CIO PERSPECTIVES

FROM IDG

Regional Events for Senior IT Leaders

PRODUCED BY CIO FROM IDG

IDG Communications, Inc.

Think Your Network is Safe? Check All of Your Endpoints

Pamela Dill

Sr. Security Advisory, World Wide HP Security Practice

HP Inc.

Are you concerned about print security?

You should be.

Pam Dill

Sr Security Advisor

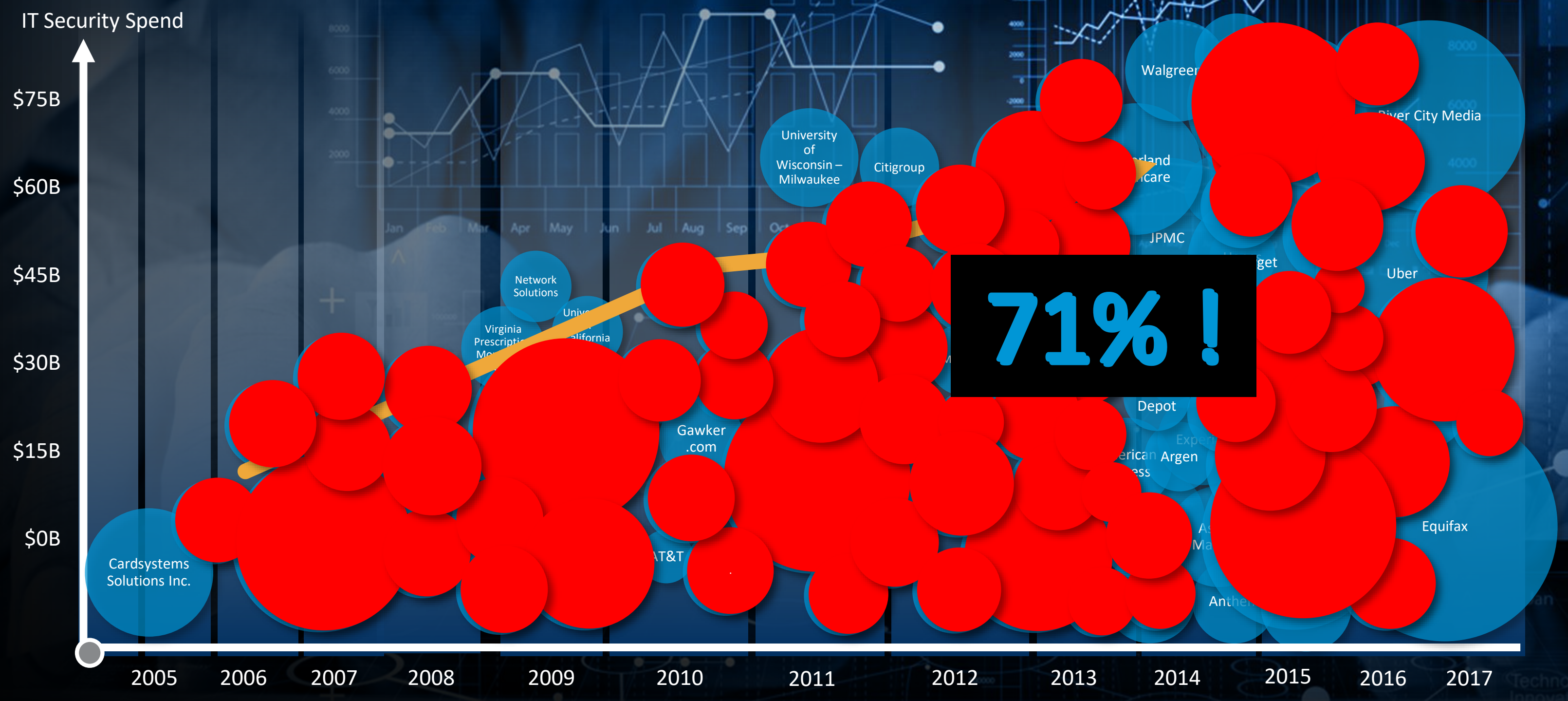
MSc MIS, CNDA, CEH, ISO/IEC 27001 LA

WW Security Practice HP, Inc.

Do you know your **print security** risk profile?

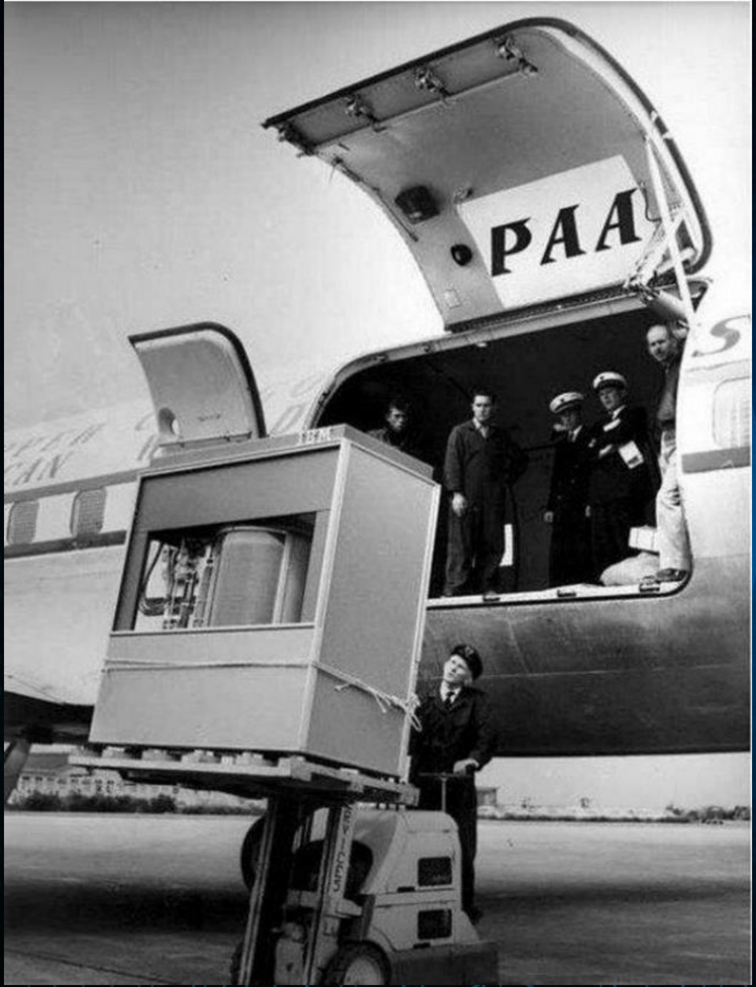
A security risk profile provides a clear and concise understanding of how to **align risk** and security activities with the expectations of the **business** and its **leadership**.

Paying Attention to the Endpoint



Informationisbeautiful.net World's Biggest Data Breaches 2017

Bubble = Size of breach



In 1956, a 5mb HDD being loaded onto a plane.

64gb microSD

The risk is real

It’s easy for hackers to break into unsecured printers

“I probe around for a multifunction printer and see that it is configured with default passwords. Great, I am in…”

Peter Kim
Industry-leading Penetration Tester, Hacker, Author

The risk is real

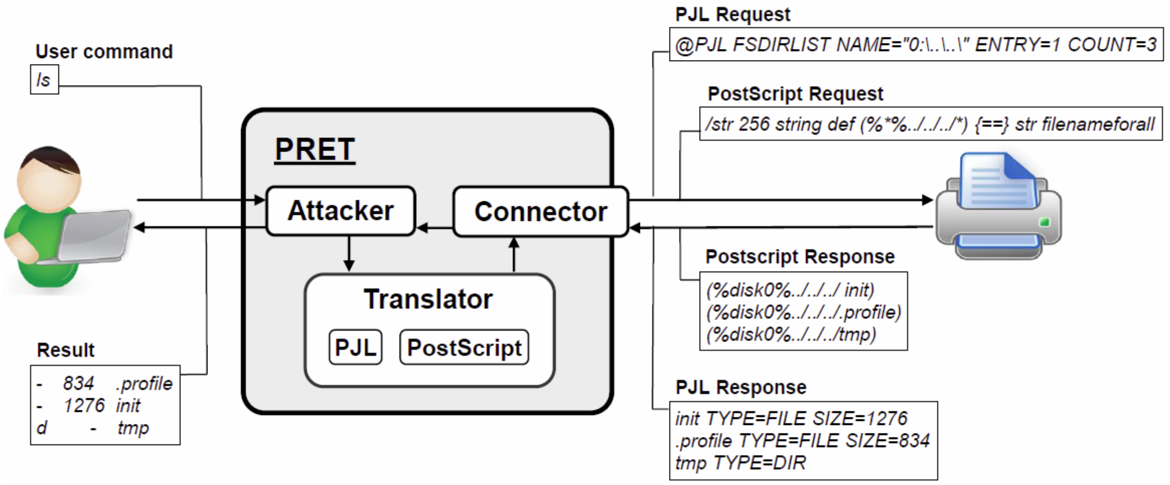
It’s easy for hackers to break into unsecured printers

“We've compromised a number of companies using **printers as our initial foothold**. We move laterally from the printer, find Active Directory, query it with an account from the printer and bingo, **we hit GOLD**…”

Jens Müller - **Exploiting Network Printers**

PRinter **E**xploitation **T**oolkit (PRET)

Hacking Printers Wiki



User command

```
ls
```

PJL Request

```
@PJL FSDIRLIST NAME="0:\..\..\" ENTRY=1 COUNT=3
```

PostScript Request

```
/str 256 string def (%*%../../../*) {==} str filenameforall
```

Postscript Response

```
(%disk0%../../../ init)
(%disk0%../../../.profile)
(%disk0%../../../tmp)
```

PJL Response

```
init TYPE=FILE SIZE=1276
.profile TYPE=FILE SIZE=834
tmp TYPE=DIR
```

Result

```
-   834   .profile
-   1276  init
d     -   tmp
```

https://www.blackhat.com/docs/us-17/thursday/us-17-Mueller-Exploiting-Network-Printers.pdf

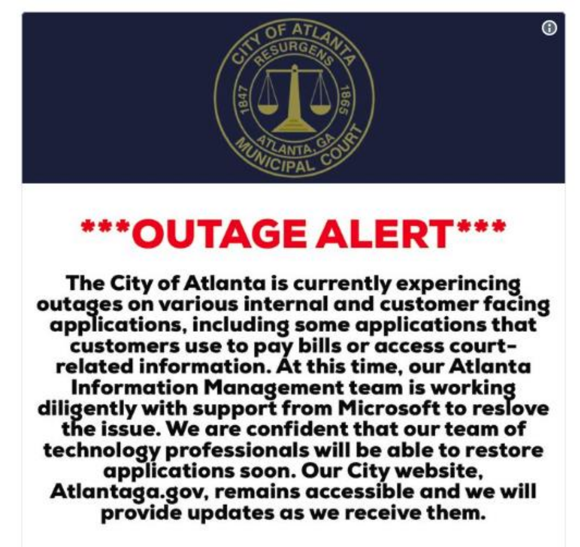
Today’s printers act a whole lot like PCs

Yet only 16% of companies think printers are a high security risk.*

- Hardware
- Email
- Network access
- Firmware and software
- Internet

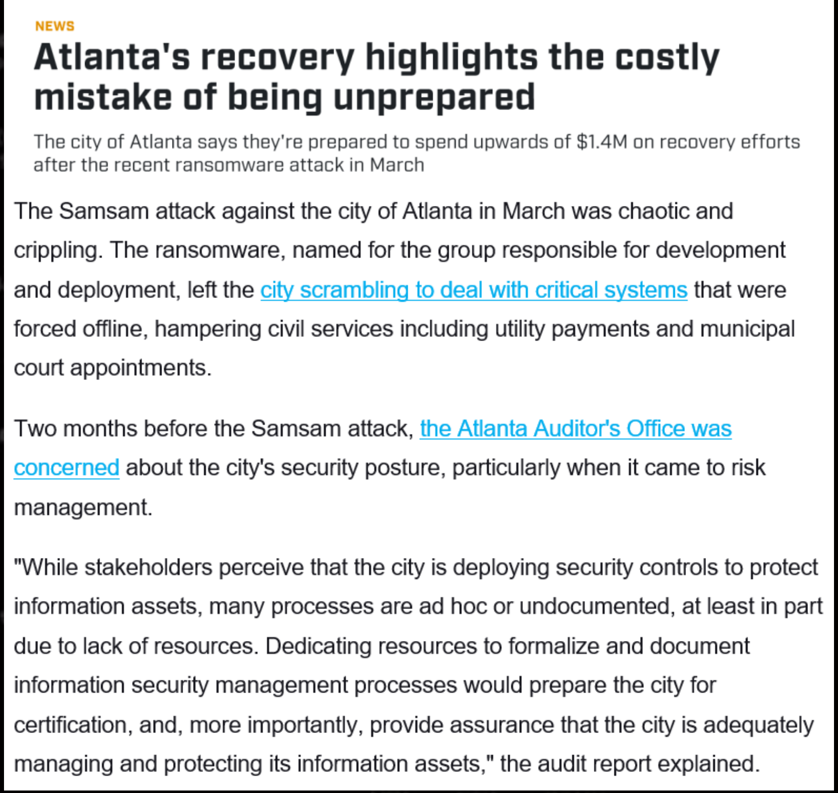
Known Attacks

March 2018



*****OUTAGE ALERT*****

The City of Atlanta is currently experincing outages on various internal and customer facing applications, including some applications that customers use to pay bills or access court-related information. At this time, our Atlanta Information Management team is working diligently with support from Microsoft to reslove the issue. We are confident that our team of technology professionals will be able to restore applications soon. Our City website, Atlantaga.gov, remains accessible and we will provide updates as we receive them.



NEWS

Atlanta's recovery highlights the costly mistake of being unprepared

The city of Atlanta says they're prepared to spend upwards of $1.4M on recovery efforts after the recent ransomware attack in March

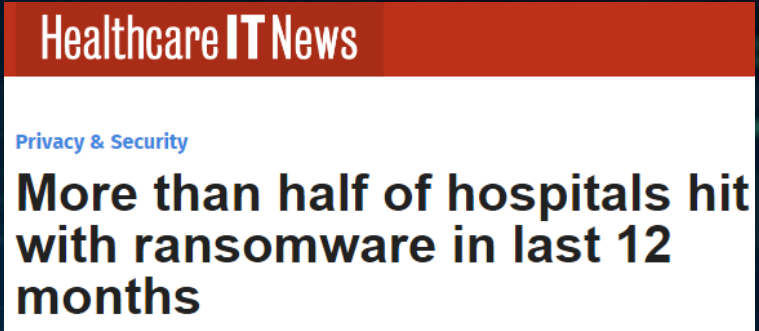
The Samsam attack against the city of Atlanta in March was chaotic and crippling. The ransomware, named for the group responsible for development and deployment, left the city scrambling to deal with critical systems that were forced offline, hampering civil services including utility payments and municipal court appointments.

Two months before the Samsam attack, the Atlanta Auditor's Office was concerned about the city's security posture, particularly when it came to risk management.

"While stakeholders perceive that the city is deploying security controls to protect information assets, many processes are ad hoc or undocumented, at least in part due to lack of resources. Dedicating resources to formalize and document information security management processes would prepare the city for certification, and, more importantly, provide assurance that the city is adequately managing and protecting its information assets," the audit report explained.

January 2018 exploit critical vulnerabilities in processors

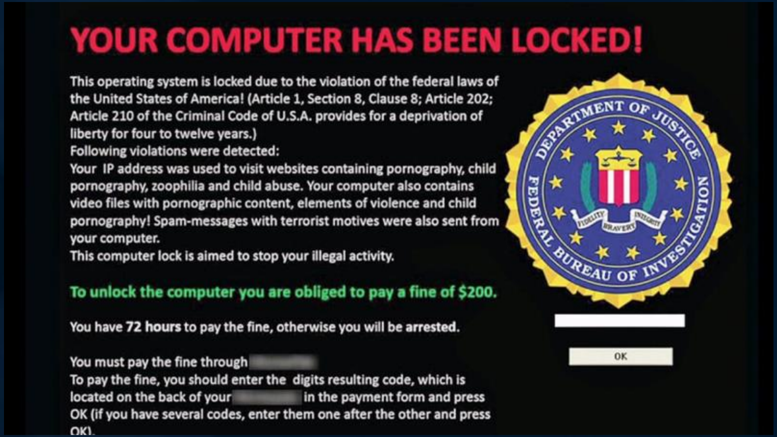
May 2017 Ransomware hits more than 12,000 drives



Healthcare IT News

Privacy & Security

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



YOUR COMPUTER HAS BEEN LOCKED!

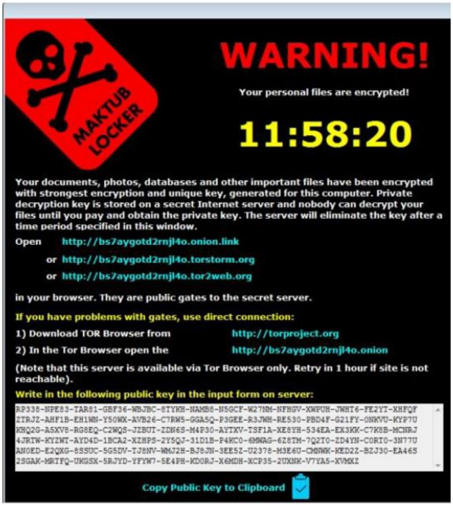
This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have **72 hours** to pay the fine, otherwise you will be arrested.

You must pay the fine through [redacted]
To pay the fine, you should enter the digits resulting code, which is located on the back of your [redacted] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).

OK



WARNING!

Your personal files are encrypted!

11:58:20

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer. Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key. The server will eliminate the key after a time period specified in this window.

Open http://bs7aygotd2rnjl4o.onion.link
or http://bs7aygotd2rnjl4o.torstorm.org
or http://bs7aygotd2rnjl4o.tor2web.org

in your browser. They are public gates to the secret server.

If you have problems with gates, use direct connection:

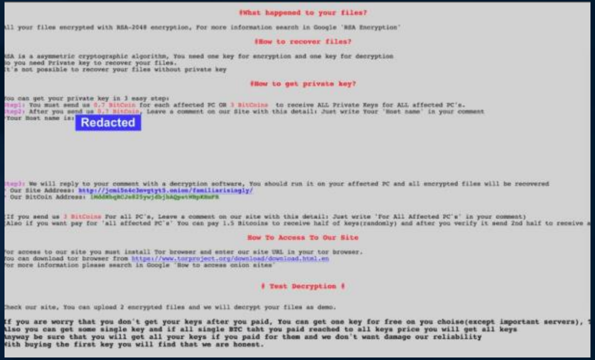
1) Download TOR Browser from http://torproject.org
2) In the Tor Browser open the http://bs7aygotd2rnjl4o.onion

(Note that this server is available via Tor Browser only. Retry in 1 hour if site is not reachable).

Write in the following public key in the input form on server:

```
RP338-NPE83-TAR81-GBF36-WBJBC-8TYKH-NAMB8-N5GCF-W27NM-NFHGV-XWPUH-JWHT6-FE2YT-XHFQF
ZTRJZ-AHF1B-EH1WN-Y50WX-AVB26-C7RW5-GGA5Q-P3GEE-R3JWH-RE530-PBD4F-G21FY-0NKVU-KYP7U
KHQ2G-A5XV8-RG8EQ-C2WQS-JZBUT-ZDN6S-M4P30-AYTXV-TSF1A-XE8YH-534EA-EX3KK-C7K8B-MCHRJ
4JRTW-KYZWT-AYD4D-1BCA2-XZHPS-2Y5QJ-31D1B-P4KC0-6MWAG-6Z8TM-7Q2T0-ZD4YN-C0RT0-3N77U
AN0ED-E2QXG-8SSUC-5G5DV-TJ8NV-WMJ2H-BJ8JN-3EE5Z-U2378-M3E6U-CMNWK-KED2Z-BZJ30-EA46S
2SGAK-MRTFQ-UKGSX-5RJYD-YFYW7-5E4PH-KD0RJ-X6MDH-XCP35-2UXNK-V7YA5-XVMXZ
```

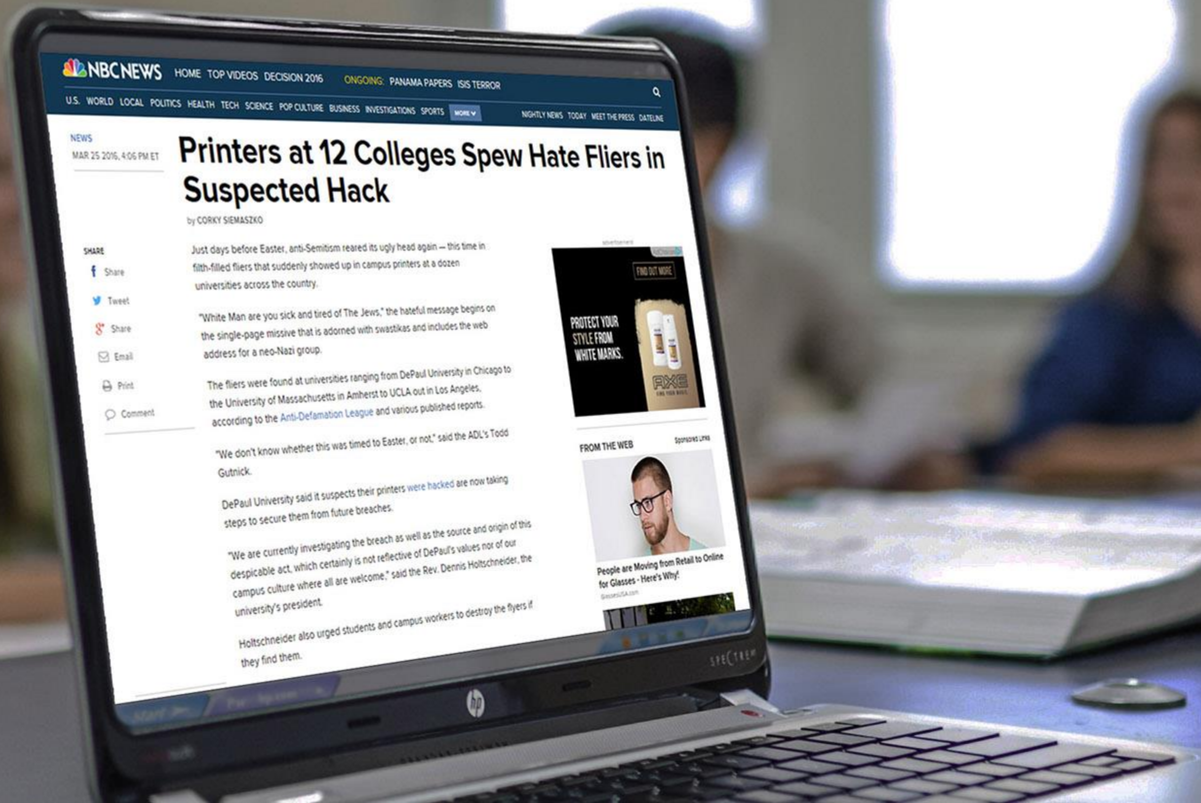
Copy Public Key to Clipboard



```
                     #What happened to your files?
All your files encrypted with RSA-2048 encryption, For more information search in Google 'RSA Encryption'
                        #How to recover files?
RSA is a asymmetric cryptographic algorithm, You need one key for encryption and one key 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 get your private key in 3 easy step:
Step1: You must send us 0.7 BitCoin for each affected PC OR 3 BitCoins  to receive ALL Private Keys for ALL affected PC's.
Step2: After you send us 0.7 BitCoin, Leave a comment on our Site with this detail: Just write Your 'Host name' in your comment
*Your Host name is: Redacted

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 Site Address: http://jcmi5n4c3mvgtyt5.onion/familiarisingly/
* Our BitCoin Address: 1MddNbqRCJe825ywjdbjhAQpetWhpKBmFR

(If you send us 3 BitCoins For all PC's, Leave a comment on our site with this detail: Just write 'For All Affected PC's' in your comment)
(Also if you want pay for 'all affected PC's' You can pay 1.5 Bitcoins to receive half of keys(randomly) and after you verify it send 2nd half to receive a
                       How To Access To Our Site
For access to our site you must install Tor browser and enter our site URL in your tor browser.
You can download tor browser from https://www.torproject.org/download/download.html.en
For more information please search in Google 'How to access onion sites'

                         # Test Decryption #

Check our site, You can upload 2 encrypted files and we will decrypt your files as demo.
If you are worry that you don't get your keys after you paid, You can get one key for free on you choise(except important servers), t
Also you can get some single key and if all single BTC taht you paid reached to all keys price you will get all keys
Anyway be sure that you will get all your keys if you paid for them and we don't want damage our reliability
With buying the first key you will find that we are honest.
```

29,000 printers exploited

Real-world events reveal an alarming trend



NEWS
MAR 25 2016, 4:06 PM ET

Printers at 12 Colleges Spew Hate Fliers in Suspected Hack

by CORKY SIEMASZKO

Just days before Easter, anti-Semitism reared its ugly head again — this time in filth-filled fliers that suddenly showed up in campus printers at a dozen universities across the country.

"White Man are you sick and tired of The Jews," the hateful message begins on the single-page missive that is adorned with swastikas and includes the web address for a neo-Nazi group.

The fliers were found at universities ranging from DePaul University in Chicago to the University of Massachusetts in Amherst to UCLA out in Los Angeles, according to the Anti-Defamation League and various published reports.

"We don't know whether this was timed to Easter, or not," said the ADL's Todd Gutnick.

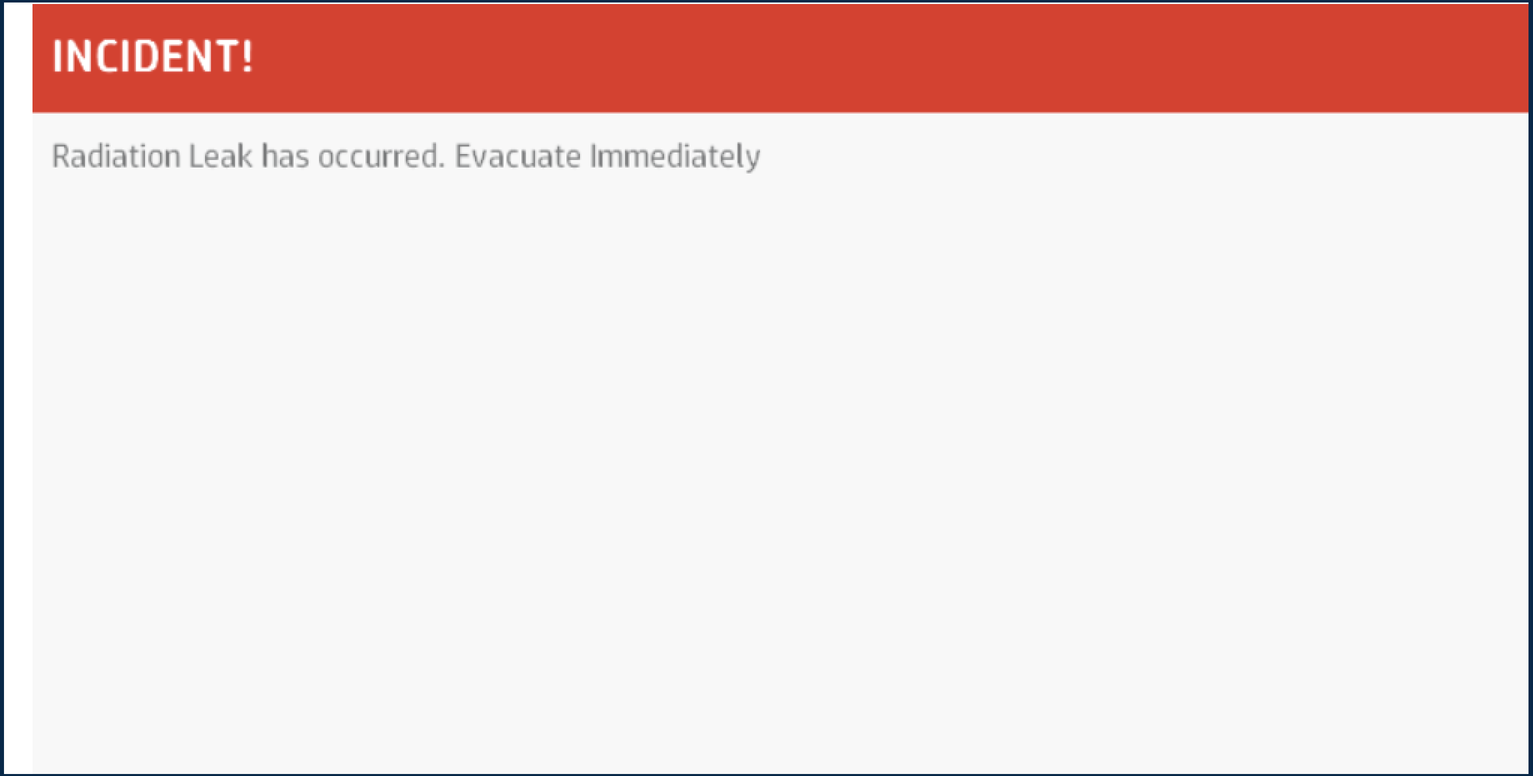
DePaul University said it suspects their printers were hacked are now taking steps to secure them from future breaches.

"We are currently investigating the breach as well as the source and origin of this despicable act, which certainly is not reflective of DePaul's values nor of our campus culture where all are welcome," said the Rev. Dennis Holtschneider, the university's president.

Holtschneider also urged students and campus workers to destroy the flyers if they find them.

People are Moving from Retail to Online for Glasses - Here's Why!
GlassesUSA.com

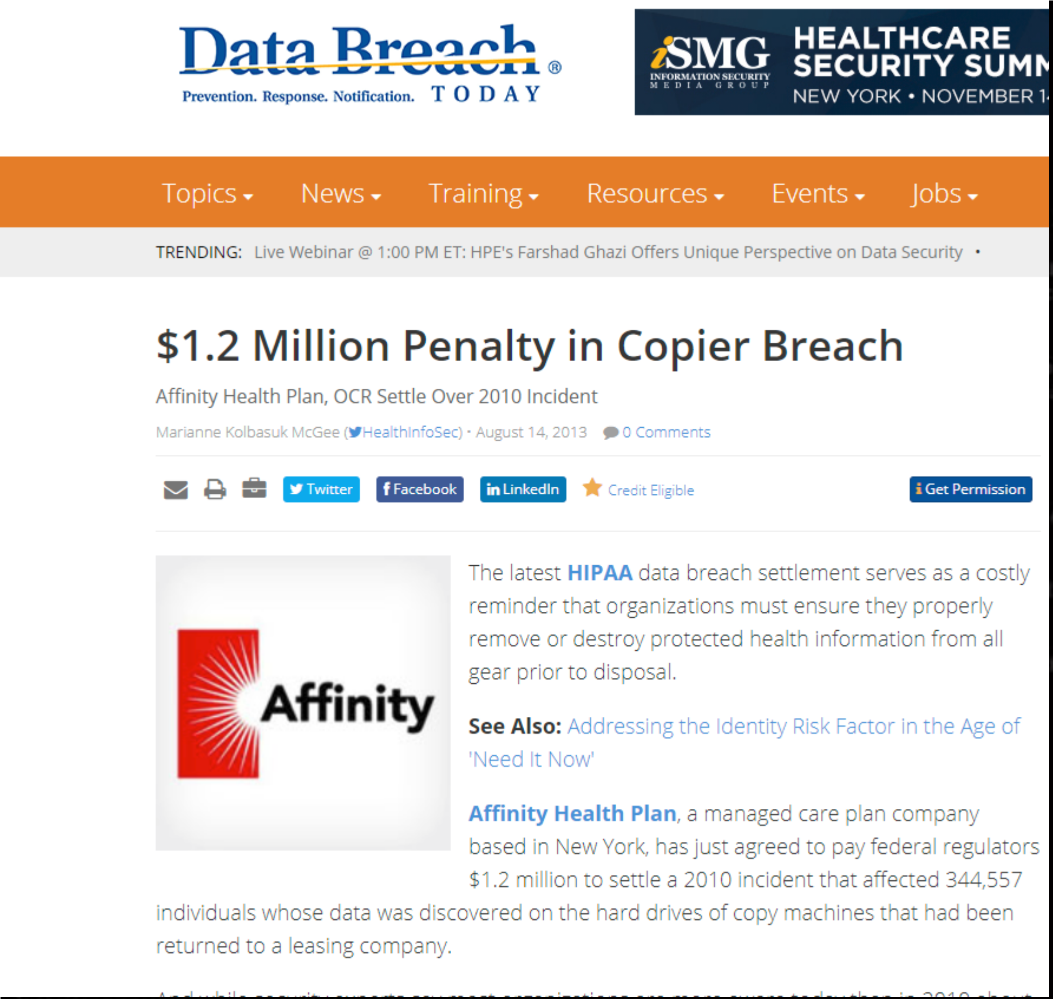
Touchscreen Control Panel of MFP



INCIDENT!

Radiation Leak has occurred. Evacuate Immediately

Affinity Health



TRENDING: Live Webinar @ 1:00 PM ET: HPE's Farshad Ghazi Offers Unique Perspective on Data Security •

$1.2 Million Penalty in Copier Breach

Affinity Health Plan, OCR Settle Over 2010 Incident

Marianne Kolbasuk McGee (HealthInfoSec) • August 14, 2013 0 Comments

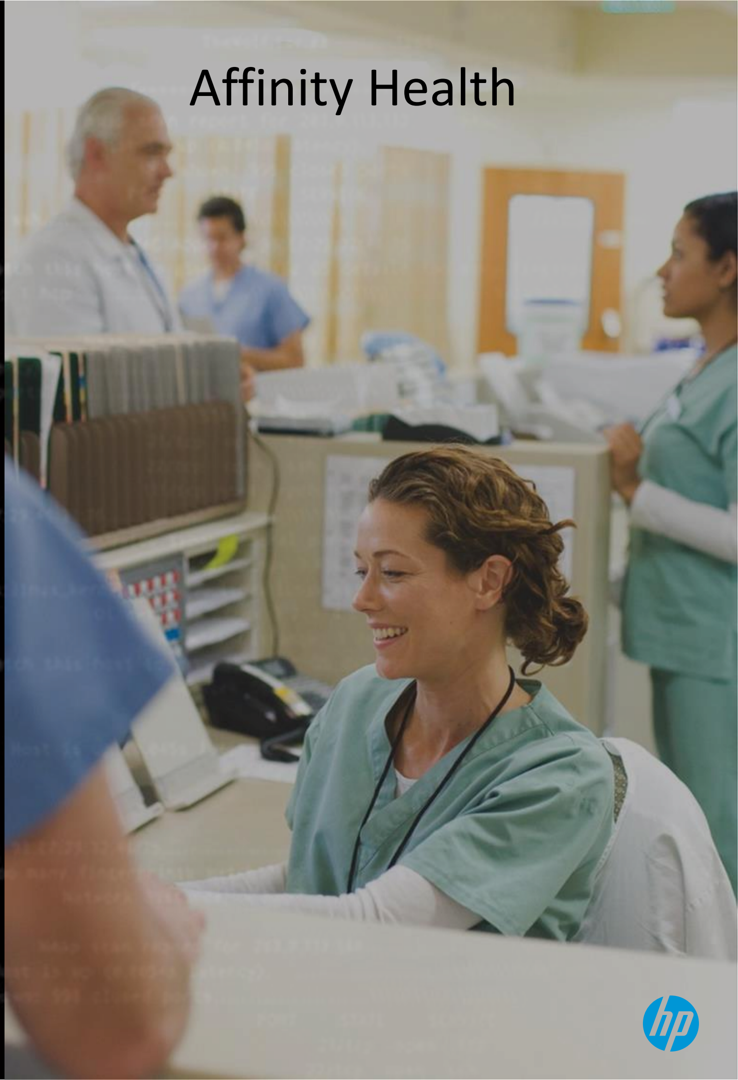
The latest **HIPAA** data breach settlement serves as a costly reminder that organizations must ensure they properly remove or destroy protected health information from all gear prior to disposal.

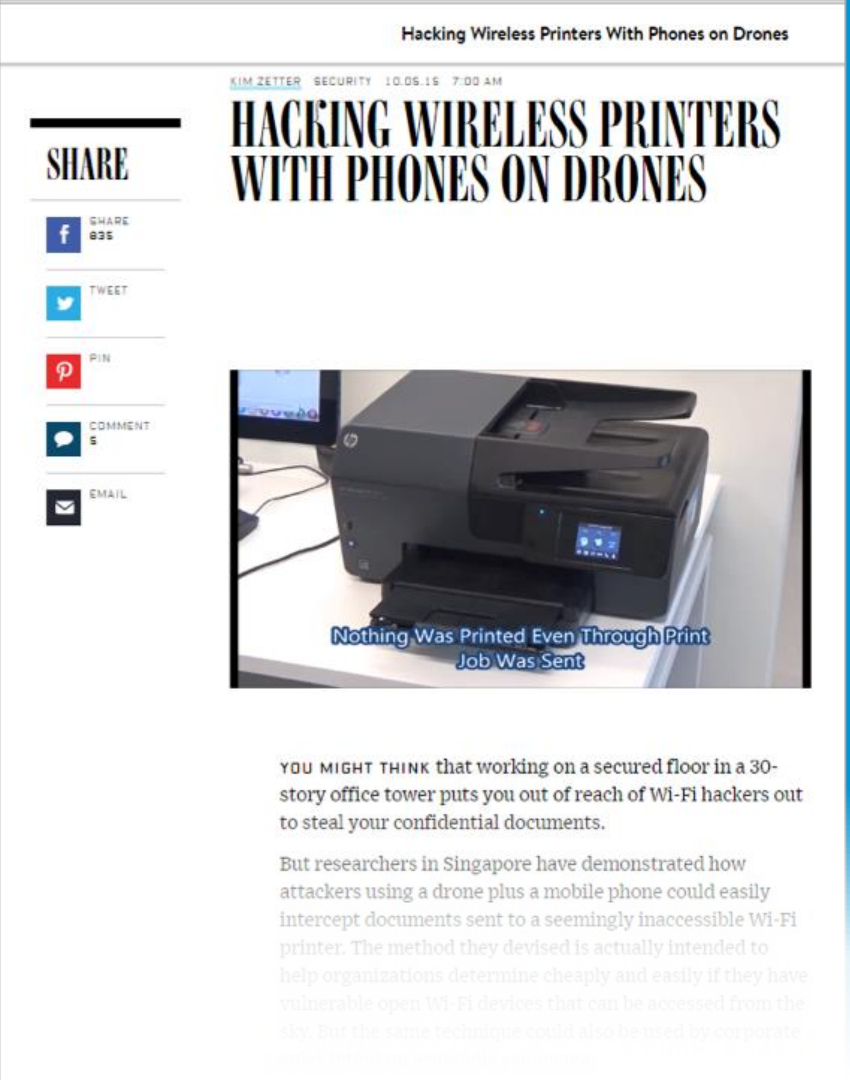
See Also: Addressing the Identity Risk Factor in the Age of 'Need It Now'

Affinity Health Plan, a managed care plan company based in New York, has just agreed to pay federal regulators $1.2 million to settle a 2010 incident that affected 344,557 individuals whose data was discovered on the hard drives of copy machines that had been returned to a leasing company.

And while security experts say most organizations are more aware today than in 2010 about

```
054s latency).      /////////////..............     Host is up (0.0054s latency).
  758 closed ports  /////////////////////.....................     Not shown: 998 closed ports
                    PORT     STATE     SERVICE
```





Hacking Wireless Printers With Phones on Drones

KIM ZETTER SECURITY 10.05.15 7:00 AM

HACKING WIRELESS PRINTERS WITH PHONES ON DRONES

SHARE

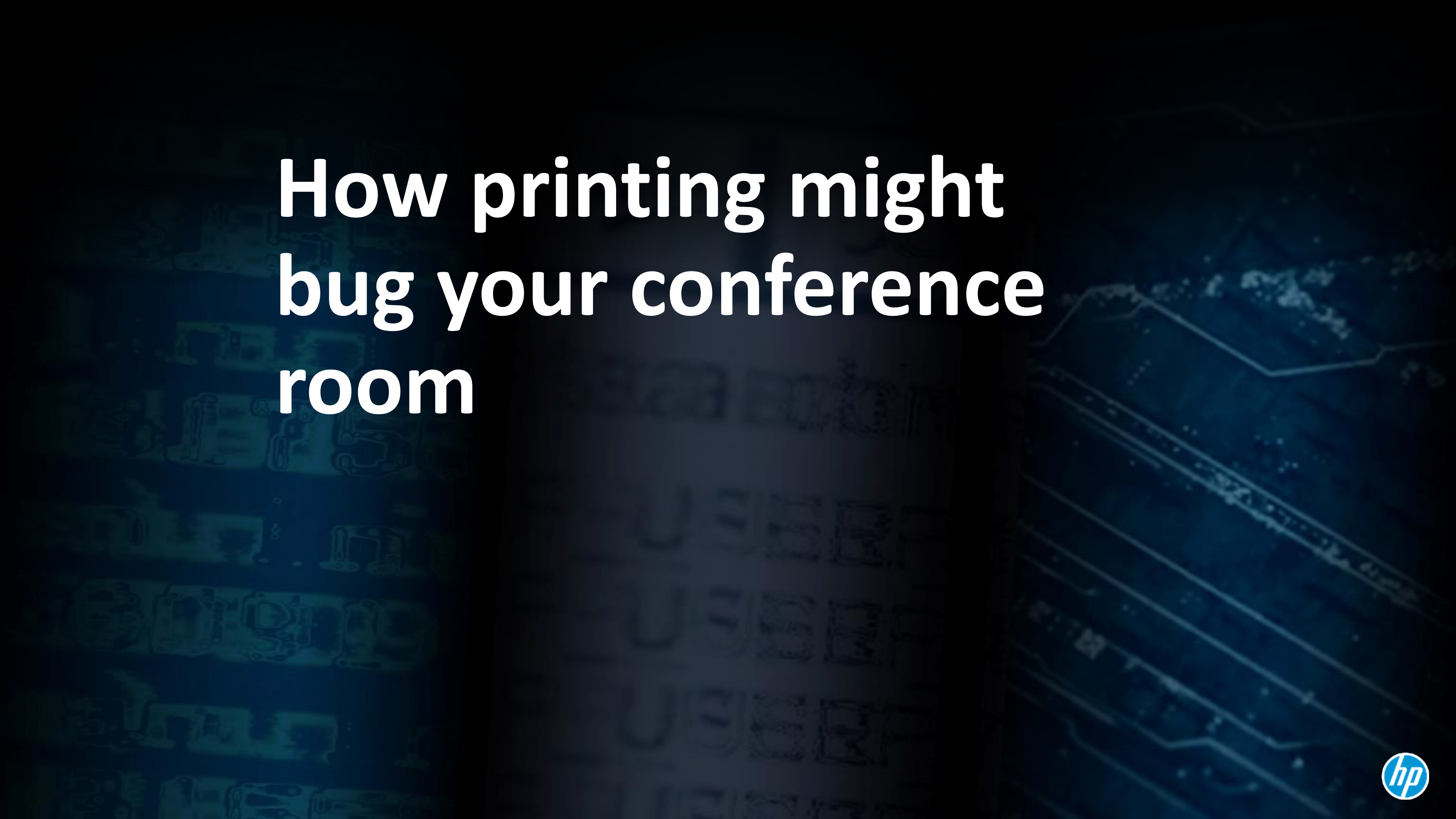
YOU MIGHT THINK that working on a secured floor in a 30-story office tower puts you out of reach of Wi-Fi hackers out to steal your confidential documents.

But researchers in Singapore have demonstrated how attackers using a drone plus a mobile phone could easily intercept documents sent to a seemingly inaccessible Wi-Fi printer. The method they devised is actually intended to help organizations determine cheaply and easily if they have vulnerable open Wi-Fi devices that can be accessed from the sky. But the same technique could also be used by corporate spies intent on economic espionage.

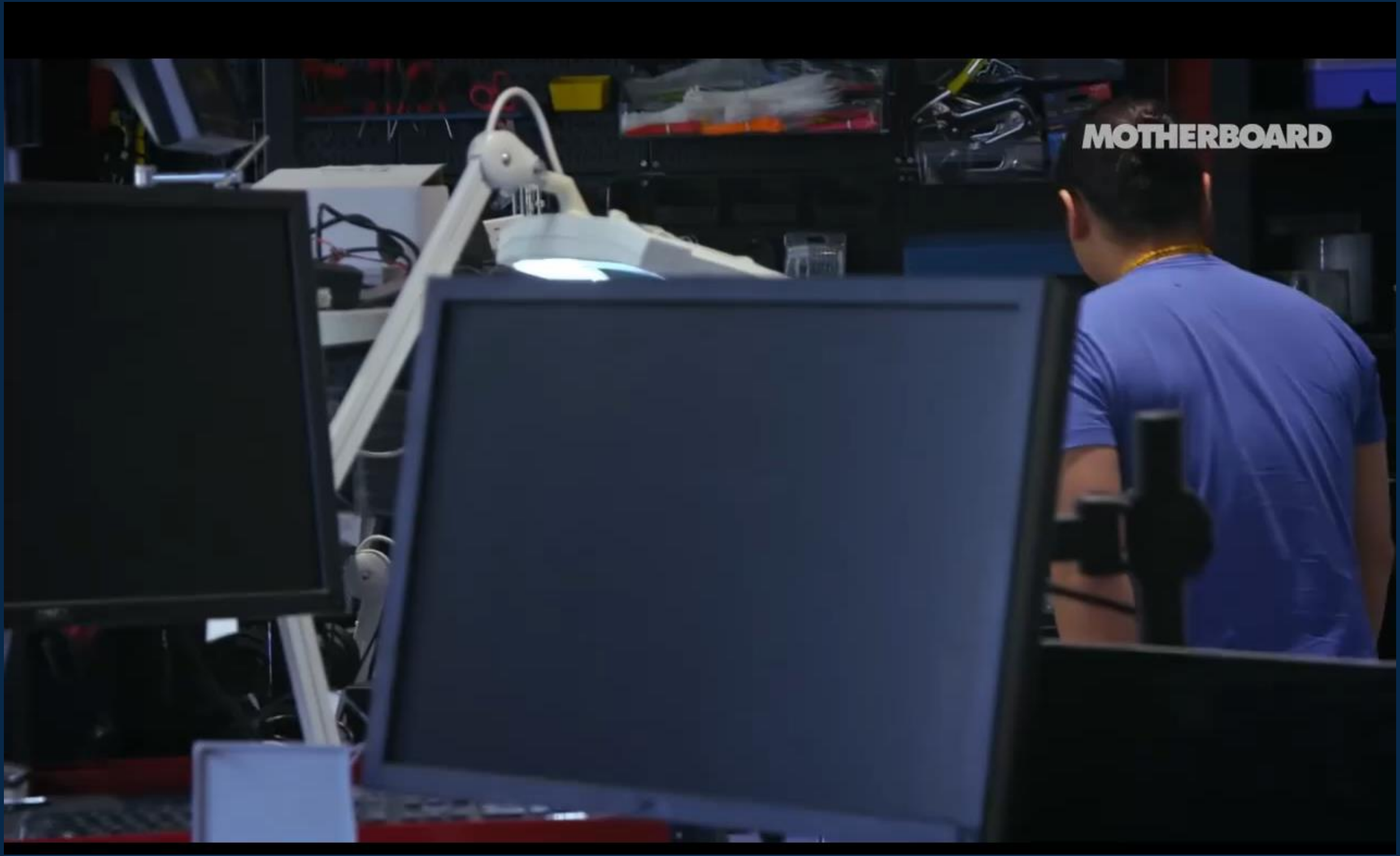
WIRELESS HACKING

Researchers in Singapore developed a drone with a mobile phone that can detect open wireless printers in close proximity then establish the mobile device as a fake access point that mimics the printer and intercepts documents intended for the real device.

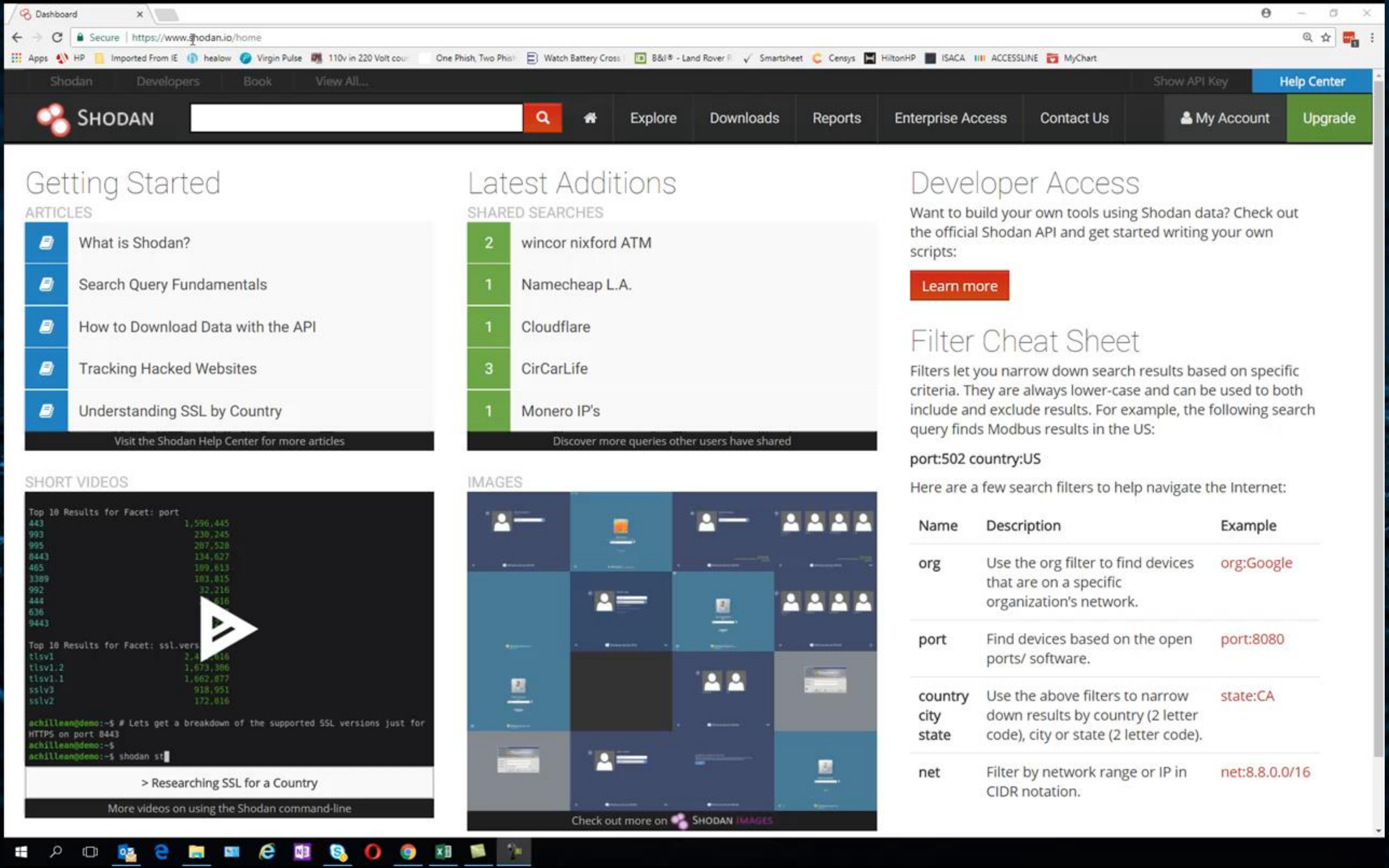
iTrust
Center for Research in Cyber Security



How printing might bug your conference room


MOTHERBOARD

Malware Injection using open ports


Dashboard
Secure | https://www.shodan.io/home
Apps HP Imported From IE healow Virgin Pulse 110v in 220 Volt cou One Phish, Two Phish Watch Battery Cross B&I® - Land Rover R Smartsheet Censys HiltonHP ISACA ACCESSLINE MyChart
Shodan Developers Book View All...
Show API Key
Help Center
SHODAN
Explore Downloads Reports Enterprise Access Contact Us
My Account
Upgrade

Getting Started

ARTICLES

- What is Shodan?
- Search Query Fundamentals
- How to Download Data with the API
- Tracking Hacked Websites
- Understanding SSL by Country

Visit the Shodan Help Center for more articles

SHORT VIDEOS

```
Top 10 Results for Facet: port
443                                    1,596,445
993                                      230,245
995                                      207,528
8443                                     134,627
465                                      109,613
3389                                     103,815
992                                       32,216
444                                          616
636
9443

Top 10 Results for Facet: ssl.vers
tlsv1                                  2,4   016
tlsv1.2                                1,673,306
tlsv1.1                                1,662,877
sslv3                                    918,951
sslv2                                    172,016

achillean@demo:~$ # Lets get a breakdown of the supported SSL versions just for
HTTPS on port 8443
achillean@demo:~$
achillean@demo:~$ shodan st
```

> Researching SSL for a Country

More videos on using the Shodan command-line

Latest Additions

SHARED SEARCHES

2	wincor nixford ATM
1	Namecheap L.A.
1	Cloudflare
3	CirCarLife
1	Monero IP's

Discover more queries other users have shared

IMAGES

Check out more on SHODAN IMAGES

Developer Access

Want to build your own tools using Shodan data? Check out the official Shodan API and get started writing your own scripts:

Learn more

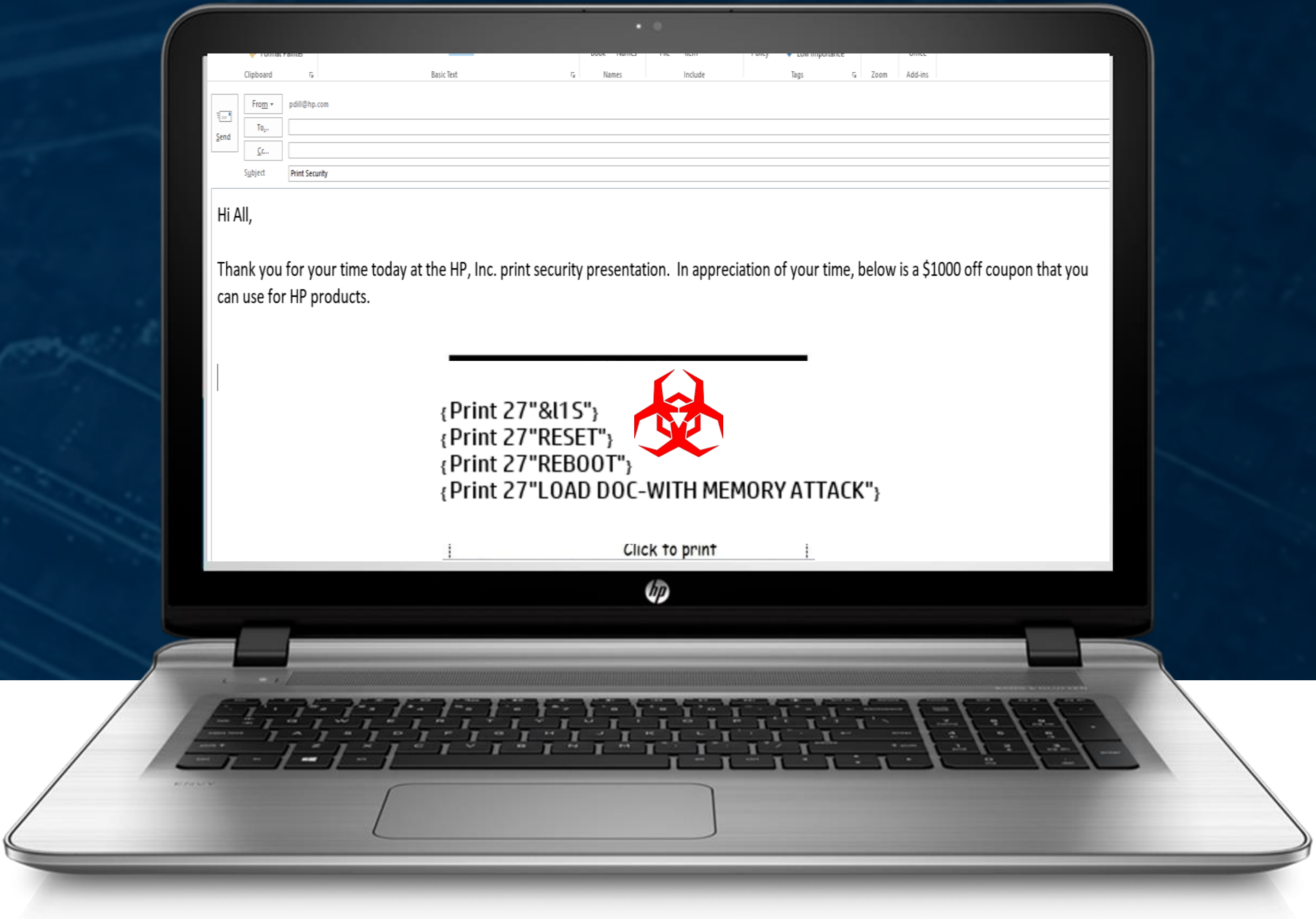
Filter Cheat Sheet

Filters let you narrow down search results based on specific criteria. They are always lower-case and can be used to both include and exclude results. For example, the following search query finds Modbus results in the US:

port:502 country:US

Here are a few search filters to help navigate the Internet:

Name	Description	Example
org	Use the org filter to find devices that are on a specific organization's network.	org:Google
port	Find devices based on the open ports/ software.	port:8080
country city state	Use the above filters to narrow down results by country (2 letter code), city or state (2 letter code).	state:CA
net	Filter by network range or IP in CIDR notation.	net:8.8.0.0/16



From pdill@hp.com

Subject Print Security

Hi All,

Thank you for your time today at the HP, Inc. print security presentation. In appreciation of your time, below is a $1000 off coupon that you can use for HP products.

```
{Print 27"&l1S"}
{Print 27"RESET"}
{Print 27"REBOOT"}
{Print 27"LOAD DOC-WITH MEMORY ATTACK"}
```

- Consult with print security experts
- Assess your environment
- Define and implement a print security policy

Take Action Now

Improve the security of your imaging and printing environment

What will you think the next time you press print ?

www.hp.com/go/ReInventSecurity

Thank You!

Pamela Dill

Sr. Security Advisory, World Wide HP Security Practice

HP Inc.