://followsec7.wordpress.com</a>

<font color="DrakRed">*</font>Our Bitcoin address: 1D6ScsG2BmZu3VFDegfnMC6CzjnWtZi6Kj

(If you send us <font color="red">22 Bitcoin</font> For all PC, Leave a comment on our blog with this detail: Just write "For All Affected PC" in your comment)

<font color="Maroon"><center><h3>#### Test Decryption ####</h3></center></font>

Check our blog, We generated a decryption software for one of your computer randomly, Don't worry it's not malicious software.
If you afraid to run "Test Decryption" software, You can run it on a VM(Virtual machine), also you need some encrypted file in VM from test computer

<font color="Maroon"><center><h3>#What is Bitcoin?</h3></center></font>

Bitcoin is an innovative payment network and a new kind of money.
You can create a Bitcoin account at https://blockchain.info/ and deposit some money into your account and then send to us

<font color="Maroon"><center><h3>#How to buy Bitcoin?</h3></center></font>
```

# Summary

## Behavioral Indicators

Threat Score: 90

### + Process Modified a File in a System Directory

Severity: 90 Confidence: 100

### ● Process Modified a File in the Program Files Directory

Severity: 80 Confidence: 90

Malware will modify files within the Program Files to hamper legitimate applications (such as security software) and attempt to appear as a legitimate application on the system. Other reasons for modification include attempts to remove evidence of malicious software activity.

Categories file

Tags executable, file, process

Report Error

| Path   | Process Name | Process ID        |
|--|--------------|-------------------|
| \Program Files\Common Files\Microsoft Shared\OFFICE12\Office Setup Controller\Rosebud.en-us\SETUP.XML.encryptedRSA | SAMSAM.EXE   | 1988 (SAMSAM.EXE) |
| \Program Files\Common Files\Microsoft Shared\THEMES12\CANYON\THMBNAIL.PNG.encryptedRSA                             | SAMSAM.EXE   | 1988 (SAMSAM.EXE) |
| \Program Files\Adobe\Reader 9.0\Resource\TypeSupport\Unicode\Mappings\Mac\SYMBOL.TXT.encryptedRSA                  | SAMSAM.EXE   | 1988 (SAMSAM.EXE) |
| \Program Files\Common Files\Microsoft Shared\web server extensions\40\bin\1033\HELP_DECRYPT_YOUR_FILES.html        | SAMSAM.EXE   | 1988 (SAMSAM.EXE) |
| \Program Files\Common Files\Microsoft Shared\Stationery\HELP_DECRYPT_YOUR_FILES.html                               | SAMSAM.EXE   | 1988 (SAMSAM.EXE) |
| \Program Files\Adobe\Acrobat.com\assets\icons  |              |                   |

- Exploiting Network Vulnerabilities
  - JBoss
- Laterally targets multiple systems
- Payment is in Bitcoin
- Obtain Private Key via Blog Comment

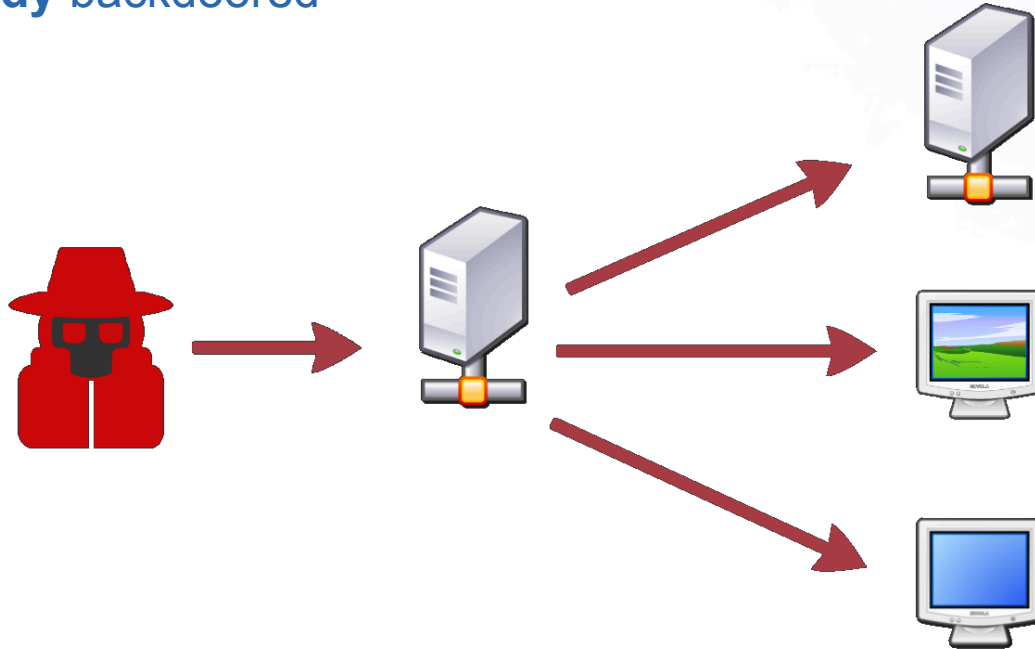
# Forensic timeline developed by Cisco IR

- Day X
  - JexBoss Invocation & JBossAss backdoor installation
- X+47 Days
  - File Upload Installed on web server
- X+49 Days
  - Full Webshell installed and CVSDE Executed – Active Directory dump
- X+73 Days
  - tunnel.jsp installed allowing IP Tunnel
  - Elevated privileged user connect via RDP
  - Recon with Hyena
  - Likely first use of admin credential
- X+74 Days
  - Samsam encryption operation begins

# JBoss Server Backdoors

# Changes in the Threat Landscape

- 3.2m vulnerable JBoss servers are being used as an attack vector
- ~5000 **already** backdoored



## Application list

[localhost/jbossass](#) •  
[localhost/mela](#) •  
[localhost/oss](#)  
[localhost/IPTV/LCO](#)  
[localhost/exam](#)  
[localhost/web-console](#) •  
[localhost/jbossinvoker](#)  
[localhost/iptv/broadcaster](#)  
[localhost/shellinvoker](#) •  
[localhost/invoker](#)  
[localhost/report](#)  
[localhost/destiny](#) •  
[localhost/x](#) •  
[localhost/](#)  
[localhost/wcZRCZPqUxXkJg](#) •  
[localhost/miss](#)  
[localhost/jbossws](#)  
[localhost/IPTV/BILLING](#)  
[localhost/console](#) •  
[localhost/jbossmq-httpil](#)  
[localhost/mjos](#)  
[localhost/iptv/middleware](#)  
[localhost/axis](#)  
[localhost/genesis](#) •  
[localhost/iptv](#)  
[localhost/iptv/secreport](#)

Omgyoureowned.com/status&full=true



**Matthew Olney** @kpyke · Apr 11

New metric: Actors per JBOSS server.



5



4



# Want more Talos info?

- Blogs: <http://blog.talosintelligence.com/>
- White papers: <http://www.talosintelligence.com/additional-resources/>
- Vulnerability Reports: <http://www.talosintelligence.com/vulnerability-reports/>
- Email Notificaitons/FREE Webinars: <http://cs.co/TalosUpdate>



talosintelligence.com  
@talossecurity  
@security\_craig





# Thank You

[blogs.cisco.com/security](https://blogs.cisco.com/security)

[blog.staynings.com](https://blog.staynings.com)

[@rstaynings](https://twitter.com/rstaynings)



Richard Staynings  
Security Principal and Director, Security Advisory Services, Cisco  
28 March 2015  
Security World Conference, Harlow, UK

