Introduction to Cyber Security

Ghana Sep ‘19

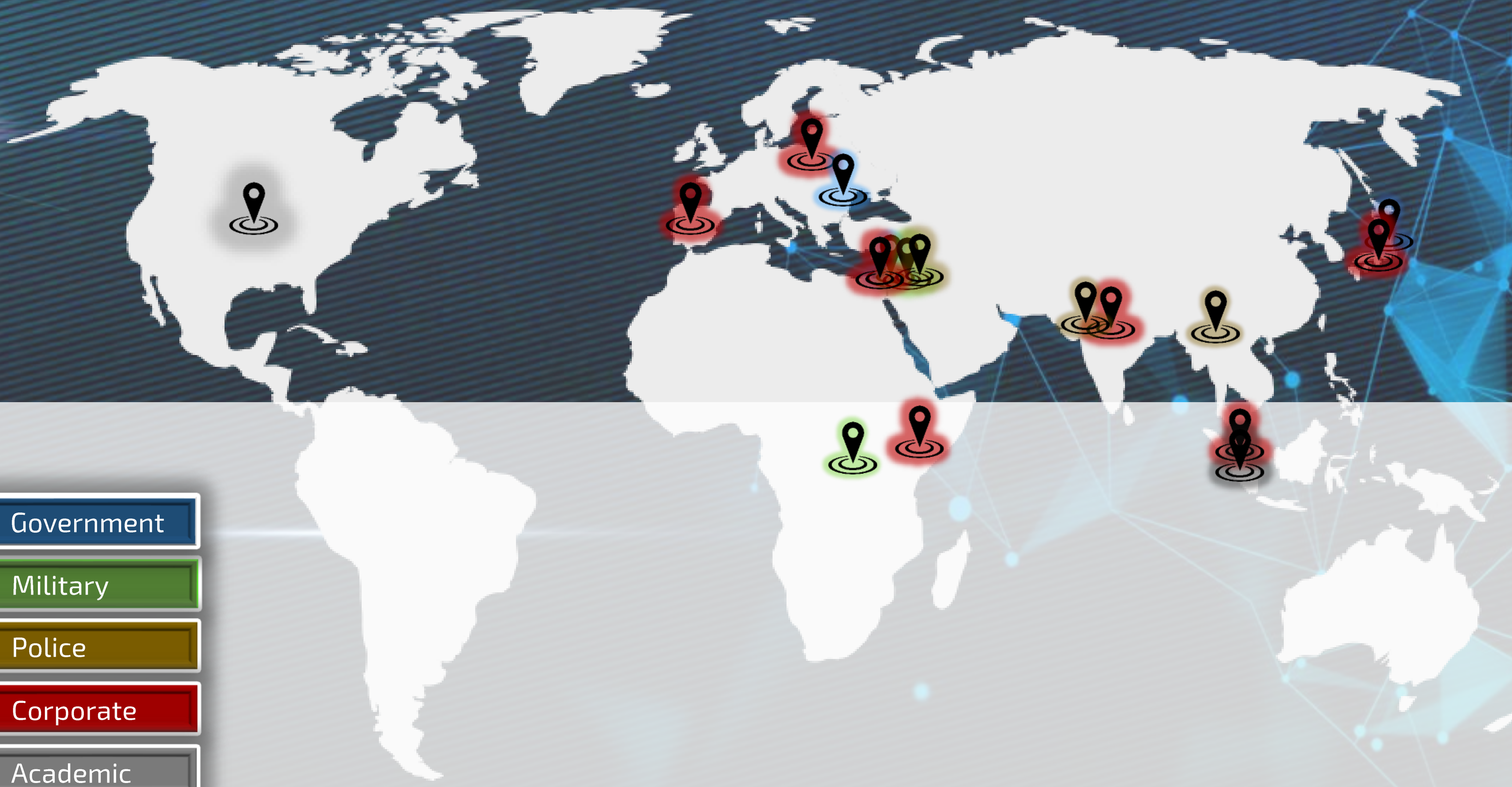
ThinkCyber

The Company

ThinkCyber is an Israeli company focused exclusively on cybersecurity training. ThinkCyber has developed a unique and powerful tool, the CYBERIUM ARENA, to evaluate and train professionals dealing with cybersecurity and cyberterrorism. The company trains army, police, government and corporate cyber units in Israel and around the world, including the IDF’s famed 8200 unit.

The ThinkCyber team constantly upgrades and updates its investigation methodologies, conducting digital investigations on a daily basis.

ThinkCyber Projects

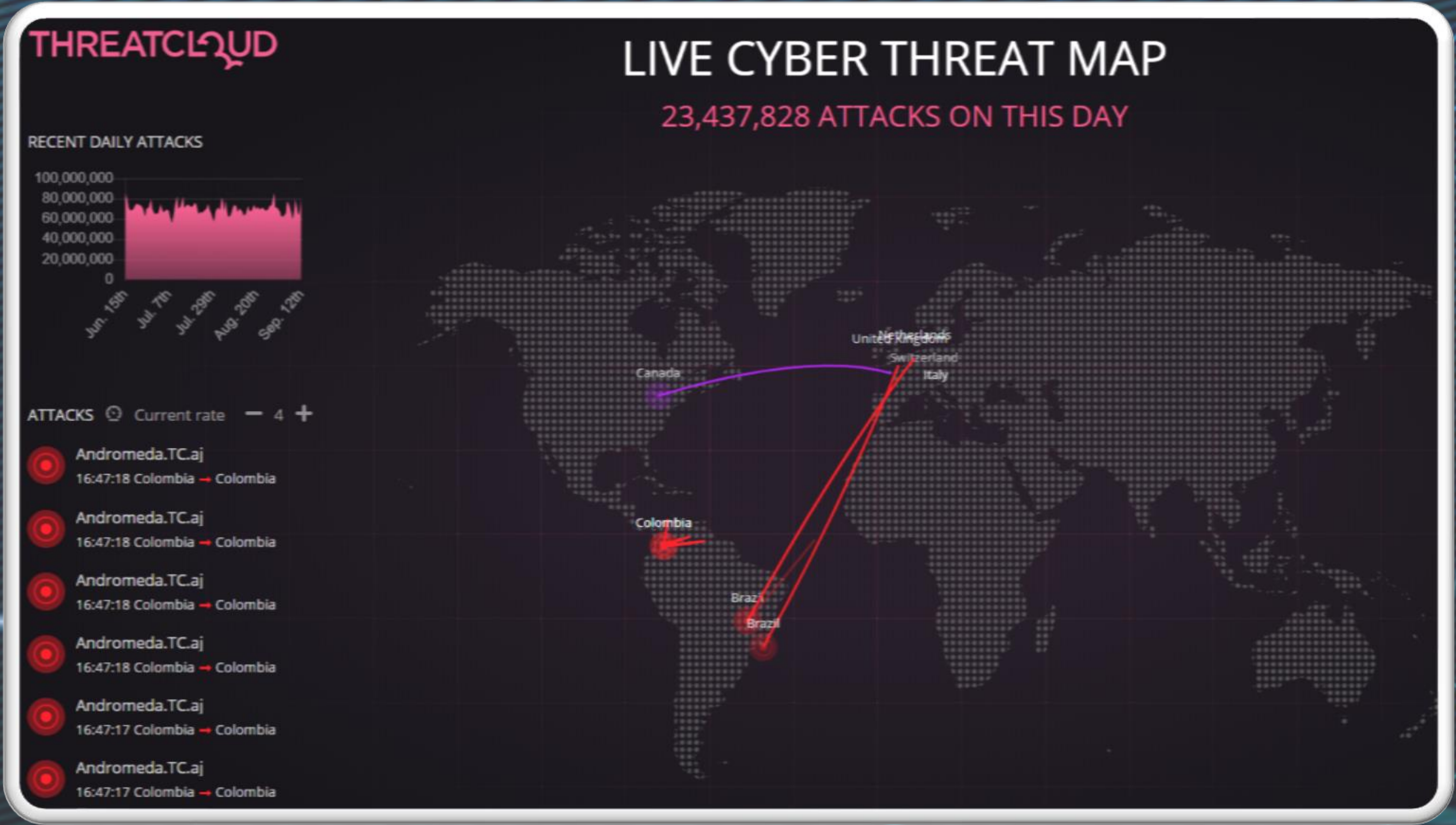


- How many attacks accrue a day?
- Are small businesses under threat as well as the big players?
- What industry is most vulnerable and why?
- What country is most likely to be under attack?

Under attack

ThinkCyber

Live Cyber-Map



THREATCLOUD

LIVE CYBER THREAT MAP

23,437,828 ATTACKS ON THIS DAY

RECENT DAILY ATTACKS

ATTACKS Current rate − 4 +

Andromeda.TC.aj
16:47:18 Colombia → Colombia

Andromeda.TC.aj
16:47:18 Colombia → Colombia

Andromeda.TC.aj
16:47:18 Colombia → Colombia

Andromeda.TC.aj
16:47:18 Colombia → Colombia

Andromeda.TC.aj
16:47:17 Colombia → Colombia

Andromeda.TC.aj
16:47:17 Colombia → Colombia

https://threatmap.checkpoint.com/

ThinkCyber

What happens (in Cyber) every day

There is a hacker attack every **39 seconds**

Every 34 seconds a malicious software/malware is being downloaded

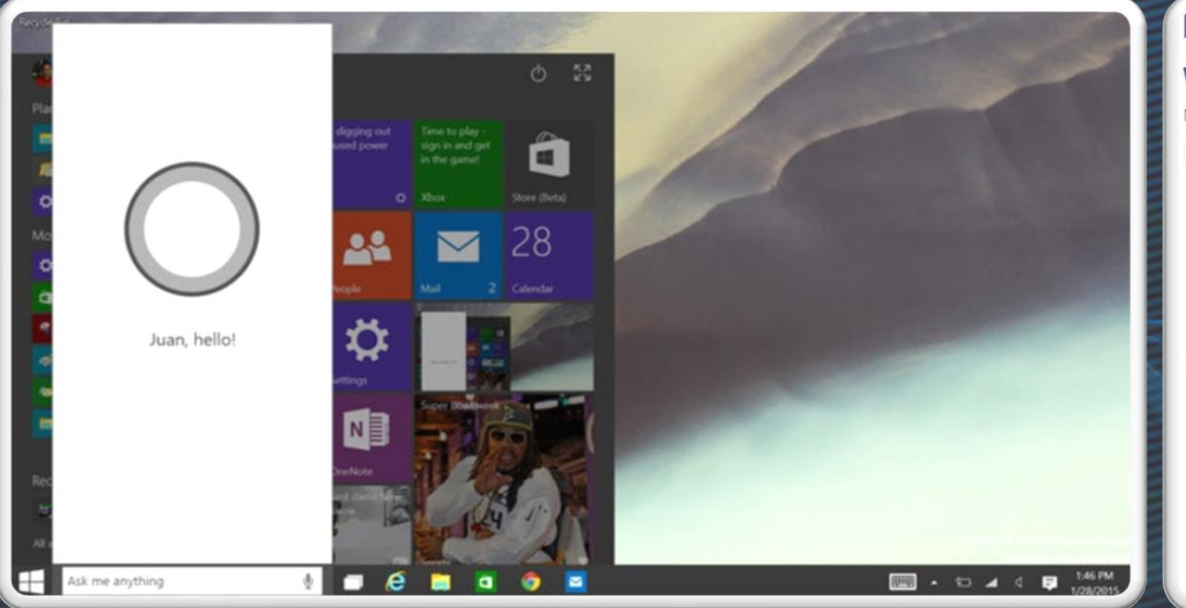
43% of cyber attacks target small business

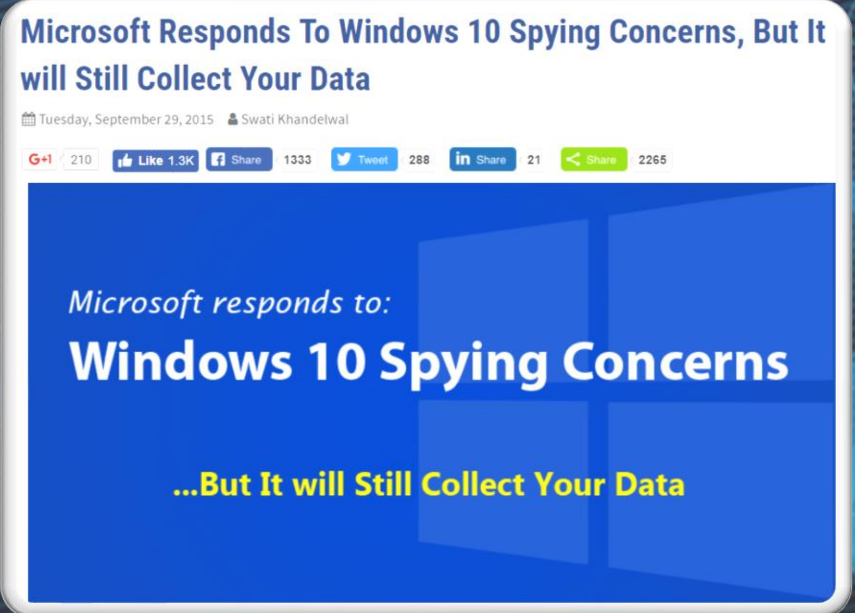
Every 36 minutes sensitive information is being leaked out of an organization

95% of cybersecurity breaches are due to human error

ThinkCyber

Scary facts..





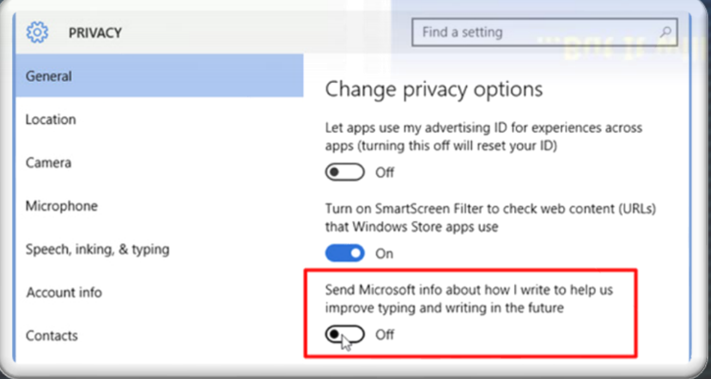
Microsoft Responds To Windows 10 Spying Concerns, But It will Still Collect Your Data

Tuesday, September 29, 2015 Swati Khandelwal

Microsoft responds to:

Windows 10 Spying Concerns

...But It will Still Collect Your Data



Change privacy options

Let apps use my advertising ID for experiences across apps (turning this off will reset your ID)

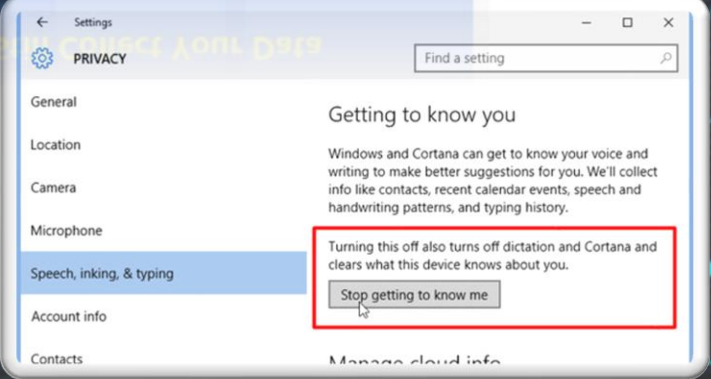
○ Off

Turn on SmartScreen Filter to check web content (URLs) that Windows Store apps use

● On

Send Microsoft info about how I write to help us improve typing and writing in the future

○ Off



Getting to know you

Windows and Cortana can get to know your voice and writing to make better suggestions for you. We'll collect info like contacts, recent calendar events, speech and handwriting patterns, and typing history.

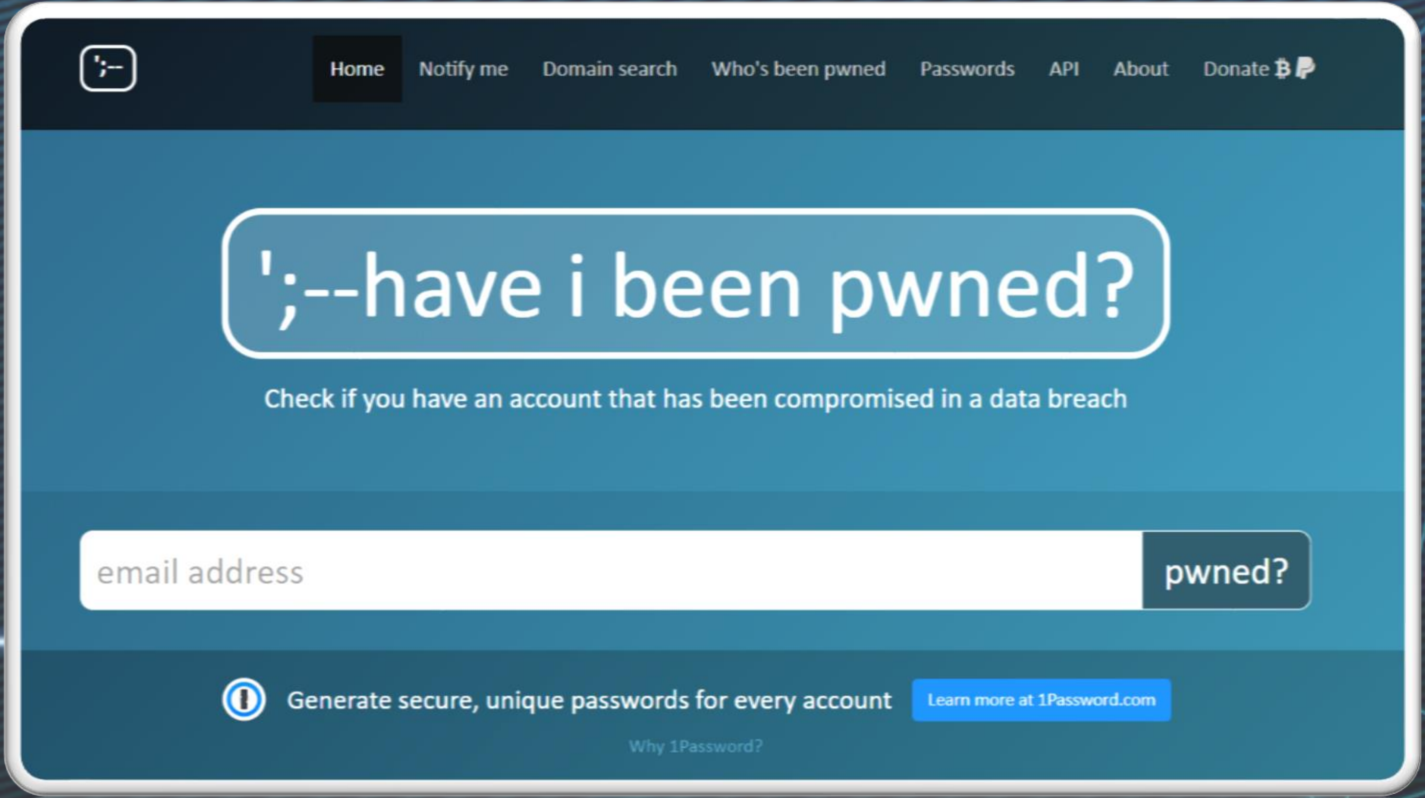
Turning this off also turns off dictation and Cortana and clears what this device knows about you.

Stop getting to know me

Manage cloud info

ThinkCyber

Have you been HACKED?!



';--have i been pwned?

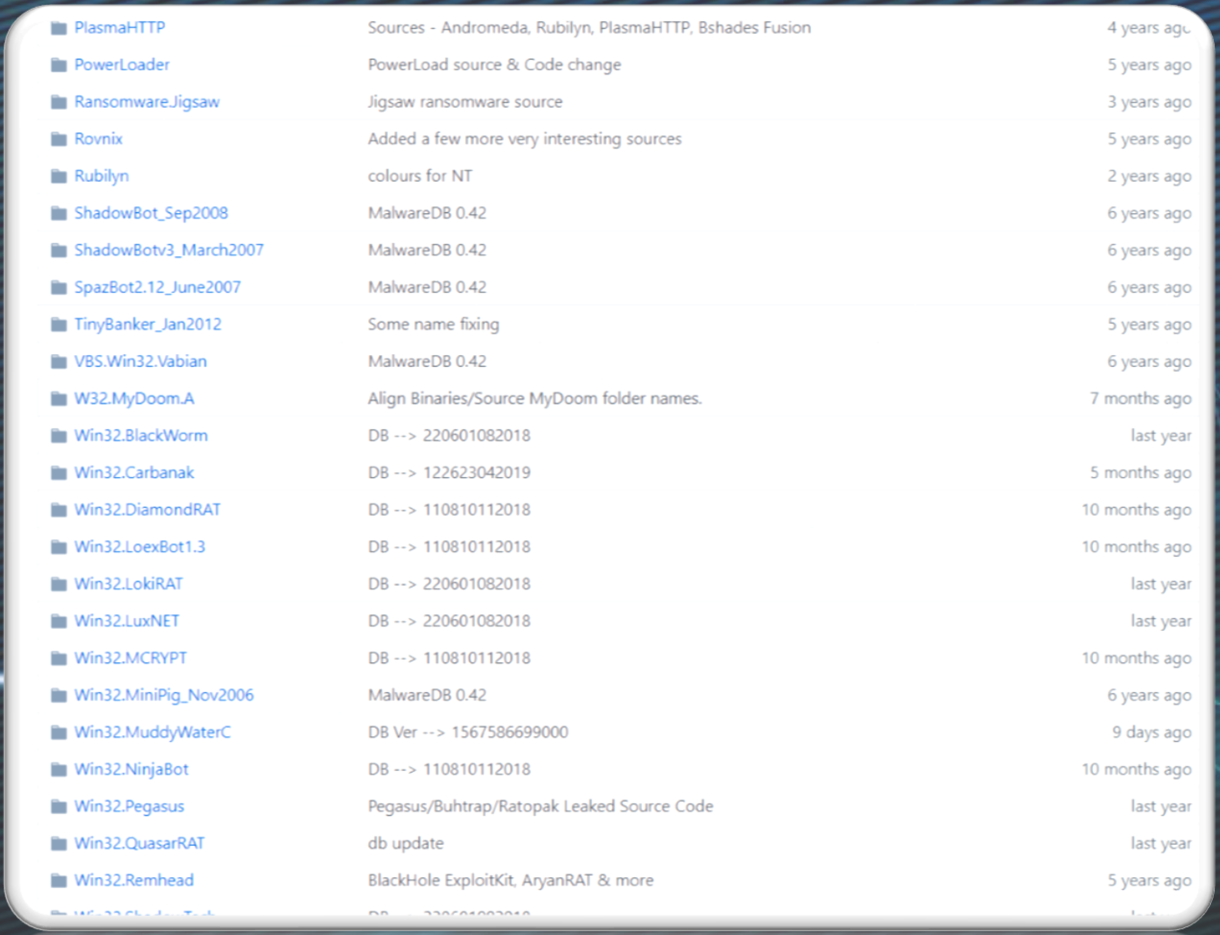
Check if you have an account that has been compromised in a data breach

Generate secure, unique passwords for every account

https://haveibeenpwned.com/

ThinkCyber

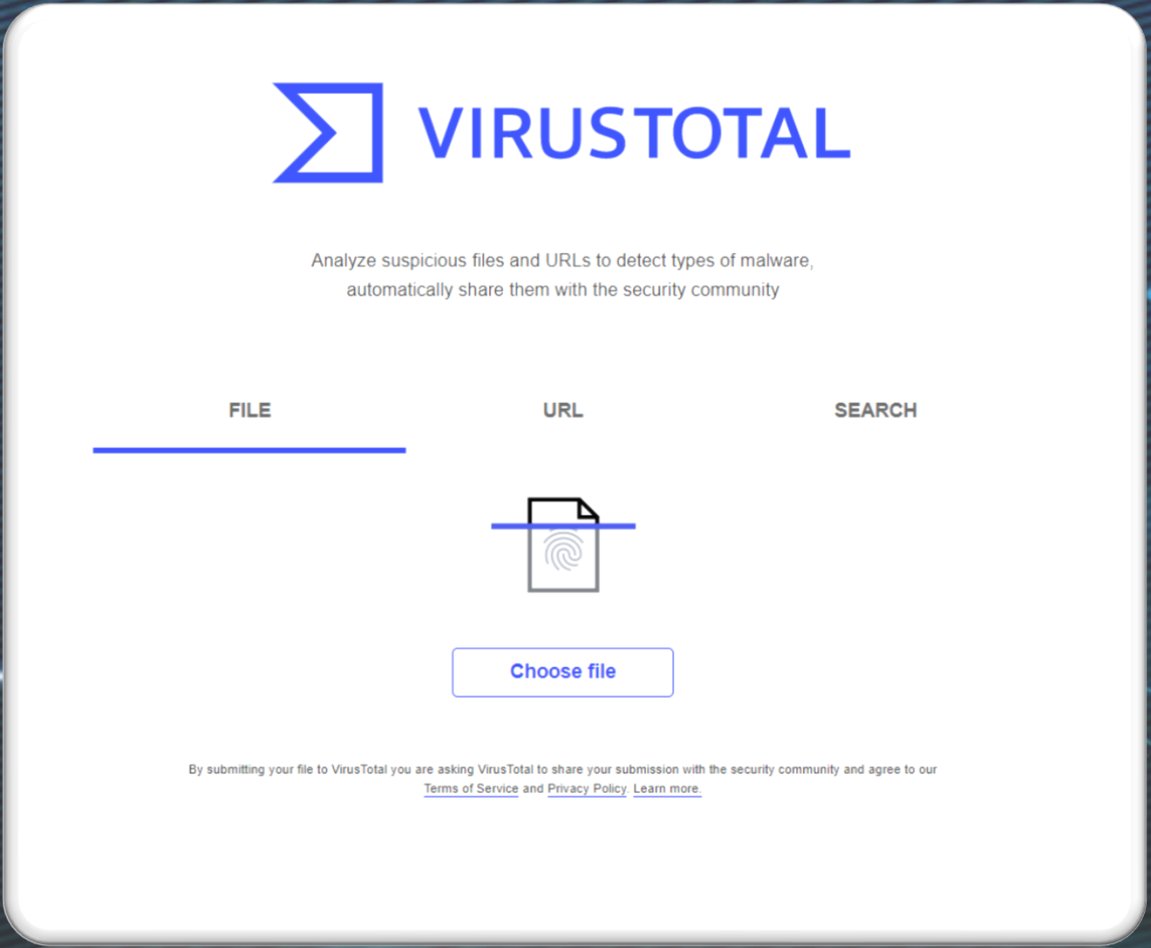
How easy is it really..



PlasmaHTTP	Sources - Andromeda, Rubilyn, PlasmaHTTP, Bshades Fusion	4 years ago
PowerLoader	PowerLoad source & Code change	5 years ago
Ransomware.Jigsaw	Jigsaw ransomware source	3 years ago
Rovnix	Added a few more very interesting sources	5 years ago
Rubilyn	colours for NT	2 years ago
ShadowBot_Sep2008	MalwareDB 0.42	6 years ago
ShadowBotv3_March2007	MalwareDB 0.42	6 years ago
SpazBot2.12_June2007	MalwareDB 0.42	6 years ago
TinyBanker_Jan2012	Some name fixing	5 years ago
VBS.Win32.Vabian	MalwareDB 0.42	6 years ago
W32.MyDoom.A	Align Binaries/Source MyDoom folder names.	7 months ago
Win32.BlackWorm	DB --> 220601082018	last year
Win32.Carbanak	DB --> 122623042019	5 months ago
Win32.DiamondRAT	DB --> 110810112018	10 months ago
Win32.LoexBot1.3	DB --> 110810112018	10 months ago
Win32.LokiRAT	DB --> 220601082018	last year
Win32.LuxNET	DB --> 220601082018	last year
Win32.MCRYPT	DB --> 110810112018	10 months ago
Win32.MiniPig_Nov2006	MalwareDB 0.42	6 years ago
Win32.MuddyWaterC	DB Ver --> 1567586699000	9 days ago
Win32.NinjaBot	DB --> 110810112018	10 months ago
Win32.Pegasus	Pegasus/Buhtrap/Ratopak Leaked Source Code	last year
Win32.QuasarRAT	db update	last year
Win32.Remhead	BlackHole ExploitKit, AryanRAT & more	5 years ago
Win32.ShadowTech	DB --> 220601082018	last year

https://github.com/ytisf/theZoo/tree/master/malwares/Source/Original

Virus Check

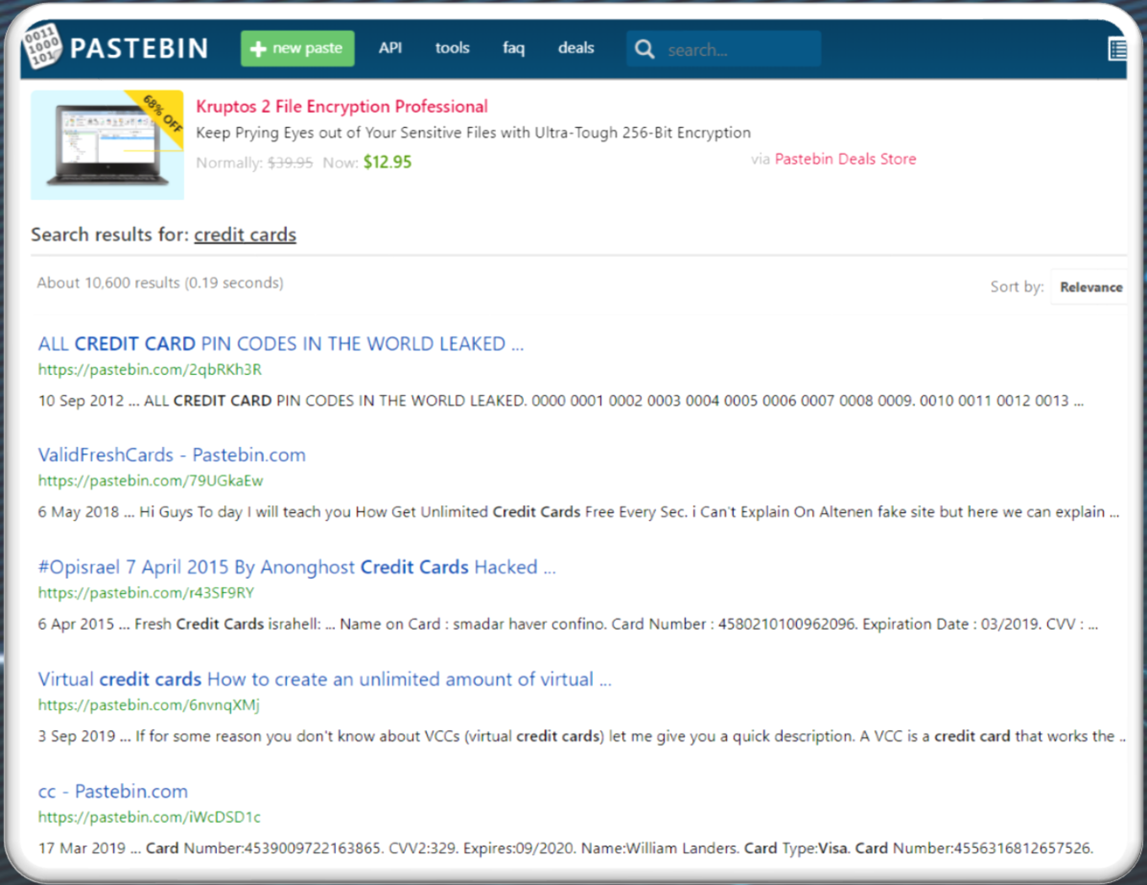


Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community

By submitting your file to VirusTotal you are asking VirusTotal to share your submission with the security community and agree to our Terms of Service and Privacy Policy. Learn more.

https://www.virustotal.com/

Sensitive data around the internet



Kruptos 2 File Encryption Professional

Keep Prying Eyes out of Your Sensitive Files with Ultra-Tough 256-Bit Encryption

Normally: ~~$39.95~~ Now: $12.95 via Pastebin Deals Store

Search results for: credit cards

About 10,600 results (0.19 seconds) Sort by: Relevance

ALL **CREDIT CARD** PIN CODES IN THE WORLD LEAKED ...
https://pastebin.com/2qbRKh3R
10 Sep 2012 ... ALL **CREDIT CARD** PIN CODES IN THE WORLD LEAKED. 0000 0001 0002 0003 0004 0005 0006 0007 0008 0009. 0010 0011 0012 0013 ...

ValidFreshCards - Pastebin.com
https://pastebin.com/79UGkaEw
6 May 2018 ... Hi Guys To day I will teach you How Get Unlimited **Credit Cards** Free Every Sec. i Can't Explain On Altenen fake site but here we can explain ...

#Opisrael 7 April 2015 By Anonghost **Credit Cards** Hacked ...
https://pastebin.com/r43SF9RY
6 Apr 2015 ... Fresh **Credit Cards** israhell: ... Name on Card : smadar haver confino. Card Number : 4580210100962096. Expiration Date : 03/2019. CVV : ...

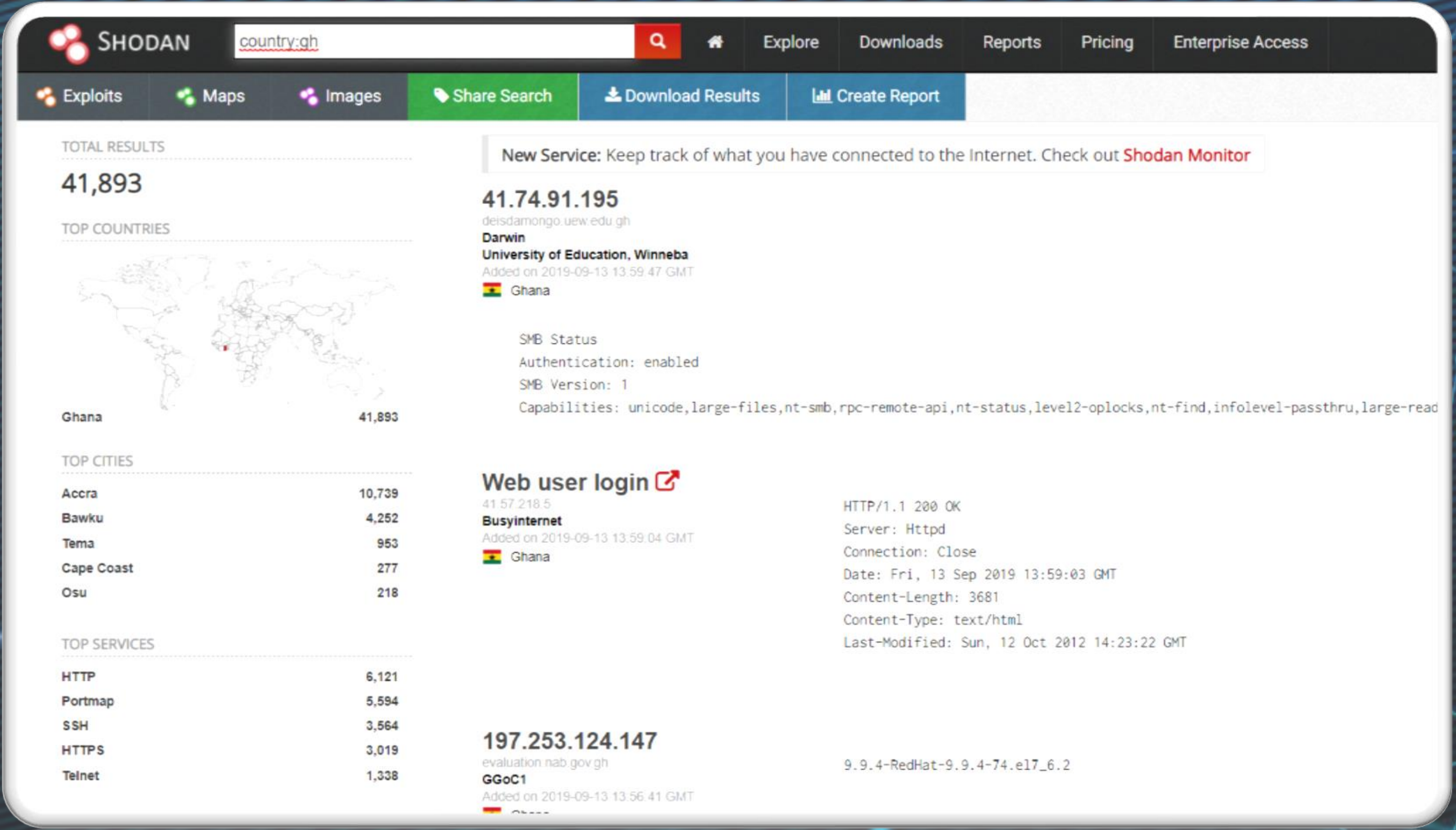
Virtual **credit cards** How to create an unlimited amount of virtual ...
https://pastebin.com/6nvnqXMj
3 Sep 2019 ... If for some reason you don't know about VCCs (virtual **credit cards**) let me give you a quick description. A VCC is a **credit card** that works the ..

cc - Pastebin.com
https://pastebin.com/iWcDSD1c
17 Mar 2019 ... **Card** Number:4539009722163865. CVV2:329. Expires:09/2020. Name:William Landers. **Card** Type:**Visa**. **Card** Number:4556316812657526.

https://pastebin.com

ThinkCyber

How do hackers find us?!



TOTAL RESULTS

41,893

TOP COUNTRIES

Ghana	41,893

TOP CITIES

Accra	10,739
Bawku	4,252
Tema	953
Cape Coast	277
Osu	218

TOP SERVICES

HTTP	6,121
Portmap	5,594
SSH	3,564
HTTPS	3,019
Telnet	1,338

New Service: Keep track of what you have connected to the Internet. Check out Shodan Monitor

41.74.91.195
deisdamongo.uew.edu.gh
Darwin
University of Education, Winneba
Added on 2019-09-13 13:59:47 GMT
Ghana

```
SMB Status
Authentication: enabled
SMB Version: 1
Capabilities: unicode,large-files,nt-smb,rpc-remote-api,nt-status,level2-oplocks,nt-find,infolevel-passthru,large-read
```

Web user login
41.57.218.5
Busyinternet
Added on 2019-09-13 13:59:04 GMT
Ghana

```
HTTP/1.1 200 OK
Server: Httpd
Connection: Close
Date: Fri, 13 Sep 2019 13:59:03 GMT
Content-Length: 3681
Content-Type: text/html
Last-Modified: Sun, 12 Oct 2012 14:23:22 GMT
```

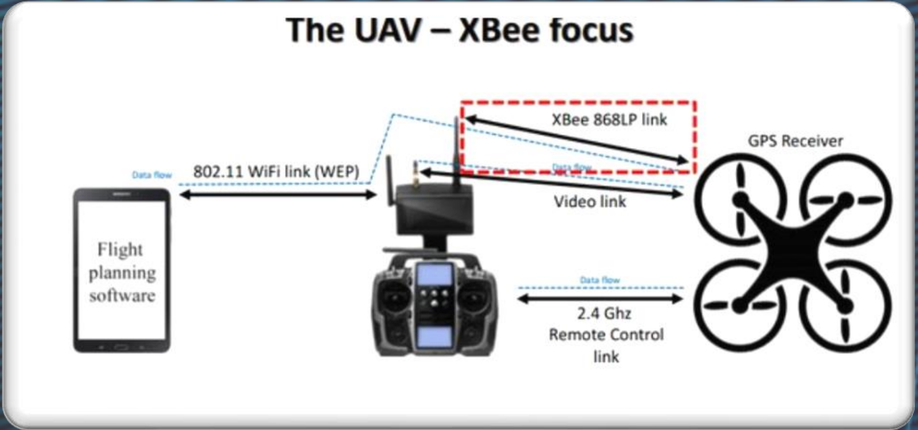
197.253.124.147
evaluation.nab.gov.gh
GGoC1
Added on 2019-09-13 13:56:41 GMT

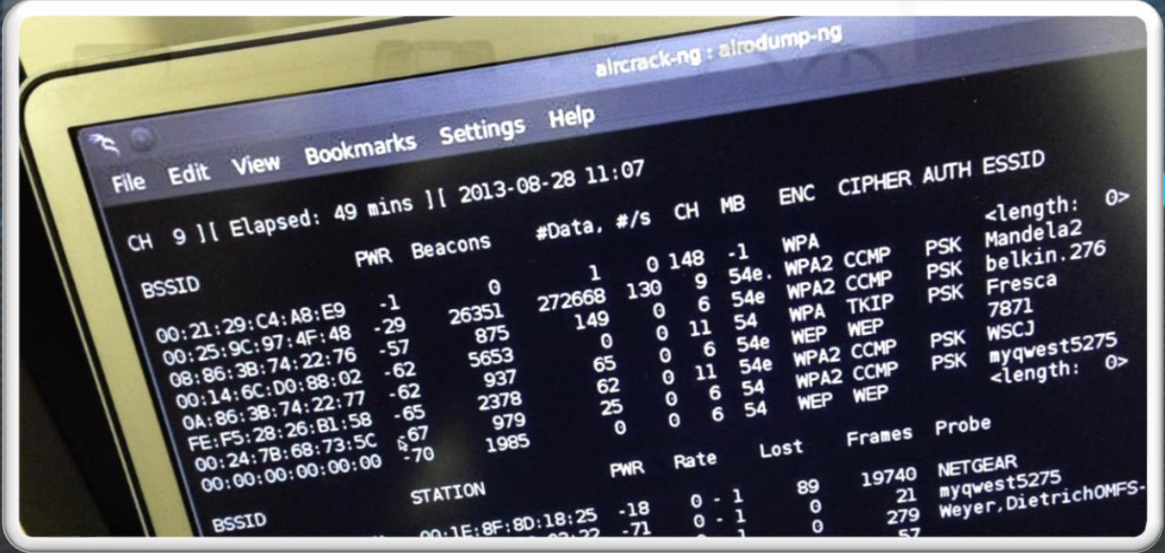
```
9.9.4-RedHat-9.9.4-74.el7_6.2
```

https://www.shodan.io

ThinkCyber

Wi-Fi attacks




aircrack-ng : airodump-ng
File Edit View Bookmarks Settings Help

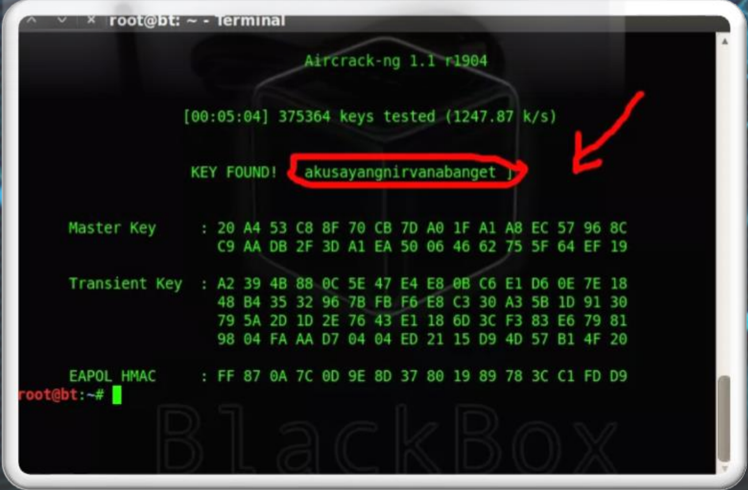
```
CH  9 ][ Elapsed: 49 mins ][ 2013-08-28 11:07

BSSID              PWR  Beacons    #Data, #/s  CH  MB   ENC  CIPHER AUTH ESSID

00:21:29:C4:A8:E9   -1        0        1    0 148  -1   WPA              <length:  0>
00:25:9C:97:4F:48  -29    26351   272668  130   9  54e. WPA2 CCMP   PSK  Mandela2
08:86:3B:74:22:76  -57      875      149    0   6  54e  WPA2 CCMP   PSK  belkin.276
00:14:6C:D0:88:02  -62     5653        0    0  11  54   WPA  TKIP   PSK  Fresca
0A:86:3B:74:22:77  -62      937       65    0   6  54e  WEP  WEP         7871
FE:F5:28:26:B1:58  -65     2378       62    0  11  54e  WPA2 CCMP   PSK  WSCJ
00:24:7B:68:73:5C  -67      979       25    0   6  54   WPA2 CCMP   PSK  myqwest5275
00:00:00:00:00:00  -70     1985        0    0   6  54   WEP  WEP         <length:  0>

BSSID              STATION            PWR   Rate    Lost    Frames  Probe

                   00:1E:8F:8D:18:25  -18    0 - 1    89     19740  NETGEAR
                                      -71    0 - 1     0        21  myqwest5275
                                             0 - 1     0       279  Weyer,DietrichOMFS-
                                                                57
```



```
                    Aircrack-ng 1.1 r1904


      [00:05:04] 375364 keys tested (1247.87 k/s)


           KEY FOUND! [ akusayangnirvanabanget ]


   Master Key     : 20 A4 53 C8 8F 70 CB 7D A0 1F A1 A8 EC 57 96 8C
                    C9 AA DB 2F 3D A1 EA 50 06 46 62 75 5F 64 EF 19

   Transient Key  : A2 39 4B 88 0C 5E 47 E4 E8 0B C6 E1 D6 0E 7E 18
                    48 B4 35 32 96 7B FB F6 E8 C3 30 A3 5B 1D 91 30
                    79 5A 2D 1D 2E 76 43 E1 18 6D 3C F3 83 E6 79 81
                    98 04 FA AA D7 04 04 ED 21 15 D9 4D 57 B1 4F 20

   EAPOL HMAC     : FF 87 0A 7C 0D 9E 8D 37 80 19 89 78 3C C1 FD D9
root@bt:~#
```

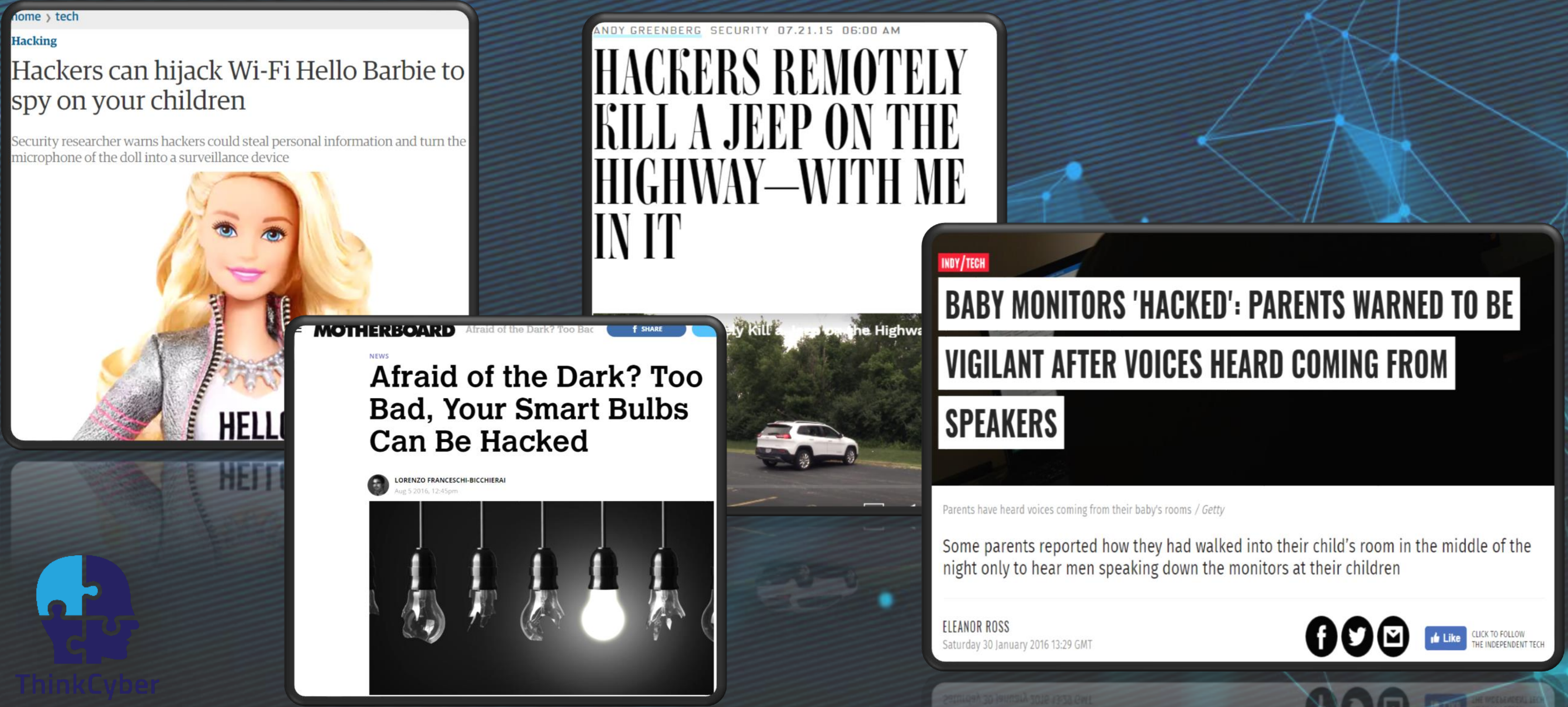
ThinkCyber

Cyber-Attack Tools

https://shop.hak5.org/

ThinkCyber

Present & Future



home › tech

Hacking

Hackers can hijack Wi-Fi Hello Barbie to spy on your children

Security researcher warns hackers could steal personal information and turn the microphone of the doll into a surveillance device

ANDY GREENBERG SECURITY 07.21.15 06:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT

MOTHERBOARD

NEWS

Afraid of the Dark? Too Bad, Your Smart Bulbs Can Be Hacked

LORENZO FRANCESCHI-BICCHIERAI
Aug 5 2016, 12:45pm

INDY/TECH

BABY MONITORS 'HACKED': PARENTS WARNED TO BE VIGILANT AFTER VOICES HEARD COMING FROM SPEAKERS

Parents have heard voices coming from their baby's rooms / *Getty*

Some parents reported how they had walked into their child's room in the middle of the night only to hear men speaking down the monitors at their children

ELEANOR ROSS
Saturday 30 January 2016 13:29 GMT

ThinkCyber

What can be done?

ThinkCyber

CYBERIUM ARENA

SIMULATOR

THE ULTIMATE CYBER SECURITY TRAINING TOOL

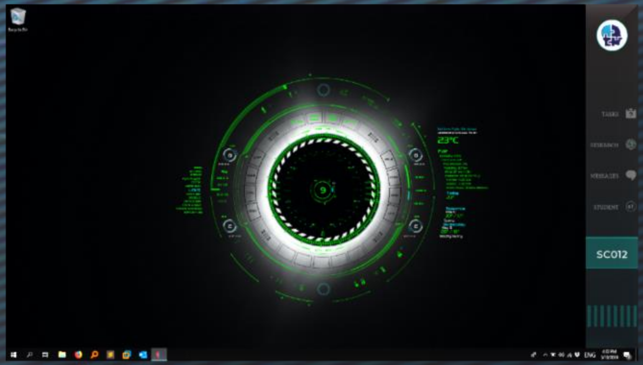
Example (video) >>

Israeli special cyber forces using the CYBERIUM scenarios to evaluate their soldiers.

https://youtu.be/5xwgzhzG1Go

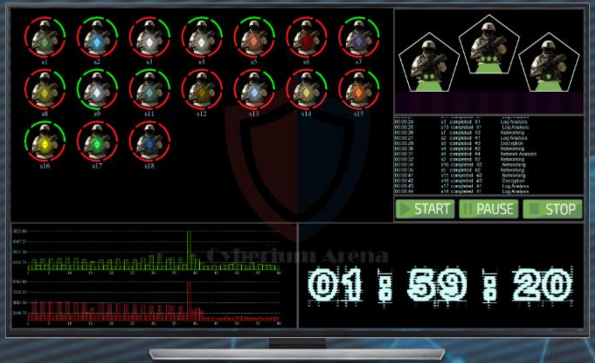
CYBERIUM ARENA

CYBERIUM



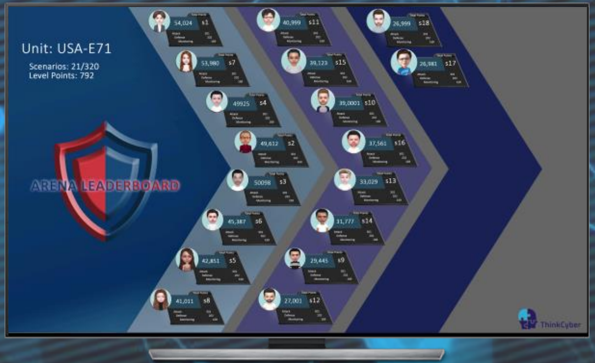
CYBERIUM CLIENT

Features a slick UI with a mission screen and helpful tools for solving the scenarios.



T1 (OPERATOR) screen

Shows the progress of the class in real time.



T2 (LEADERBOARD) screen

Calculates all the previous scores in real time.

CYBERIUM ARENA

Training Programs

The CYBERIUM ARENA is built to support any kind of cyber training.

As part of the support given with the system, the customer can also purchase study materials and arrange trainer-to-trainer programs on-site or at ThinkCyber training rooms in Israel.

ThinkCyber has created over 40 training programs, custom-made for different clients in order to support specific needs.

ThinkCyber's biggest advantage is the ability to provide the FULL PACKAGE in the cyber-security world: training, training materials and simulator.

CYBERIUM ARENA

SIMULATOR

Our Commitment

Excellence

Creativity

Teamwork

Questions?

More information can be found on our website
ThinkCyber.co.il

This presentation can be downloaded at:
https://thinkcyber.co.il/ghana

ThinkCyber