The Connected World has been disconnected: Survival Guide in IoThreats Era

Denis Makrushin
Security Researcher
Kaspersky Lab
@difezza
Internet-of-Things or Internet-of-Threats?

The recent explosion of Internet-enabled devices—known as the Internet of Things—as well as the propagation of software-based functionality in systems has led to a huge increase in the number of CVE requests we have been receiving on a daily basis. We did not anticipate this rate of growth, and, as a result, were not as prepared for the latest surge in requests over the past 12 months as we had hoped. The result has been some of the delay in CVE assignments that the software security community has recently witnessed. We recognize the inconvenience that has resulted, and are working hard to come up with a solution. Last week, we proposed a possible option to our CVE Editorial Board, but some members raised concerns about the approach, and we have withdrawn it from consideration. We are working diligently to come up with a solution that will meet the needs of all the various use cases of CVE.

CVE® International in scope and free for public use, CVE is a dictionary of publicly known information security vulnerabilities and exposures. CVE’s common identifiers enable data exchange between security products and provide a baseline index point for evaluating coverage of tools and services.
You a Hero. And it's not a Game.
My home is my castle, isn’t it?
My home is my castle, isn’t it? Show me.

Nope: “port:554 has_screenshot:true”
The cup of Smart Coffee
Cyber Jungle start right here: BMS
If you're going to San Franciscoooo... oops

San Francisco CA
@SF_CA_RR

SF Muni Fare Machines Back Up and Running
rightrelevance.com/search/article...

3:41 AM - 28 Nov 2016

Ransomware Crooks Demand $70,000 After Hacking San Francisco Transport System -- UPDATED
Public terminals vulnerability assessment

- **FULL-SCREEN APPLICATION**
  - Help Section: Jump to Control Panel

- **TAP-FUZZING**
  - Calling standard elements of the operating system

- **DATA-FUZZING**
  - Use of application’s "undocumented" features

- **VIRTUAL KEYBOARD**
  - Input of arbitrary data

- **OPERATING SYSTEM ENVIRONMENT**
PROOF-OF-CONCEPT
Parking terminal: the full screen app

The Full Screen Application contains Google Widget without any customization. Let’s try to escape.
How did you do it, David Blaine?!

The Street Magic baby:
1) Browser Properties
2) Control Panel
3) Virtual Keyboard
4) `whoami` :)

[Image of a computer screen showing command prompt output]
Keep calm and save the World!

- **Developer/Administrator:**
  - Customize all third-party components
  - Don’t use Administrative privileges
  - Restrict access to Internet
  - Default Deny all non-whitelisted

- **User**
  - Run from the terminal! Don’t trust the public device.
  - Anyway don’t input your personal/payment data
  - Found a bug? Send the report.
The End. Thank you!

https://twitter.com/difezza
https://byinsecure.com
condifesa@gmail.com
One month later

WHY?!?!
1) Application dump with Client’s data and transaction logs

2) Social Engineering (phishing, advertising, “Congrats, you’ve won the money, send us a SMS…”)

3) Botnet for DDoS-attacks, bitcoin mining, extraterrestrial civilizations search
A little more smart touch
A little more smart touch... worldwide!
A little more smart touch... worldwide! (video-demo)
How to live with that

- Developer/Administrator, think out of the box:
  - Don’t use Administrative privileges
  - Restrict access to Internet
  - Default Deny all non-whitelisted

- User
  - Run from the terminal! Don’t trust the public device.
  - Anyway don’t input your personal/payment data
  - Found a bug? Send the report.
Getting the road devices’ data
“Somebody’s watchin’ me” (c) traffic cameras

1) Traffic volume data
2) Car patterns data
3) Geo Location
How to live with that

- **Developer/Administrator:**
  - Encrypt all wireless connections
  - Don’t use Administrative privileges
  - Restrict access to Internet
  - Default Deny all non-whitelisted

- **User:**
  - Found a bug? Send the report. (In the case, if this is interactive device)
  - Anyway don’t input your personal/payment data
Connected Medicine

Diagnostic Device #1 (MR)

Diagnostic Device #2 (CT)

Diagnostic Device #3 (Cardiograph)

PACS workstation

PACS

DICOM

DICOM

DICOM

DICOM

25
“DICOM port:104”. Show me.
“DICOM port:104” returned 1,344 results
Information for Targeted Attack

“medical port:445”

Reconnaissance stage for targeted attack against medical institute provides answers for the questions:

1. What host in the medical infrastructure is most interesting?
2. What hotspot could be an entry point to sensitive data?
Where PACS is, there patient’s data is
PACS front-end as an entry point

It shouldn’t be online, but:

1) It is
2) It has public vulnerabilities
3) It’s open for everyone
What about medical device?

There are two types of medical devices:

- HOST-ORIENTED CONNECTION
- NETWORK-ORIENTED CONNECTION

Very Expensive
Expensive
No Ethernet port - no problems, right?

NOPE:

1. Compromised perimeter still contains medical workstations...
2. It has vulnerabilities and backdoors
3. And it has special medical software and drivers
What adversary can do with Analyzer.exe*

- **Steal** all medical information received from the device
- **Spoof** all medical information received from the device
- **Change** the operating parameters (for ransom purposes?), that would entail a costly calibration procedures
- Notify you and help you to fix the issues ;)

*Analyzer.exe* is a software for a diagnostic medical device
How to live with that

- Developer/Administrator:
  - Don’t store data on medical device and organize easy restore point of the software (ransomware mitigation)
  - Isolate all medical data storages (DICOM-devices, PACS/NAS/FTP-servers, even DICOM-viewers) in a separate segment
  - Backup, encrypt, backup...

- User:
  - Be healthy.
We still have a “human factor”
Keep calm and save the World!
Thank you!

https://twitter.com/difezza
https://byinsecure.com
condifesa@gmail.com