IBM Security

Between chair and keyboard

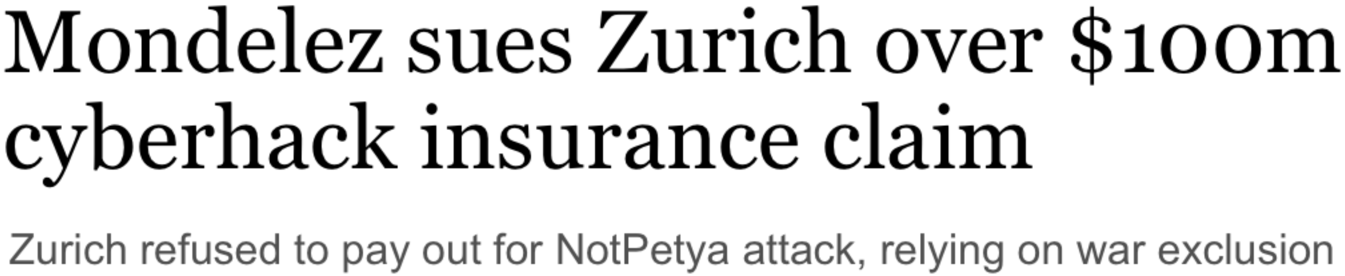
BIGGEST CHALLENGE OF SECURITY DEPARTMENTS?

Marcin Spychała
Senior Security Architect
marcin.spychala@pl.ibm.com

10.09.2019

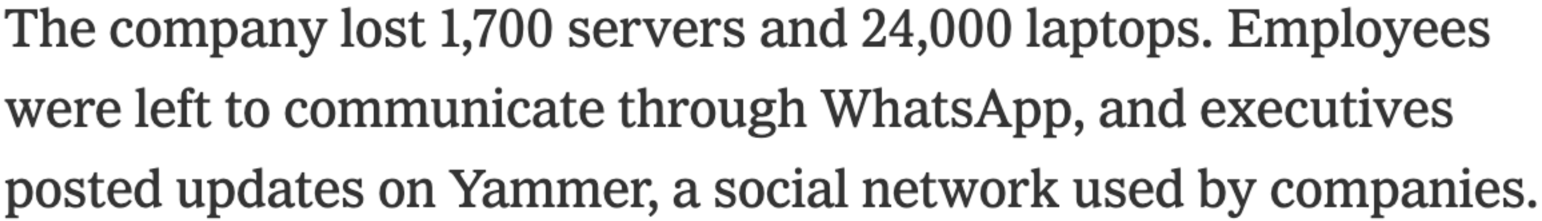
Two approaches – one example

Two challenges – one example



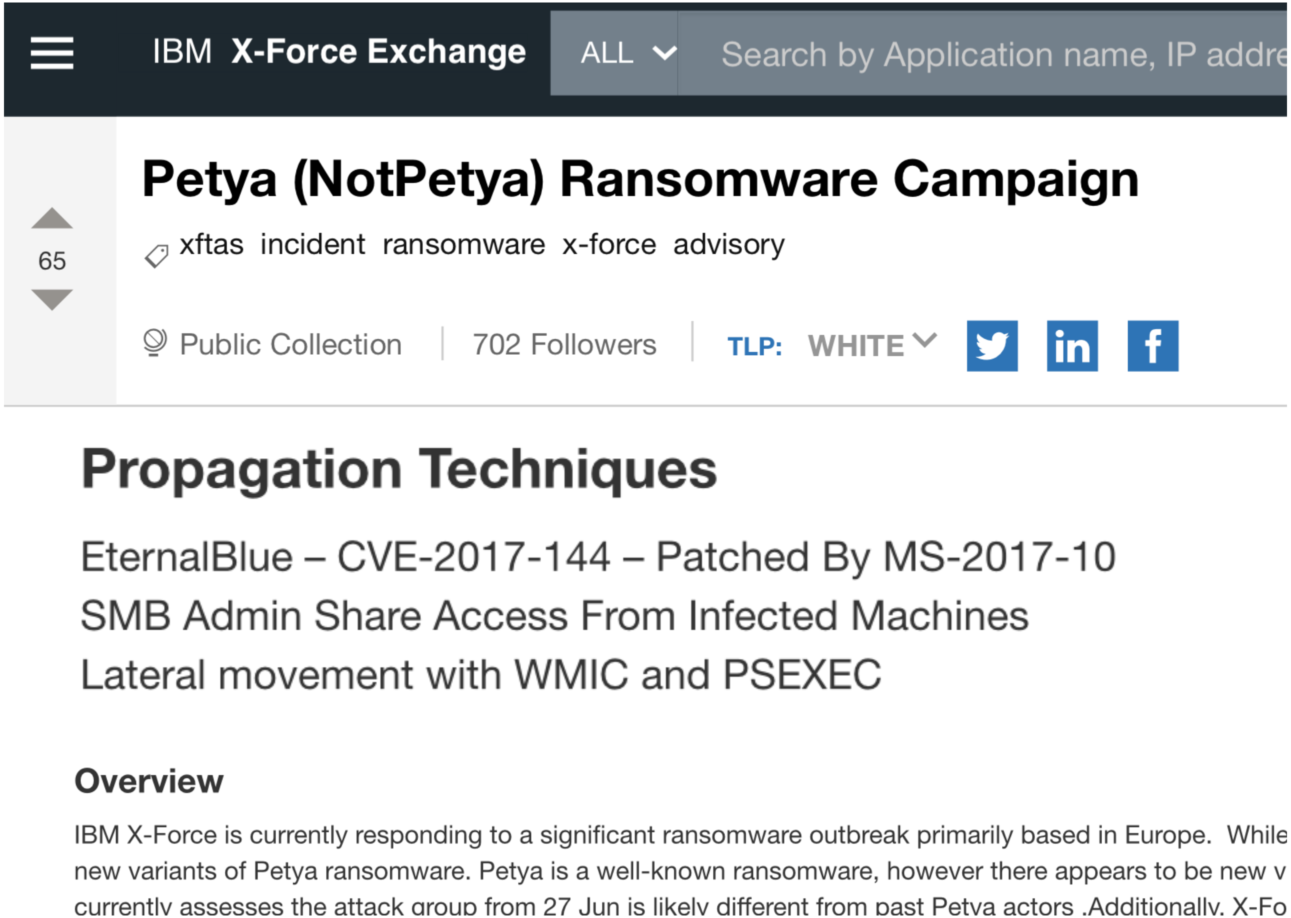
Mondelez sues Zurich over $100m cyberhack insurance claim

Zurich refused to pay out for NotPetya attack, relying on war exclusion



The company lost 1,700 servers and 24,000 laptops. Employees were left to communicate through WhatsApp, and executives posted updates on Yammer, a social network used by companies.

NotPetya – no problem



IBM X-Force Exchange
ALL
Search by Application name, IP addre

Petya (NotPetya) Ransomware Campaign

65
xftas incident ransomware x-force advisory
Public Collection
702 Followers
TLP: WHITE

Propagation Techniques

EternalBlue – CVE-2017-144 – Patched By MS-2017-10

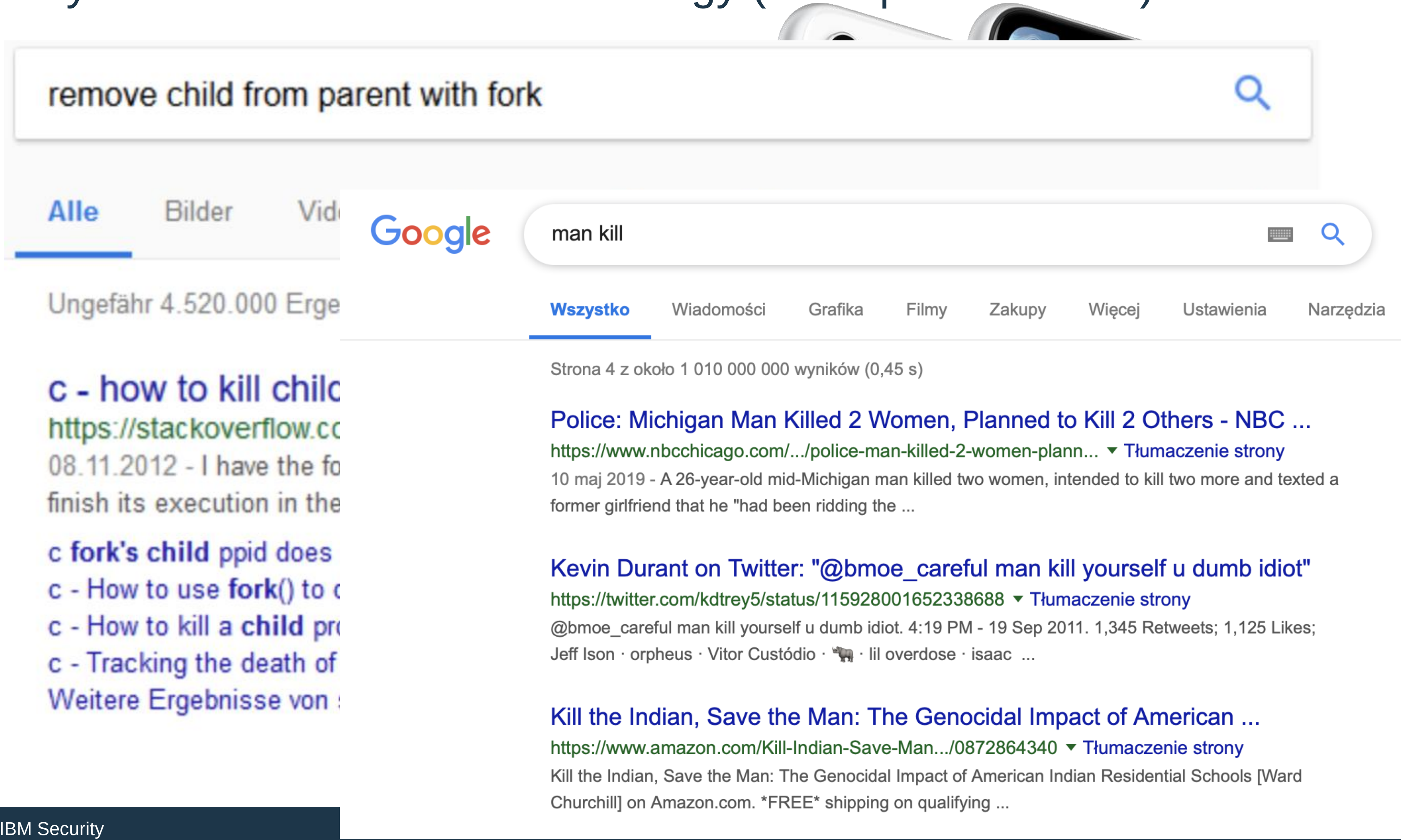
SMB Admin Share Access From Infected Machines

Lateral movement with WMIC and PSEXEC

Overview

IBM X-Force is currently responding to a significant ransomware outbreak primarily based in Europe. While new variants of Petya ransomware. Petya is a well-known ransomware, however there appears to be new v currently assesses the attack group from 27 Jun is likely different from past Petya actors .Additionally, X-Fo

Why we don’t understand technology (no hope I’m affraid)



remove child from parent with fork

Ungefähr 4.520.000 Erge

c - how to kill chilc
https://stackoverflow.cc
08.11.2012 - I have the fo
finish its execution in the

c **fork's child** ppid does
c - How to use **fork**() to c
c - How to kill a **child** pro
c - Tracking the death of
Weitere Ergebnisse von

man kill

Strona 4 z około 1 010 000 000 wyników (0,45 s)

Police: Michigan Man Killed 2 Women, Planned to Kill 2 Others - NBC ...
https://www.nbcchicago.com/.../police-man-killed-2-women-plann... ▾ Tłumaczenie strony
10 maj 2019 - A 26-year-old mid-Michigan man killed two women, intended to kill two more and texted a former girlfriend that he "had been ridding the ...

Kevin Durant on Twitter: "@bmoe_careful man kill yourself u dumb idiot"
https://twitter.com/kdtrey5/status/115928001652338688 ▾ Tłumaczenie strony
@bmoe_careful man kill yourself u dumb idiot. 4:19 PM - 19 Sep 2011. 1,345 Retweets; 1,125 Likes; Jeff Ison · orpheus · Vitor Custódio · 🦏 · lil overdose · isaac ...

Kill the Indian, Save the Man: The Genocidal Impact of American ...
https://www.amazon.com/Kill-Indian-Save-Man.../0872864340 ▾ Tłumaczenie strony
Kill the Indian, Save the Man: The Genocidal Impact of American Indian Residential Schools [Ward Churchill] on Amazon.com. *FREE* shipping on qualifying ...

Digging deeper…

Don’t click

(despite the fact that reading emails and clicking links is your work responsibility)

Don’t run/don’t open

(but printing out PDF with CV of candidate could be difficult – especially when we apply also recomendation 1.)

Don’t put anything it

(your laptop don’t work with projector on conference – well – go home then…)

By analogy…

Do not brake!

You may block wheels and cause an accident!

Do not change line!

You may collide with other car!

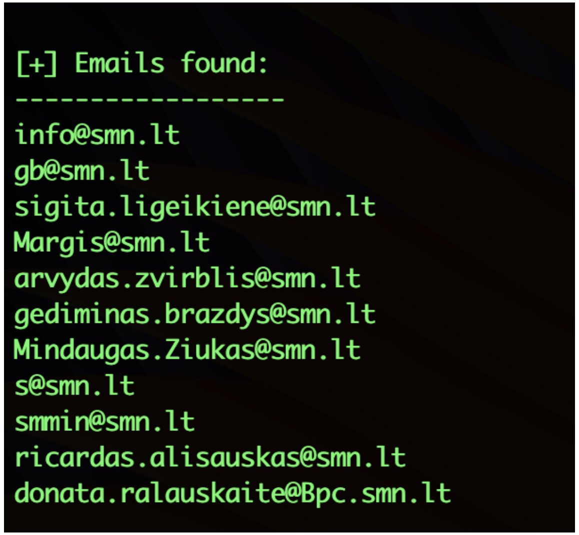
ABS
ACC
AFIL
AFL
ASR
BAS
BLIS
EBD
ESP
TPMS
TSR
Common sense*

Do not turn!

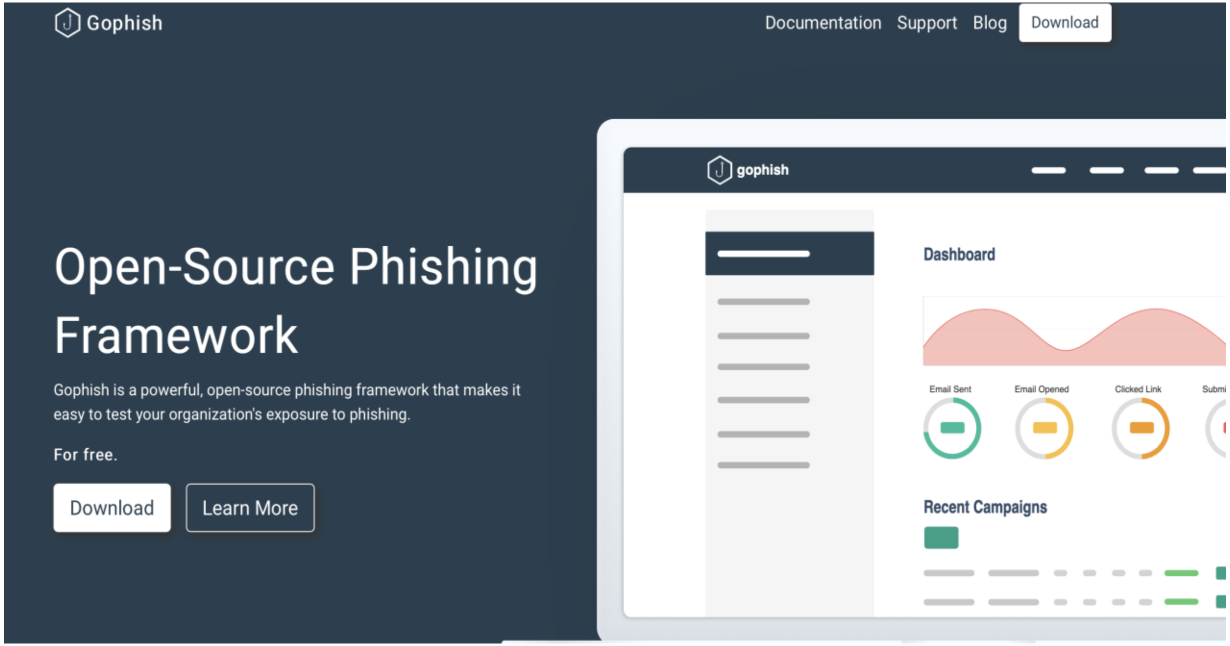
You may skid and cause an accident!

* Extra charge

Frequent question…



```
[+] Emails found:
------------------
info@smn.lt
gb@smn.lt
sigita.ligeikiene@smn.lt
Margis@smn.lt
arvydas.zvirblis@smn.lt
gediminas.brazdys@smn.lt
Mindaugas.Ziukas@smn.lt
s@smn.lt
smmin@smn.lt
ricardas.alisauskas@smn.lt
donata.ralauskaite@Bpc.smn.lt
```

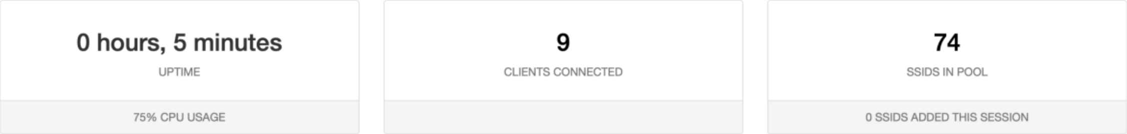


Open-Source Phishing Framework

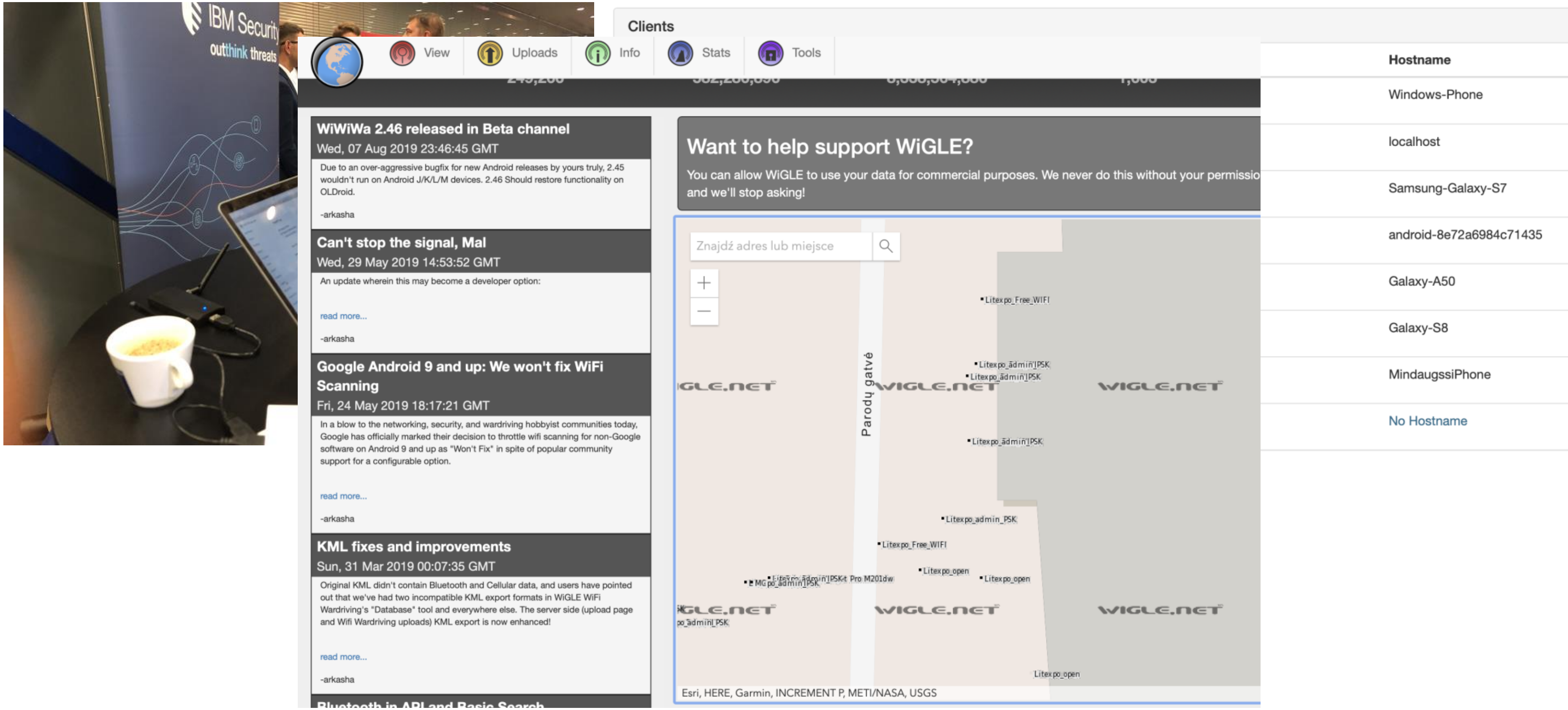
Gophish is a powerful, open-source phishing framework that makes it easy to test your organization's exposure to phishing.

For free.

For stalkers…



0 hours, 5 minutes	9	74
UPTIME	CLIENTS CONNECTED	SSIDS IN POOL
75% CPU USAGE		0 SSIDS ADDED THIS SESSION



Clients

Hostname
Windows-Phone
localhost
Samsung-Galaxy-S7
android-8e72a6984c71435
Galaxy-A50
Galaxy-S8
MindaugssiPhone
No Hostname

WiWiWa 2.46 released in Beta channel
Wed, 07 Aug 2019 23:46:45 GMT

Due to an over-aggressive bugfix for new Android releases by yours truly, 2.45 wouldn't run on Android J/K/L/M devices. 2.46 Should restore functionality on OLDroid.

-arkasha

Can't stop the signal, Mal
Wed, 29 May 2019 14:53:52 GMT

An update wherein this may become a developer option:

read more...

-arkasha

Google Android 9 and up: We won't fix WiFi Scanning
Fri, 24 May 2019 18:17:21 GMT

In a blow to the networking, security, and wardriving hobbyist communities today, Google has officially marked their decision to throttle wifi scanning for non-Google software on Android 9 and up as "Won't Fix" in spite of popular community support for a configurable option.

read more...

-arkasha

KML fixes and improvements
Sun, 31 Mar 2019 00:07:35 GMT

Original KML didn't contain Bluetooth and Cellular data, and users have pointed out that we've had two incompatible KML export formats in WiGLE WiFi Wardriving's "Database" tool and everywhere else. The server side (upload page and Wifi Wardriving uploads) KML export is now enhanced!

read more...

-arkasha

Bluetooth in API and Basic Search

Want to help support WiGLE?

You can allow WiGLE to use your data for commercial purposes. We never do this without your permissio and we'll stop asking!

Easy solution (theoreaticly)…*

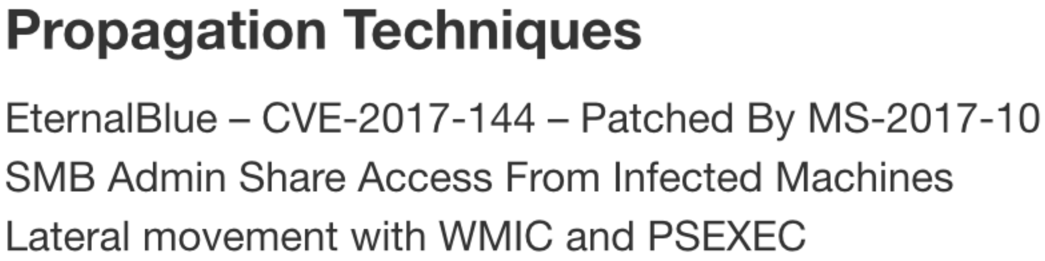
administrative rights for the application

Vs

administrative rights for the account / person

+

priviliged account management with automatic password change and SSH key rotation



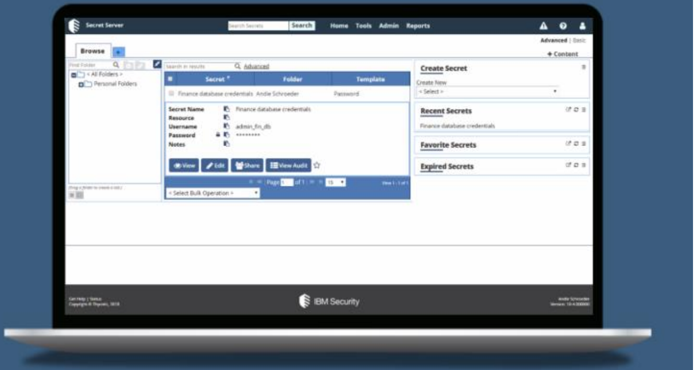
Propagation Techniques

EternalBlue – CVE-2017-144 – Patched By MS-2017-10

SMB Admin Share Access From Infected Machines

Lateral movement with WMIC and PSEXEC

* Assuming patching and vulnerability scanning



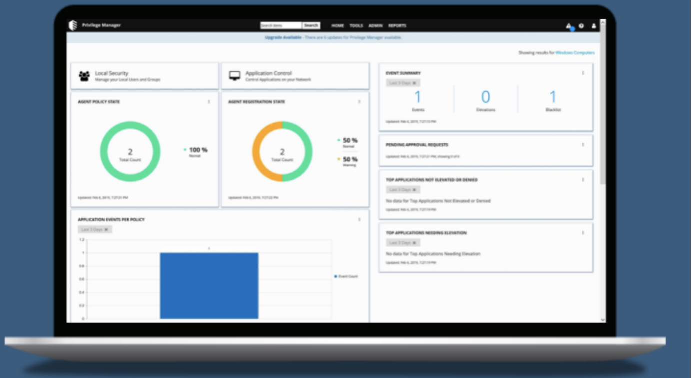
IBM Security Secret Server

Easy to use and fast to deploy enterprise-grade privileged access management for organizations of all sizes. Start your 30-day trial here.

Start your free trial

Read the eBook

Get your free Privileged Account Discovery for Windows Tool and personalized analysis → Download now



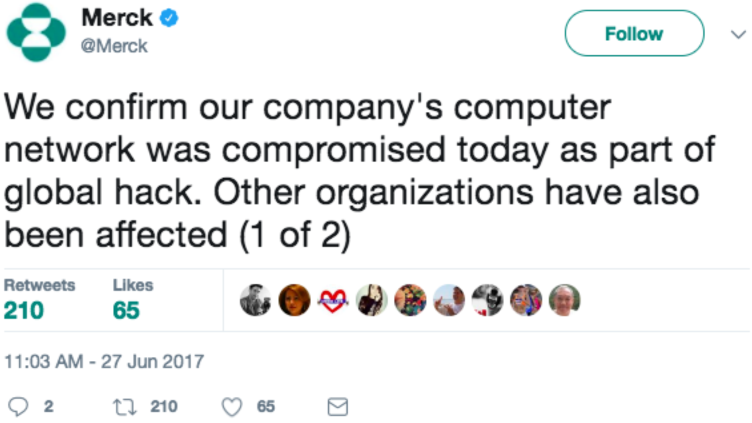
IBM Security Privilege Manager

Block malware-based attacks with least privilege and application control that’s easy for IT support teams and seamless for users.

Read the data sheet

Read the eBook

Security by obscurity no more



We confirm our company's computer network was compromised today as part of global hack. Other organizations have also been affected (1 of 2)

11:03 AM - 27 Jun 2017

IBM Security

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- ibm.com/security/community
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

IBM®