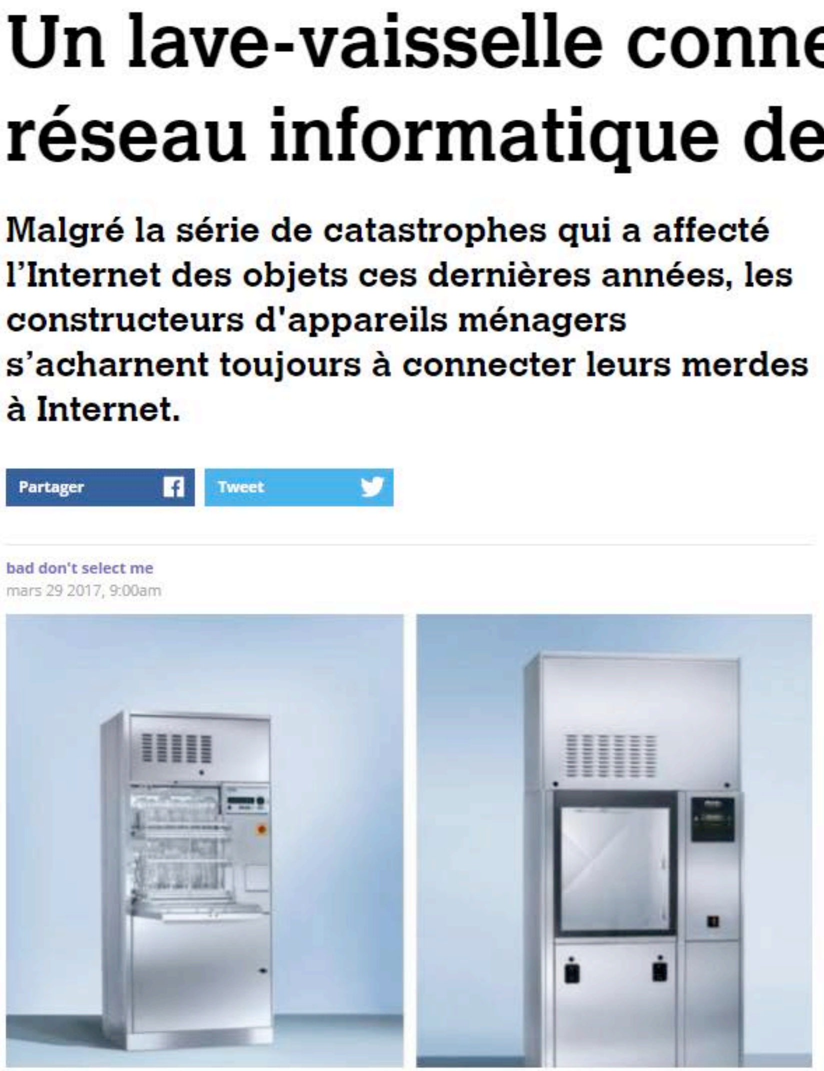
Hôpitaux face à la cybersécurité

Franck Calcavecchia
Information security Officer

INTRODUCTION



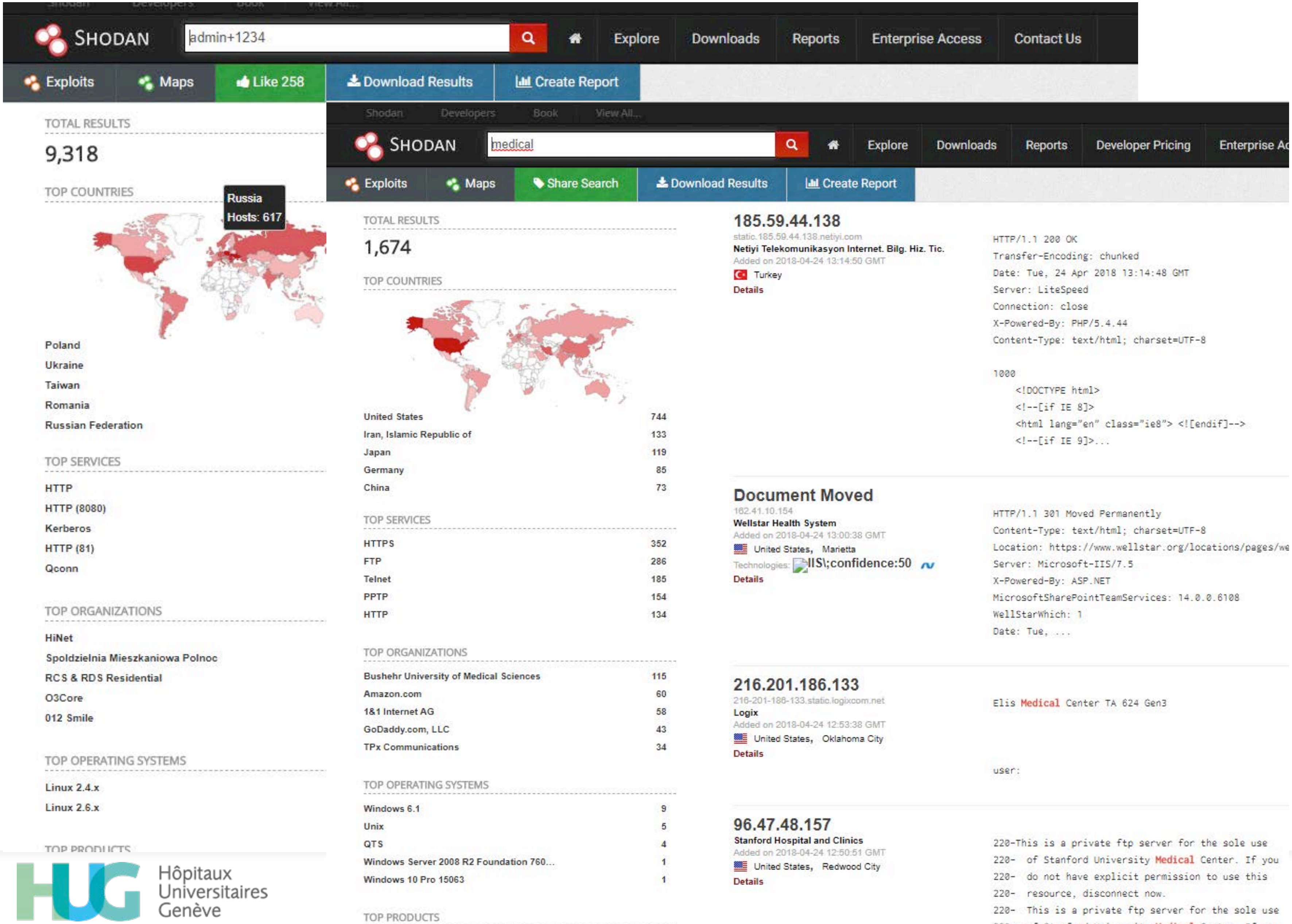
Un lave-vaisselle connecté permet de pirater le réseau informatique des hôpitaux

Malgré la série de catastrophes qui a affecté l'Internet des objets ces dernières années, les constructeurs d'appareils ménagers s'acharnent toujours à connecter leurs merdes à Internet.

bad don't select me
mars 29 2017, 9:00am

https://motherboard.vice.com/fr/article/z49w3y/un-lave-vaisselle-connecte-permet-dacceder-au-reseau-informatique-des-hopitaux

INTRODUCTION



admin+1234

TOTAL RESULTS

9,318

TOP COUNTRIES

Russia
Hosts: 617

Poland
Ukraine
Taiwan
Romania
Russian Federation

TOP SERVICES

HTTP
HTTP (8080)
Kerberos
HTTP (81)
Qconn

TOP ORGANIZATIONS

HiNet
Spoldzielnia Mieszkaniowa Polnoc
RCS & RDS Residential
O3Core
012 Smile

TOP OPERATING SYSTEMS

Linux 2.4.x
Linux 2.6.x

TOP PRODUCTS

medical

TOTAL RESULTS

1,674

TOP COUNTRIES

United States	744
Iran, Islamic Republic of	133
Japan	119
Germany	85
China	73

TOP SERVICES

HTTPS	352
FTP	286
Telnet	185
PPTP	154
HTTP	134

TOP ORGANIZATIONS

Bushehr University of Medical Sciences	115
Amazon.com	60
1&1 Internet AG	58
GoDaddy.com, LLC	43
TPx Communications	34

TOP OPERATING SYSTEMS

Windows 6.1	9
Unix	5
QTS	4
Windows Server 2008 R2 Foundation 760...	1
Windows 10 Pro 15063	1

TOP PRODUCTS

185.59.44.138
static.185.59.44.138.netiyi.com
Netiyi Telekomunikasyon Internet. Bilg. Hiz. Tic.
Added on 2018-04-24 13:14:50 GMT
Turkey
Details

```
HTTP/1.1 200 OK
Transfer-Encoding: chunked
Date: Tue, 24 Apr 2018 13:14:48 GMT
Server: LiteSpeed
Connection: close
X-Powered-By: PHP/5.4.44
Content-Type: text/html; charset=UTF-8

1000
    <!DOCTYPE html>
    <!--[if IE 8]>
    <html lang="en" class="ie8"> <![endif]-->
    <!--[if IE 9]>...
```

Document Moved
162.41.10.154
Wellstar Health System
Added on 2018-04-24 13:00:38 GMT
United States, Marietta
Technologies: IIS\;confidence:50
Details

```
HTTP/1.1 301 Moved Permanently
Content-Type: text/html; charset=UTF-8
Location: https://www.wellstar.org/locations/pages/we
Server: Microsoft-IIS/7.5
X-Powered-By: ASP.NET
MicrosoftSharePointTeamServices: 14.0.0.6108
WellStarWhich: 1
Date: Tue, ...
```

216.201.186.133
216-201-186-133.static.logixcom.net
Logix
Added on 2018-04-24 12:53:38 GMT
United States, Oklahoma City
Details

```
Elis Medical Center TA 624 Gen3


user:
```

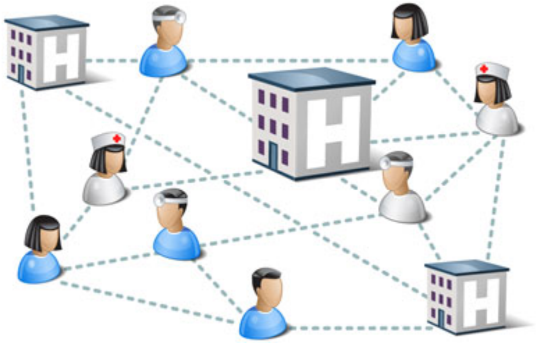
96.47.48.157
Stanford Hospital and Clinics
Added on 2018-04-24 12:50:51 GMT
United States, Redwood City
Details

```
220-This is a private ftp server for the sole use
220-  of Stanford University Medical Center. If you
220-  do not have explicit permission to use this
220-  resource, disconnect now.
220-  This is a private ftp server for the sole use
```

POURQUOI ATTAQUER LES HOPITAUX ?

1. Exposition croissante

- ❑ **+ en + connectivité**
  - o Interne (Biomédical, imagerie, DPI, PACS, technique, batiments..)
  - o Externes (Autres hôpitaux, laboratoires, fournisseurs, partenaires, patients…)

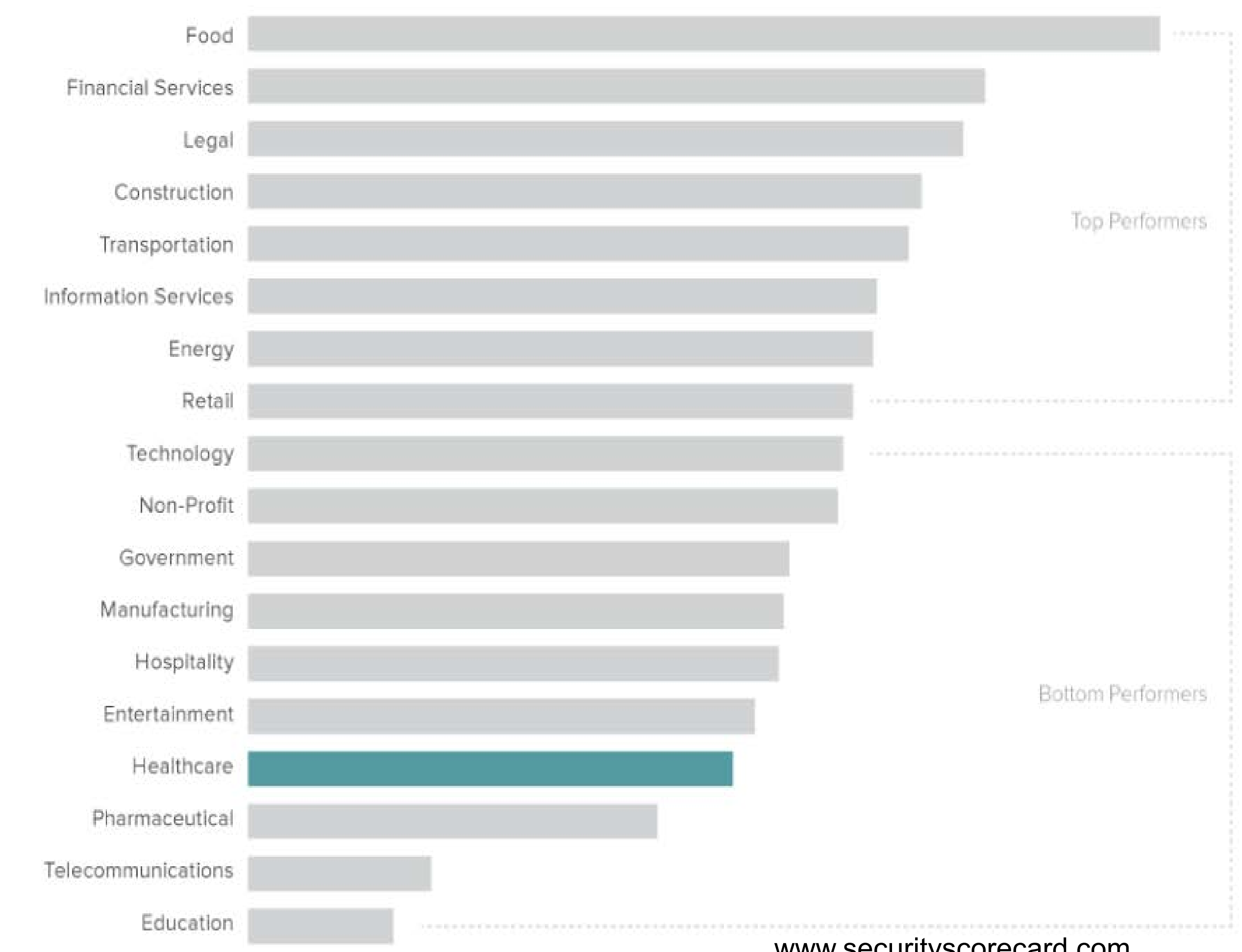


- ❑ **+ en + de CLOUD et mobiles**
  - o Notification laboratoire sur smartphone
  - o Saisie des données sur des tablettes aux pied du lit des patients
  - o Données personnes sur les mobiles / tablettes des patients

POURQUOI ATTAQUER LES HOPITAUX ?

2. Retard notoire dans les mesures de sécurité

Healthcare Industry Lagging in Cybersecurity (*Mar 5, 2018*)

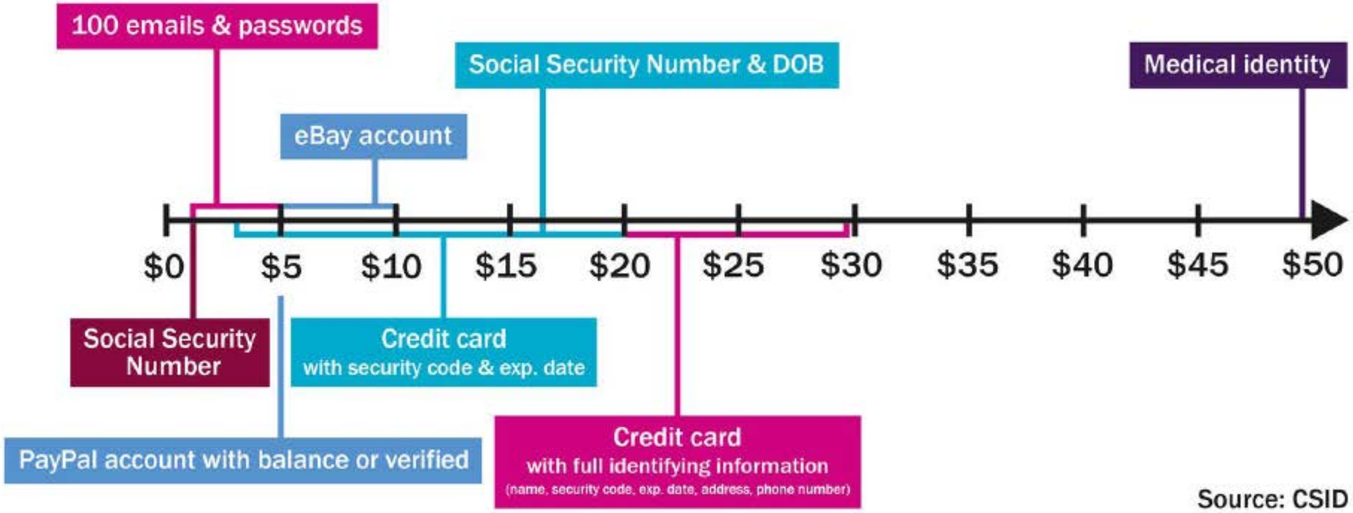


www.securityscorecard.com

Hôpitaux Universitaires Genève

POURQUOI ATTAQUER LES HOPITAUX ?

3. La valeur des données à la revente



Source: CSID

- ➢ Raisons :

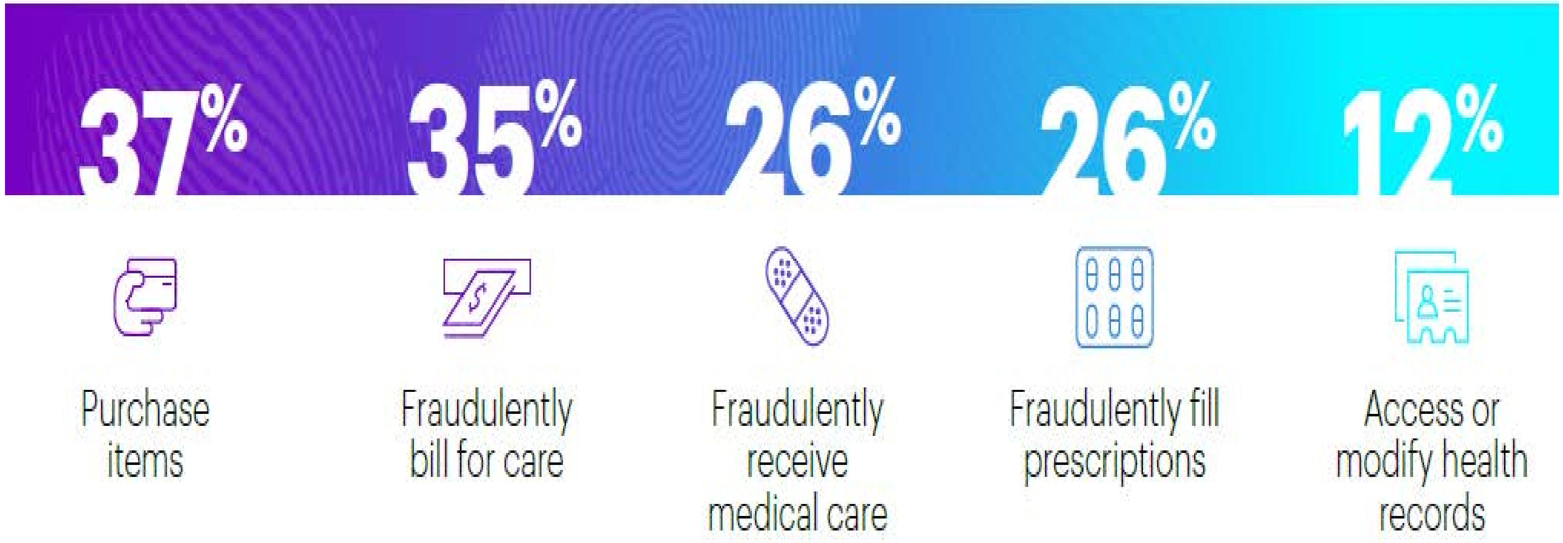
Difficile ou impossible à changer

Mois ou années avant de le détecter

Innocence difficile à prouver

QUE FONT ILS AVEC CES DONNÉES ?

FIGURE 3. Victims of medical identity theft report stolen IDs were used for fraudulent activities.



37% Purchase items

35% Fraudulently bill for care

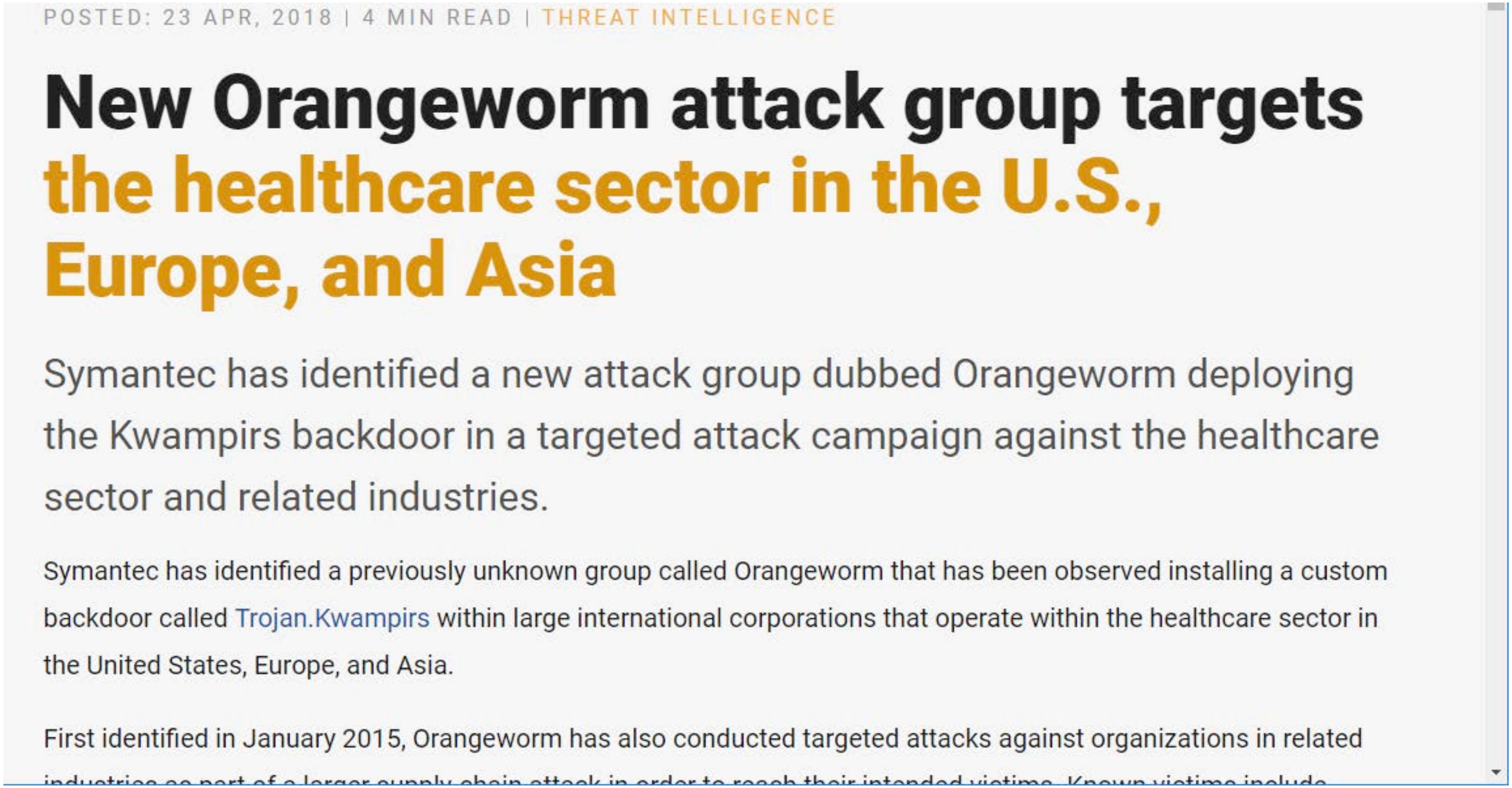
26% Fraudulently receive medical care

26% Fraudulently fill prescriptions

12% Access or modify health records

Source: Accenture 2017 Consumer Survey on Healthcare Cybersecurity and Digital Trust

HAAT : HOPITAL AS A TARGET



POSTED: 23 APR, 2018 | 4 MIN READ | THREAT INTELLIGENCE

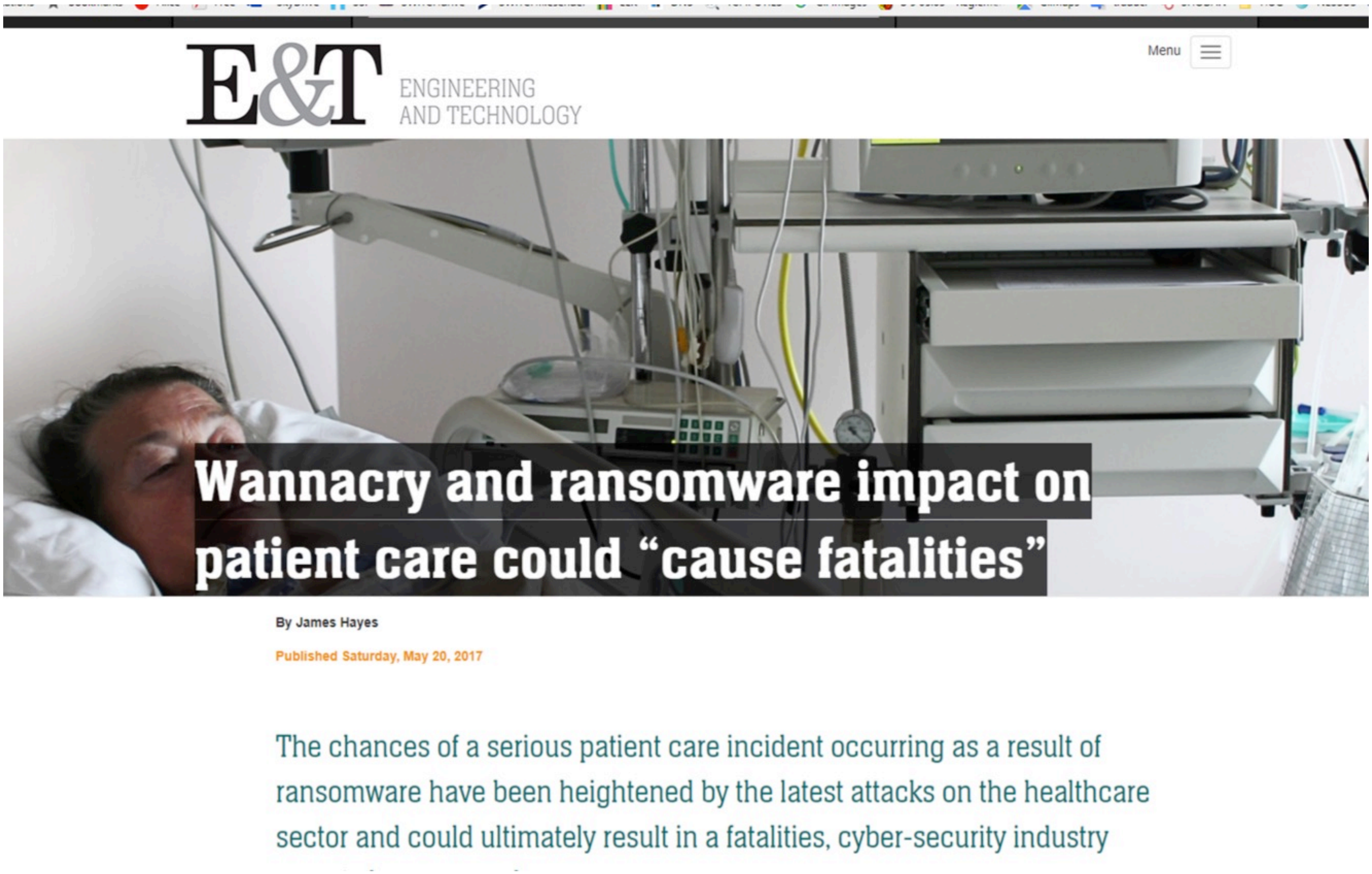
New Orangeworm attack group targets the healthcare sector in the U.S., Europe, and Asia

Symantec has identified a new attack group dubbed Orangeworm deploying the Kwampirs backdoor in a targeted attack campaign against the healthcare sector and related industries.

Symantec has identified a previously unknown group called Orangeworm that has been observed installing a custom backdoor called Trojan.Kwampirs within large international corporations that operate within the healthcare sector in the United States, Europe, and Asia.

First identified in January 2015, Orangeworm has also conducted targeted attacks against organizations in related industries as part of a larger supply chain attack in order to reach their intended victims. Known victims include

IMPACT DRAMATIQUE



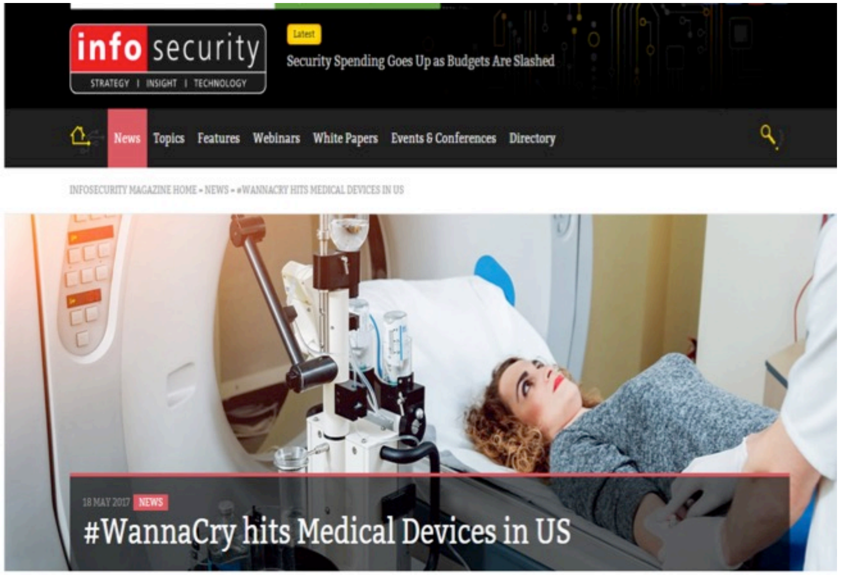
Wannacry and ransomware impact on patient care could “cause fatalities”

By James Hayes

Published Saturday, May 20, 2017

The chances of a serious patient care incident occurring as a result of ransomware have been heightened by the latest attacks on the healthcare sector and could ultimately result in a fatalities, cyber-security industry

PRINTEMPS 2007 : LE RÉVEIL

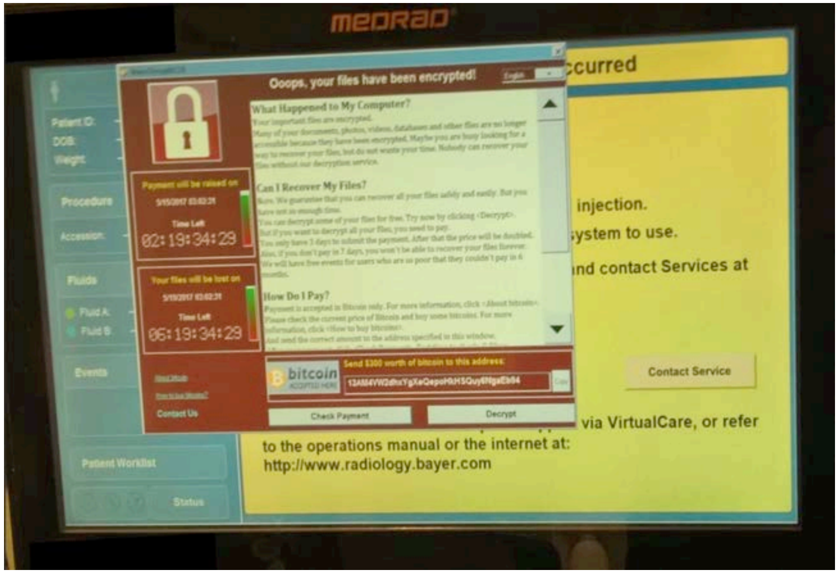


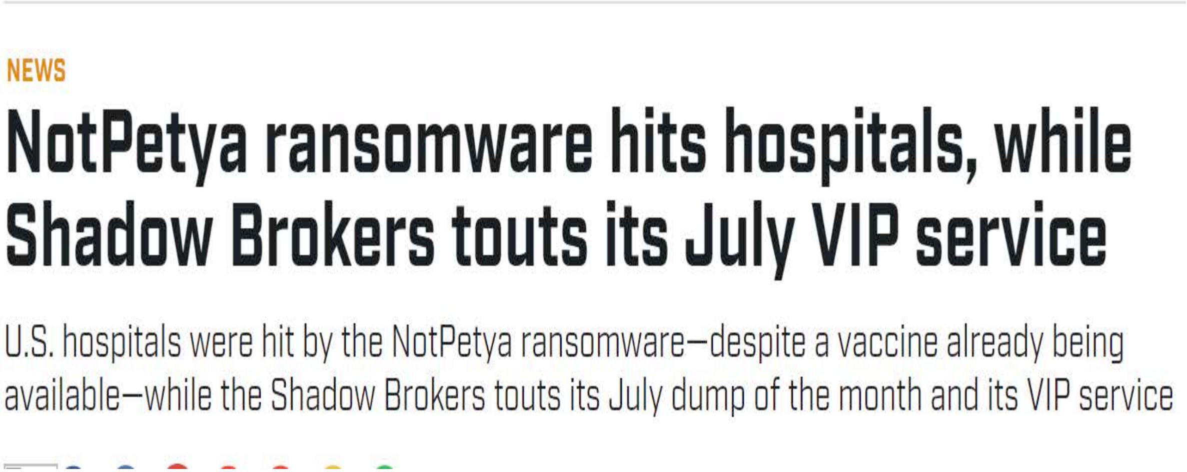
Security Spending Goes Up as Budgets Are Slashed

INFOSECURITY MAGAZINE HOME » NEWS » #WANNACRY HITS MEDICAL DEVICES IN US

18 MAY 2017 NEWS

#WannaCry hits Medical Devices in US



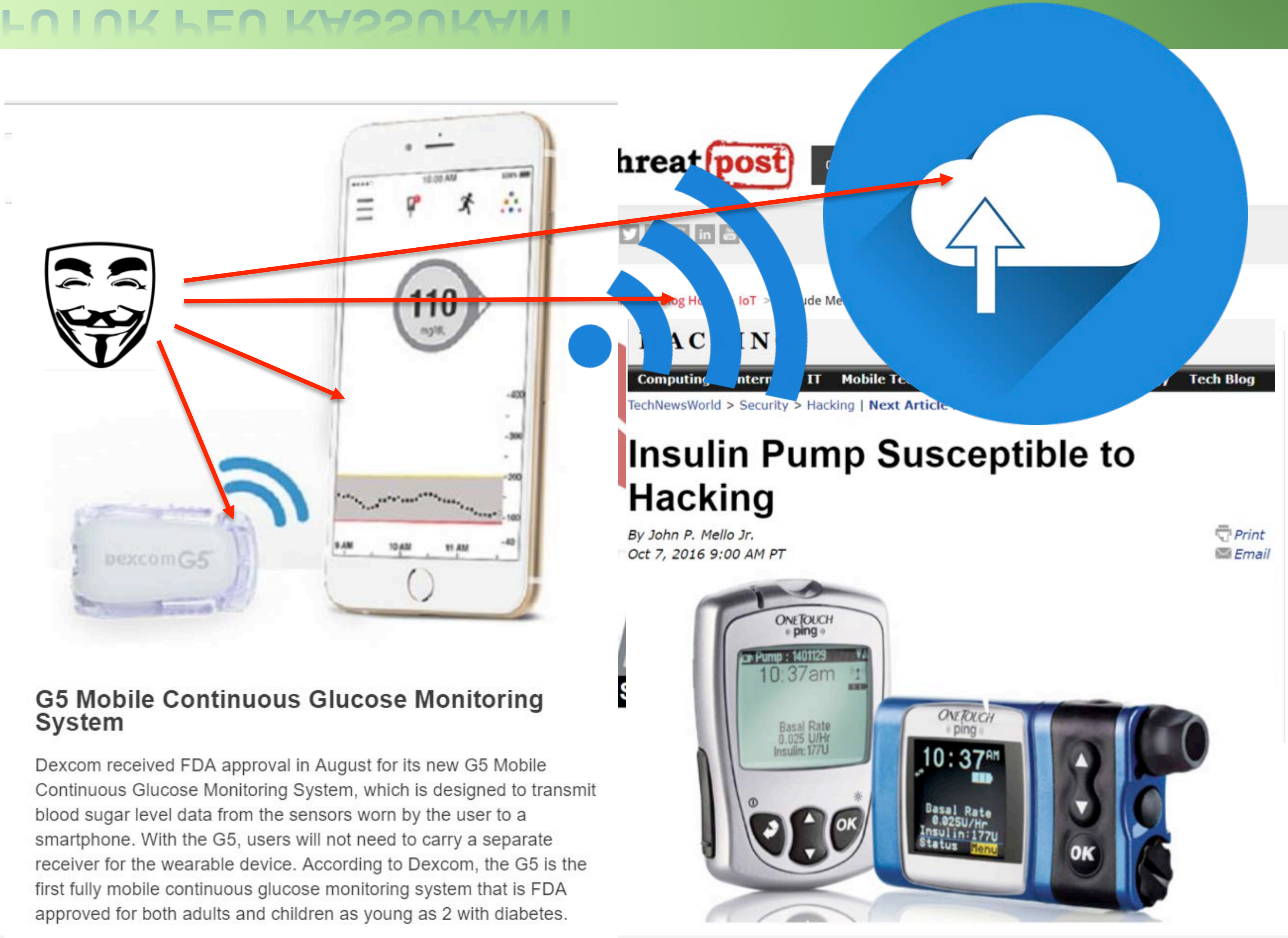


NEWS

NotPetya ransomware hits hospitals, while Shadow Brokers touts its July VIP service

U.S. hospitals were hit by the NotPetya ransomware—despite a vaccine already being available—while the Shadow Brokers touts its July dump of the month and its VIP service

UN FUTUR PEU RASSURANT



110
mg/dL
dexcom G5
hreat post
IoT
ACKIN
ONETOUCH ping
Pump : 1401129
10:37am
Basal Rate 0.025 U/Hr Insulin: 177U
10:37AM
Basal Rate 0.025U/Hr Insulin:177U Status Menu
OK

G5 Mobile Continuous Glucose Monitoring System

Dexcom received FDA approval in August for its new G5 Mobile Continuous Glucose Monitoring System, which is designed to transmit blood sugar level data from the sensors worn by the user to a smartphone. With the G5, users will not need to carry a separate receiver for the wearable device. According to Dexcom, the G5 is the first fully mobile continuous glucose monitoring system that is FDA approved for both adults and children as young as 2 with diabetes.

Computing | Intern | IT | Mobile Te | Tech Blog

TechNewsWorld > Security > Hacking | Next Article

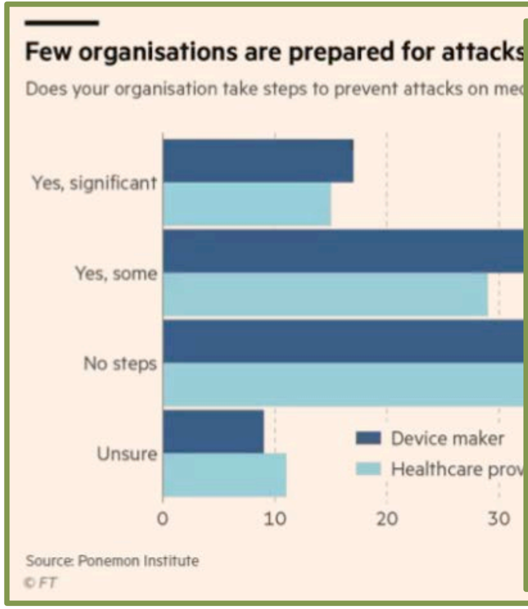
Insulin Pump Susceptible to Hacking

By John P. Mello Jr.
Oct 7, 2016 9:00 AM PT

Print
Email

POURQUOI ?

- Risque est sous estimé par les équipementiers et les hôpitaux
- OS obsolètes et plus maintenus



Few organisations are prepared for attacks

Does your organisation take steps to prevent attacks on med

Source: Ponemon Institute

© FT

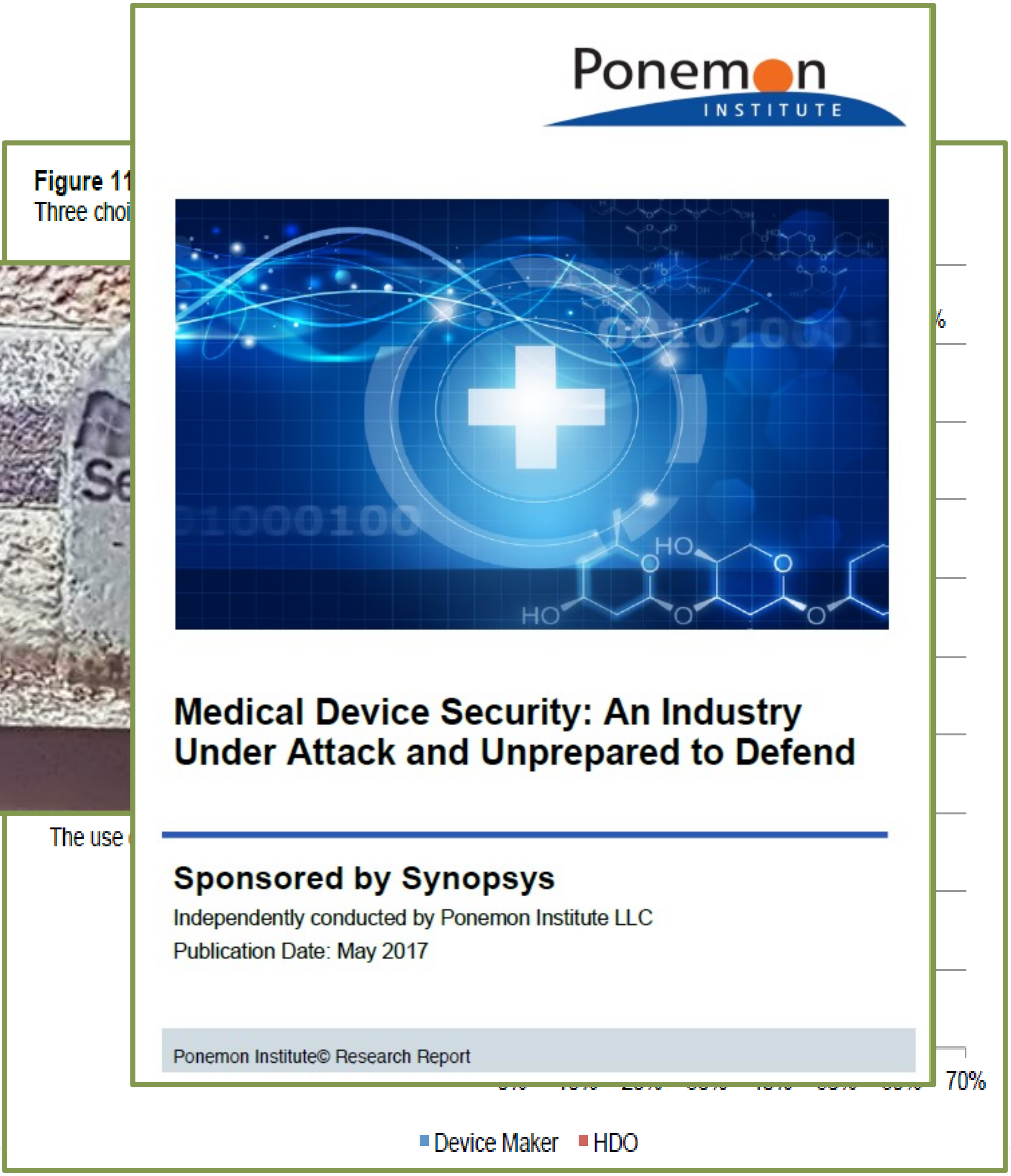


Figure 11

Three choi

The use

Ponemon INSTITUTE

Medical Device Security: An Industry Under Attack and Unprepared to Defend

Sponsored by Synopsys

Independently conducted by Ponemon Institute LLC

Publication Date: May 2017

Ponemon Institute© Research Report

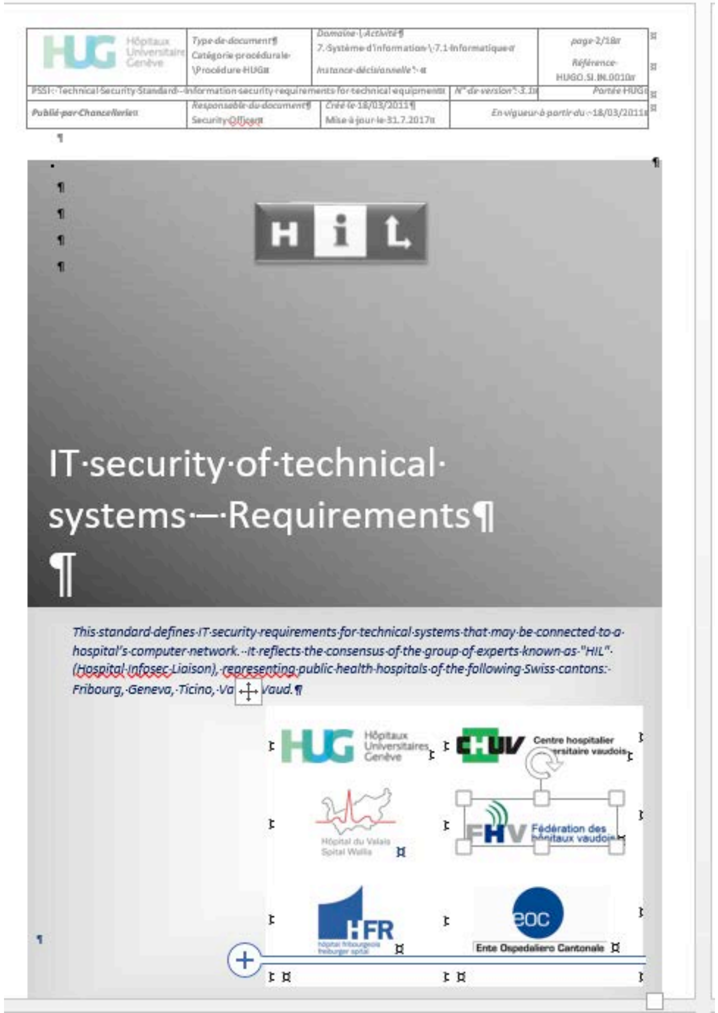
Hôpitaux Universitaires Genève

NOTRE APPROCHE

- Depuis 2013 revue systématique de toutes les demandes de raccordement au réseau (Checklist)

- Depuis 2017 version commune inter hopitaux
  - ❑ Disponible en Français, Anglais, Italien et Allemand

- 33 Exigences de base
  - ❑ Version OS et patchs
  - ❑ Authentification / Autorisation
  - ❑ Malware
  - ❑ Accès réseau et télémaintenance
  - ❑ Protection des données
  - ❑ Documentation
  - ❑ Audit et logs



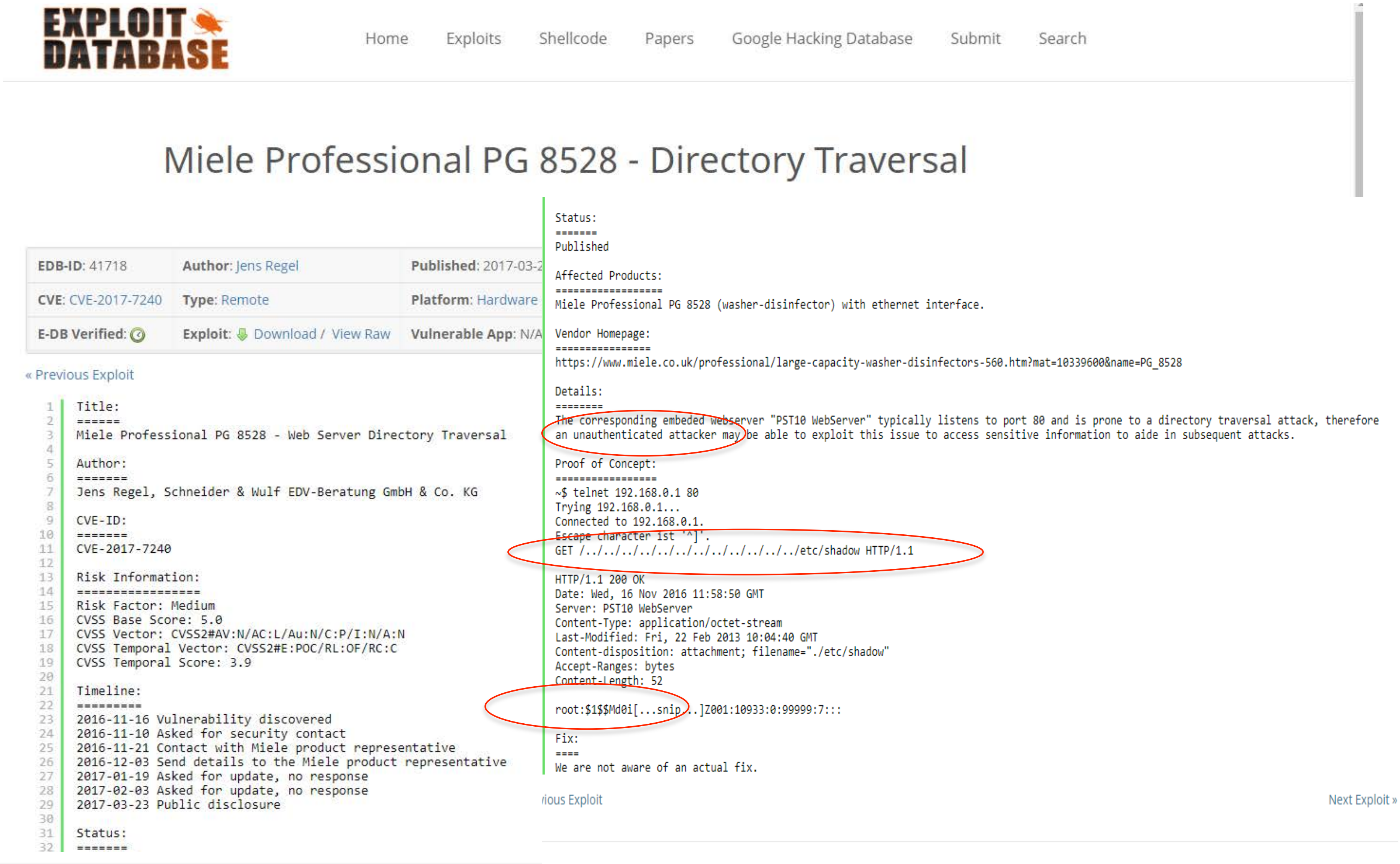
Hôpitaux Universitaires Genève	Type de document Catégorie procédurale \Procédure HUG	Domaine \ Activité 7. Système d'information \ 7.1 Informatique Instance décisionnelle :	page 2/18 Référence HUGO.SI.IN.0010
PSSI - Technical Security Standard - Information security requirements for technical equipment		N° de version : 3.1	Portée HUG
Publié par Chancellerie	Responsable du document Security Officer	Créé le 18/03/2011 Mise à jour le 31.7.2017	En vigueur à partir du : 18/03/2011

IT security of technical systems — Requirements

This standard defines IT security requirements for technical systems that may be connected to a hospital's computer network. It reflects the consensus of the group of experts known as "HIL" (Hospital Infosec Liaison), representing public health hospitals of the following Swiss cantons: Fribourg, Geneva, Ticino, Va Vaud.

H i L
Hôpitaux Universitaires Genève
CHUV Centre hospitalier universitaire vaudois
Hôpital du Valais Spital Wallis
FHV Fédération des hôpitaux vaudois
HFR hôpital fribourgeois freiburger spital
eoc Ente Ospedaliero Cantonale

UN PEU DE TECHNIQUE



Miele Professional PG 8528 - Directory Traversal

EDB-ID: 41718	**Author:** Jens Regel	**Published:** 2017-03-2
CVE: CVE-2017-7240	**Type:** Remote	**Platform:** Hardware
E-DB Verified:	**Exploit:** Download / View Raw	**Vulnerable App:** N/A

« Previous Exploit

```
Title:
======
Miele Professional PG 8528 - Web Server Directory Traversal

Author:
=======
Jens Regel, Schneider & Wulf EDV-Beratung GmbH & Co. KG

CVE-ID:
=======
CVE-2017-7240

Risk Information:
=================
Risk Factor: Medium
CVSS Base Score: 5.0
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:P/I:N/A:N
CVSS Temporal Vector: CVSS2#E:POC/RL:OF/RC:C
CVSS Temporal Score: 3.9

Timeline:
=========
2016-11-16 Vulnerability discovered
2016-11-10 Asked for security contact
2016-11-21 Contact with Miele product representative
2016-12-03 Send details to the Miele product representative
2017-01-19 Asked for update, no response
2017-02-03 Asked for update, no response
2017-03-23 Public disclosure

Status:
=======
```

```
Status:
=======
Published

Affected Products:
==================
Miele Professional PG 8528 (washer-disinfector) with ethernet interface.

Vendor Homepage:
================
https://www.miele.co.uk/professional/large-capacity-washer-disinfectors-560.htm?mat=10339600&name=PG_8528

Details:
========
The corresponding embeded webserver "PST10 WebServer" typically listens to port 80 and is prone to a directory traversal attack, therefore
an unauthenticated attacker may be able to exploit this issue to access sensitive information to aide in subsequent attacks.

Proof of Concept:
=================
~$ telnet 192.168.0.1 80
Trying 192.168.0.1...
Connected to 192.168.0.1.
Escape character ist '^]'.
GET /../../../../../../../../../../../../etc/shadow HTTP/1.1

HTTP/1.1 200 OK
Date: Wed, 16 Nov 2016 11:58:50 GMT
Server: PST10 WebServer
Content-Type: application/octet-stream
Last-Modified: Fri, 22 Feb 2013 10:04:40 GMT
Content-disposition: attachment; filename="./etc/shadow"
Accept-Ranges: bytes
Content-Length: 52

root:$1$$Md0i[...snip...]Z001:10933:0:99999:7:::

Fix:
====
We are not aware of an actual fix.
```

ious Exploit

Next Exploit »

Merci

Franck CALCAVECCHIA

(CISSP, ISO 27001LA, ISO 27005RM)

Franck.calcavecchia@hcuge.ch

https://www.linkedin.com/in/franckcalcavecchia

https://www.hug-ge.ch/