Every Contact Leaves a Trace.

BSides Dublin 2023

Ken Westin

kwestin@gmail.com
/in/kwestin
infosec.exchange/@kwestin
cybersecurity.io

Target: Ken Westin

Home Location: Newport, Oregon, USA

Employer: Panther, San Francisco

Cybereason, Elastic, Splunk, Tripwire, GadgetTrak

Current Location: BSides Dublin

Hobbies: Guitar, Records, BJJ, Shitposting

Career: 15 Years Cybersecurity

Contact Info

kwestin@gmail.com

infosec.exchange/@kwestin

Cybersecurity.io

linkedin.com/in/kwestin

CASE CLOSED


April 2012
Virginia


March 2012
Virginia


February 2012
Miami, FL


February 2012
Grants Pass, OR


January 2012
New York, NY

January 2012
Coos Bay, OR

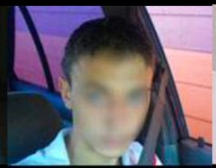

November 2009
Missouri
Tracked stolen laptop


September 2009
Oakland, California
Several laptops were


November 2011
Boulder, CO


October 2011
Olympia, WA


August 2011
Los Angeles, CA


August 2011
Portland, OR


July 2011
Curitiba, Brazil


June 2011
Portland, Oregon


August 2009
Brooklyn, New York


June 2009
Edmond, Oklahoma


May 2011
Richmond, California
Password Michael


February 2011
Portland, Oregon
Stolen MacBook Pro


January 2011
Moraga, California


February 2010
Portland, Oregon


January 2010
Springfield, Oregon


November 2009
Portland, Oregon

February 2009
Dallas, Texas


November 2008
Anchorage, Alaska

BBC NEWS

'I'm a professional cyberstalker'

10 August 2015 • Comments

Ken Westin uses advanced techniques to track down suspected thieves

By Dave Lee >
North America technology reporter

"Stupidity is the best vulnerability. That and greed."

Ken Westin openly, and enthusiastically, calls himself a professional cyberstalker. And foolish people are his target.

He uses some of the tools that are popular with the web's creepiest patrons, hacks used to spy on webcams.

But if you're wondering why he's so proud of it, it's because he's using that

MOTHERBOARD
TECH BY VICE

Meet the Real-Life Mr. Robot

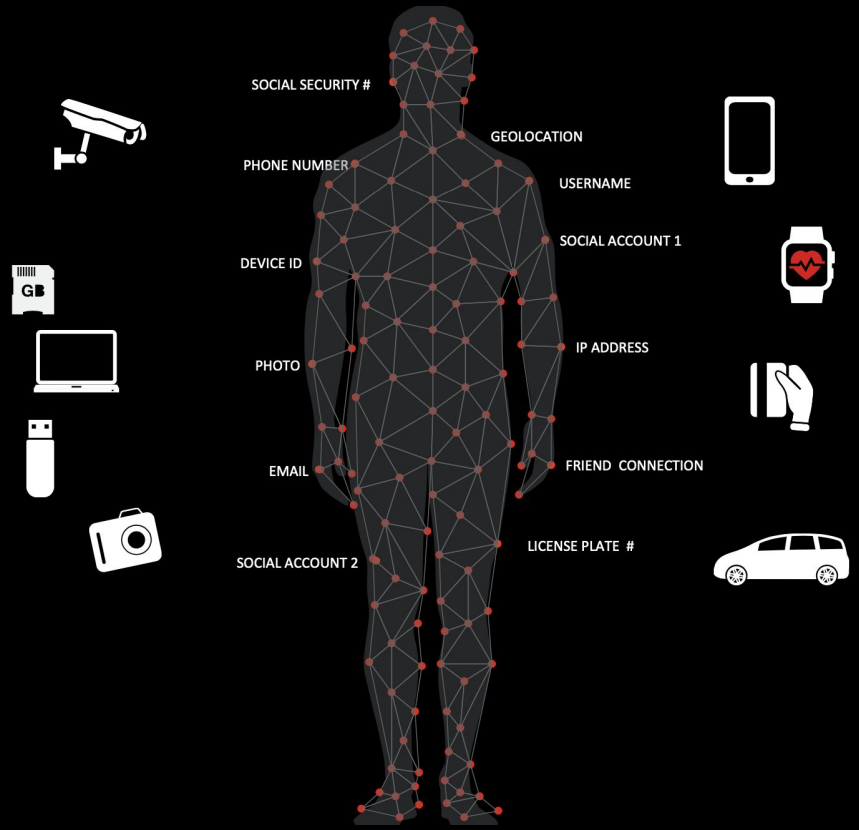
Confessions of a professional cyber stalker.

JP By J.M. Porup

October 20, 2015, 7:04am Share Tweet Snap

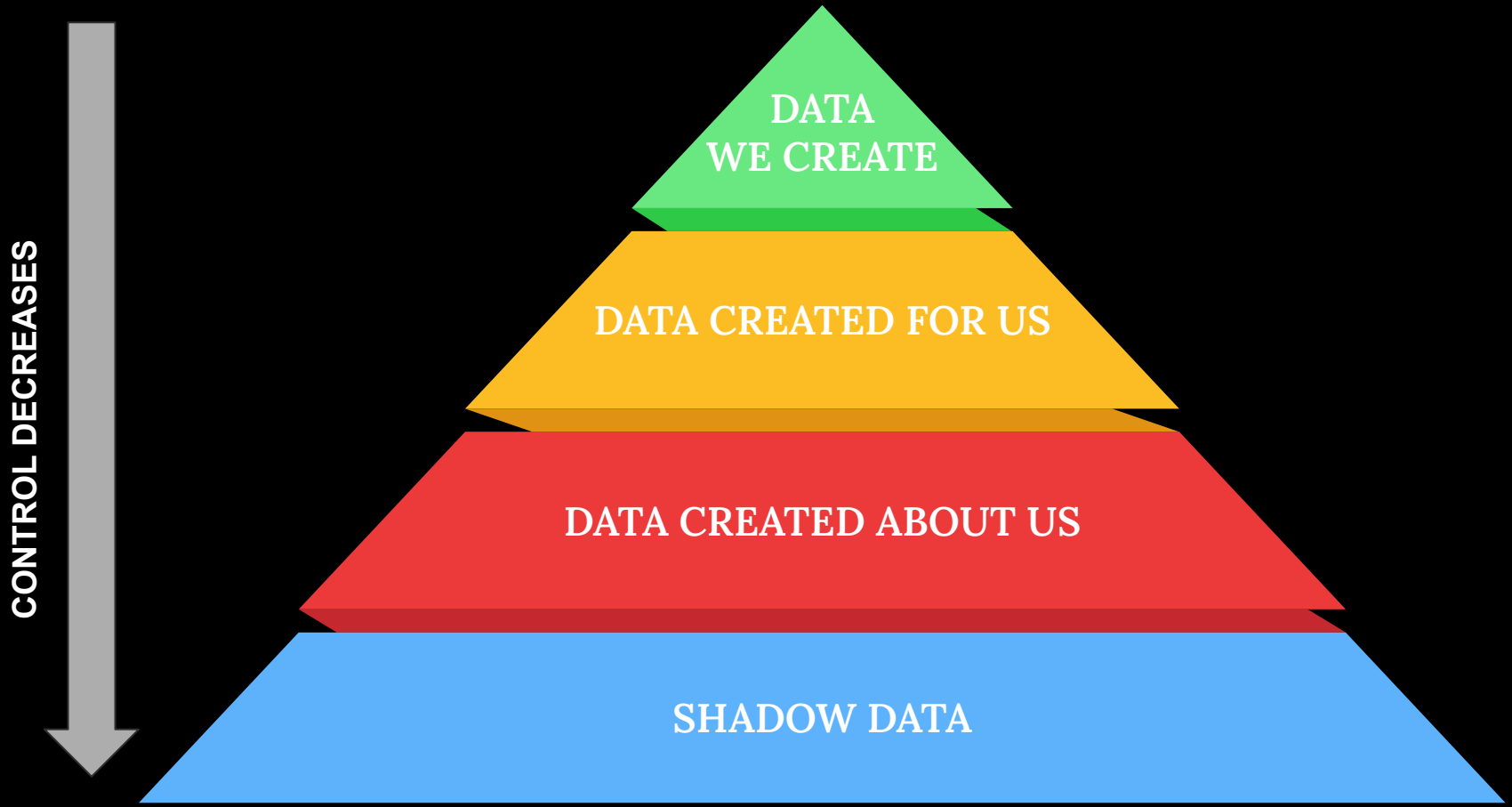

EVERY CONTACT LEAVES A TRACE.

The Quantified Self-Pwn




September
October
November
December
January
February
March
April
PANDA

Hierarchy of Data Bleed



USB Hacks

Exploit Tools

Cracking BIOS Passwords Part 1 September 7, 2008
Hacking Laptop Passwords September 6, 2008
HTTP R.A.T. October 17, 2006
Nmap for USB September 26, 2006
Slurp - (Podslurping) September 21, 2006
Sony USB Thumb Drives Install Rootkit September 24, 2007
Torpark September 28, 2006
USB Drive Phone Home October 21, 2006
USB Dumper October 6, 2006
USB Hacksaw October 7, 2006
USB Switchblade
Wireshark for USB September 25, 2006

Happy Little Spyware

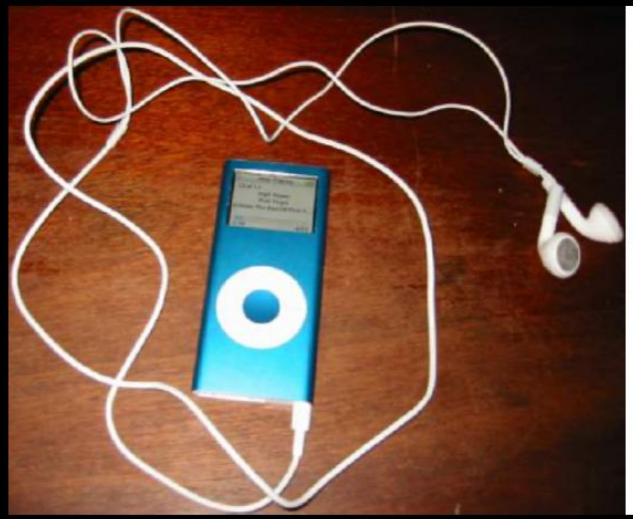
From: [redacted]
Sent: Thursday, February 22, 2007 2:25 PM
To: [redacted]
Subject: Gadget Theft: Device Located

The Flash Drive USB Flash Drive you reported lost or stolen has been plugged into a PC and we have been able to retrieve forensic data from the system

Public IP Address: 206.72.102.240
Host: 206.72.102.240

MP3 Players

Apple	Archos	Cowon



Time of Connection: Jun 15, 2007 2:08 PM (PST)
Public IP Address: 74.120.165.168
Host: CPE001217e41136-CM00194757b6a4.cpe.net.cable.rogers.com
ISP: Rogers Cable
Internal Network Address: 192.168.1.100
Computer Name: YOUR-39673CA035
User Name: kalpakis family

Location
==========
Country: CA
Region: ON
City:Newmarket

Zumo 550, Street pilot C550, c580 | Go 910, one, Go 510 | Iway 500C

Cell Phones

Sony Ericsson	Nokia	Helio
K 550,K750i,K800i,W200a,W600i,W810, W880, W950, M600, P990	5300, 6070, 7610, N73, N7-, N80	Ocean, Fin, Drift

Other Devices
Sony Playstation Portable (PSP)
PalmOne Lifedrive
LaCie External USB hard drives

Expanding Investigative Scope

2009-02-21 23:43:49

Commercial Trojan

FLIR®

ThermaTrak

FLIR ThermaTrak™

If your IR camera is lost or stolen,
ThermaTrak™ can track where it is and who has it.

- *Custom tracking system for lost, stolen or missing IR Cameras*
- *ThermaTrak™ is embedded by FLIR's Service Department in the camera's firmware*
- *Proven software solution for mobile equipment*
- *Available as an annual subscription or **Included FREE with an Extended Warranty***
- *Notification by email when stolen IR camera "found"*
- *Ideal for asset management of multiple IR cameras*
- *Aid to law enforcement in finding camera and prosecuting theft*
- *Exclusive, patented technology from FLIR and powered by GadgetTrak*

The First Theft Tracking System for IR Cameras!

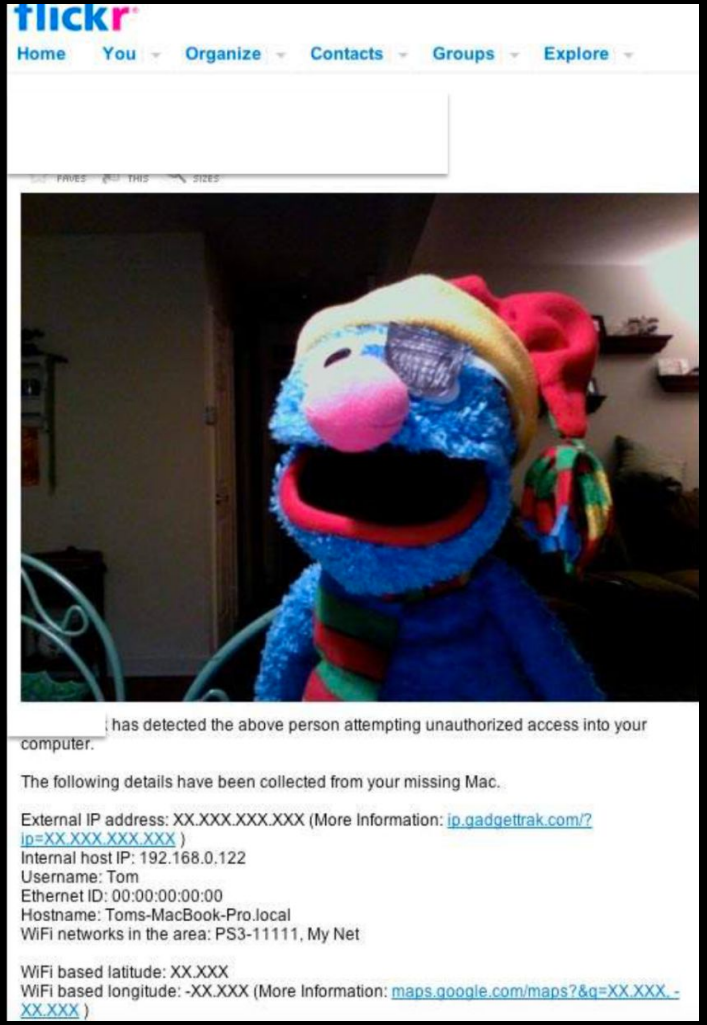
Remote activation triggers theft detection — Owners who fall victim to

ThermaTrak in action — The software must be installed on your camera and

One-time activation required at Service Center — In order to activate

Further Down the Rabbit Hole: Tracking Laptops

Building a Better Laptop Trap



First Laptop Recovery Using Wi-Fi Positioning+ Camera

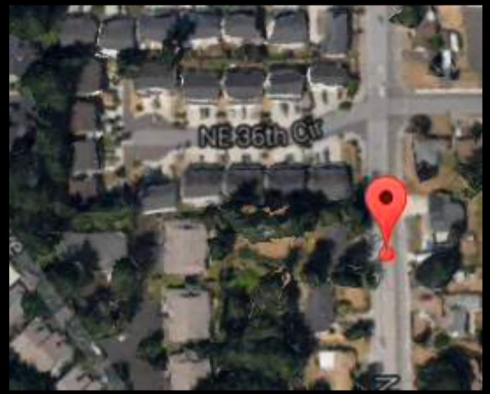
External IP address: (More Information:
ip.gadgettrak.com/?ip=)
Internal host IP: 192.168.1.116
Username:
Ethernet ID: 00:23:df:93:da:98
Hostname:
WiFi networks in the area:

WiFi based latitude:
WiFi based longitude: (More Information:
maps.google.com/maps?&q=

Thieves Targeting Portland Schools Unveil Organized Crime Group

External IP address: [redacted] (More Information: [redacted]
Internal host IP: 192.168.1.133
Username: student
Ethernet ID: [redacted]
Hostname: [redacted].local
WiFi networks in the area: BoB, junkers_network, Kernazh, Mike[redacted]

WiFi based latitude: [redacted]
WiFi based longitude: -122.585643 (More Information: http://m[redacted]



https://www.youtube.com/watch?v=Fyej2D1ofNI

More Organized Crime & Expanding to OSINT

External IP address: 209.142. (More Information: http://ip
Internal host IP: 192.168.5.156
Username: Viktor
Ethernet ID: 00:25:4b
Hostname: Macintosh.local
WiFi networks in the area: attwifi, qualityfloors, Regency2, Waypo

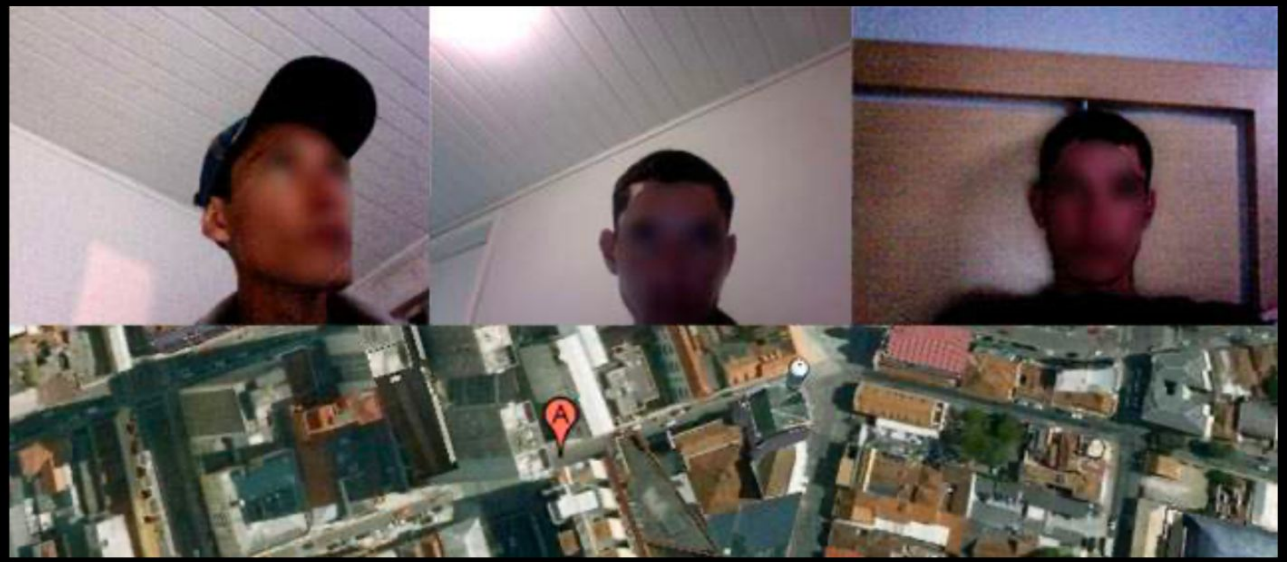
WiFi based latitude: 0.000000
WiFi based longitude: 0.000000 (More Information: http://maps.google.com/maps?&q=0.000000,0.000000)

scion

myspace

ebay

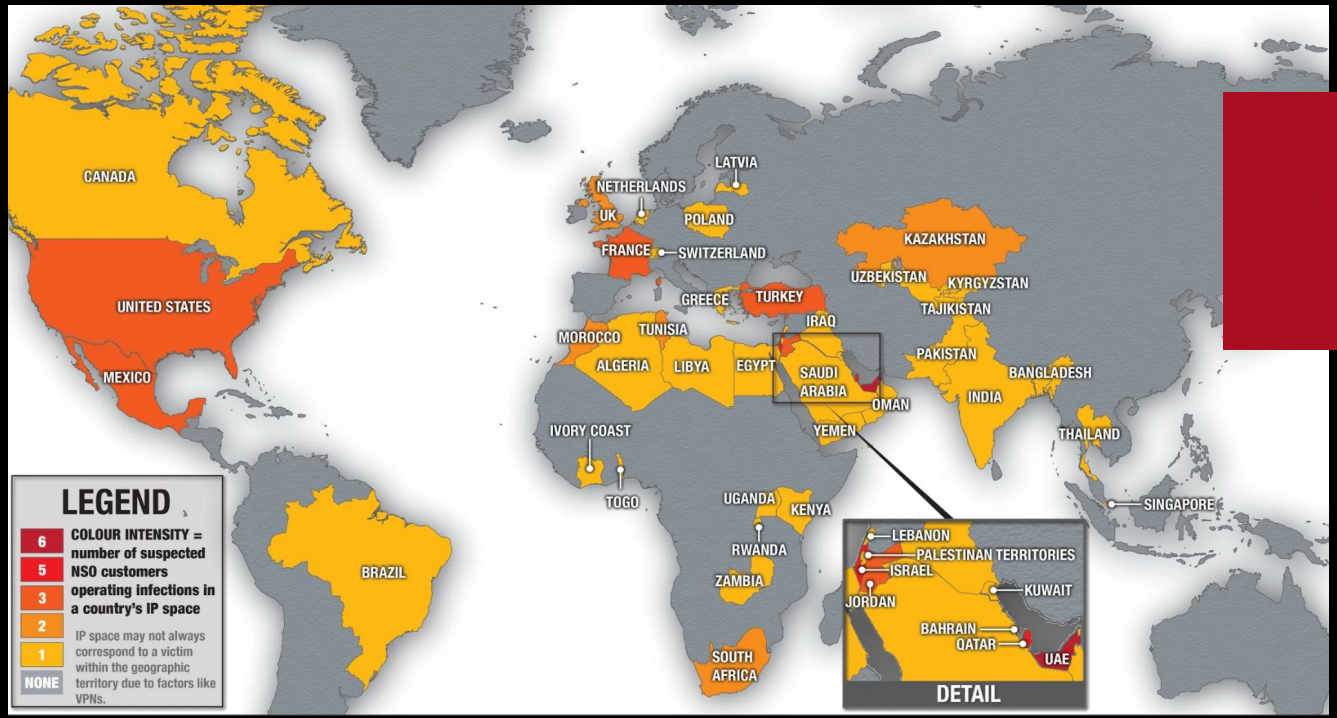
International Tracking: Brazil Carjacking & Assault



Smartphone Tracking

Fun with Smartphone Thieves

Commercial Mobile Spyware



NSO GROUP

Further Down the Rabbit Hole: EXIF Data

EXIF Data Results

Serial Number: Not found
Photo Date: 2011:08:07 15:19:49
Make: SAMSUNG
Model:

SourceFile	upload/_4fb9c5417c5fe9.38421395.jpg
FileSize	524288
FileModifyDate	2012:05:20 21:32:01-07:00
FileType	JPEG
MIMEType	image/jpeg
ExifByteOrder	II
ImageDescription	SAMSUNG
Make	SAMSUNG
Model	GT-I9000
Orientation	6
XResolution	72
YResolution	72
ResolutionUnit	2
Software	fw 31.50 prm 31.86
ModifyDate	2011:08:07 15:19:49
YCbCrPositioning	1
ExposureTime	0.03125
FNumber	2.638671875
ExposureProgram	2

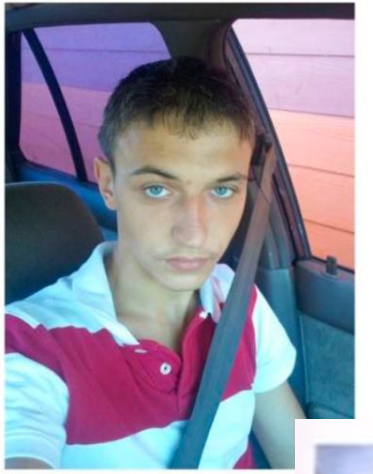
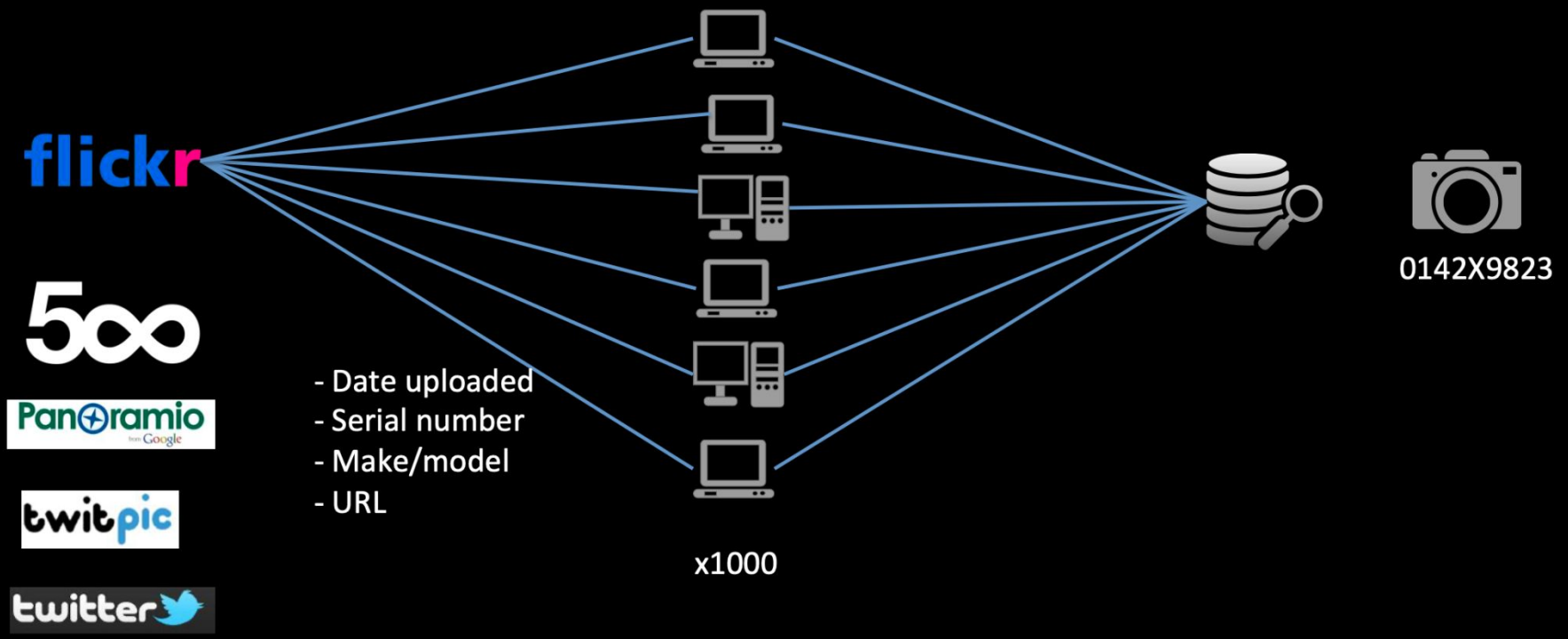


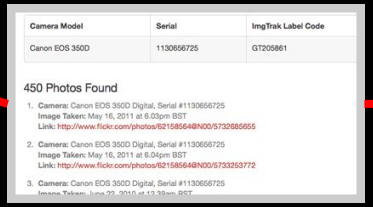
Photo Location
45.671666666667, -122.50916666667

EXIF Mining with a Legal Botnet



Holy Sh*t It Worked!

$9K Camera Gear Recovered 1 Year After Being Stolen

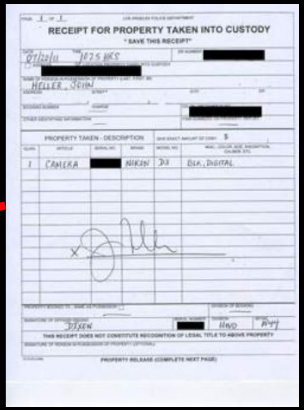


flickr

facebook

craigslist

ebay

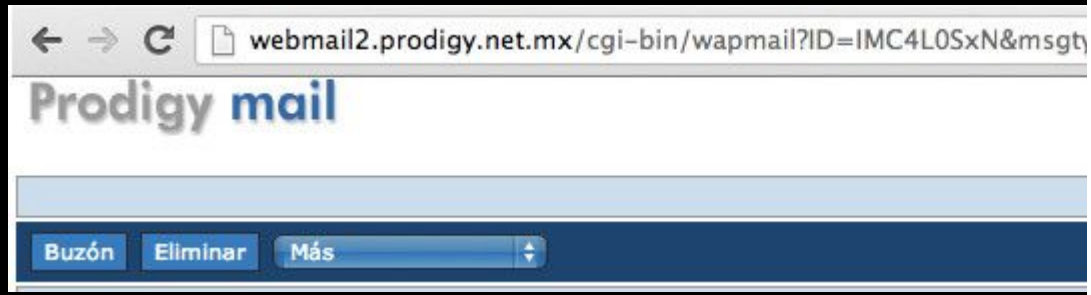


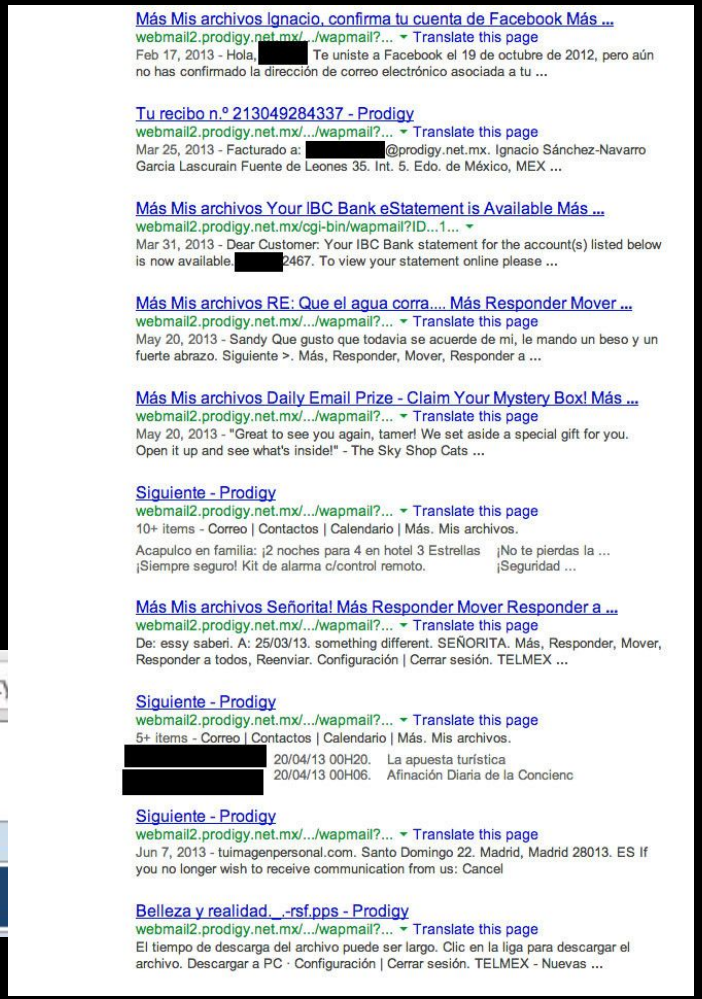
EXIF + OSINT

ICE HSI Cyber Crimes Center (C3)
Child Exploitation Investigations Unit

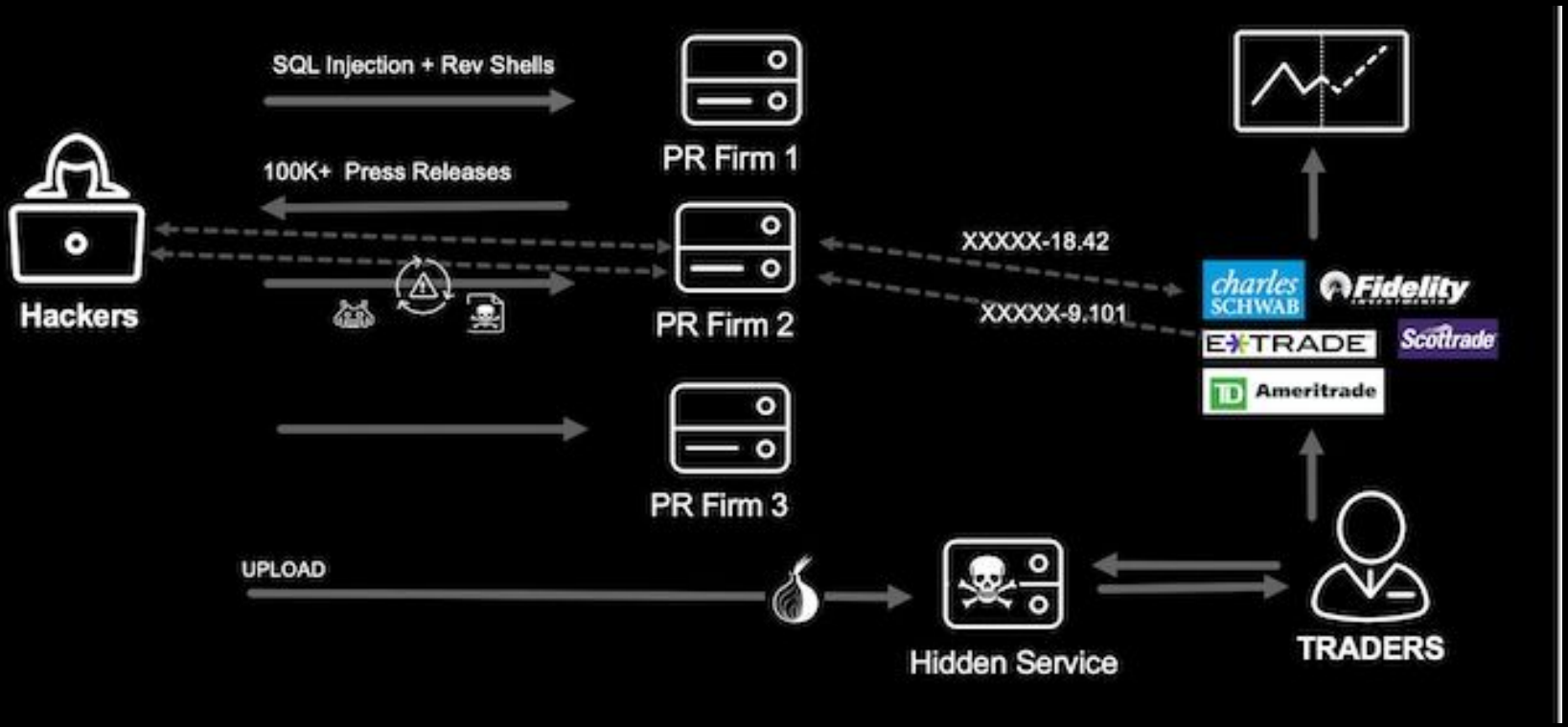
IoT Provides New Telemetry — and Targets

ISP Emails Indexed by Google



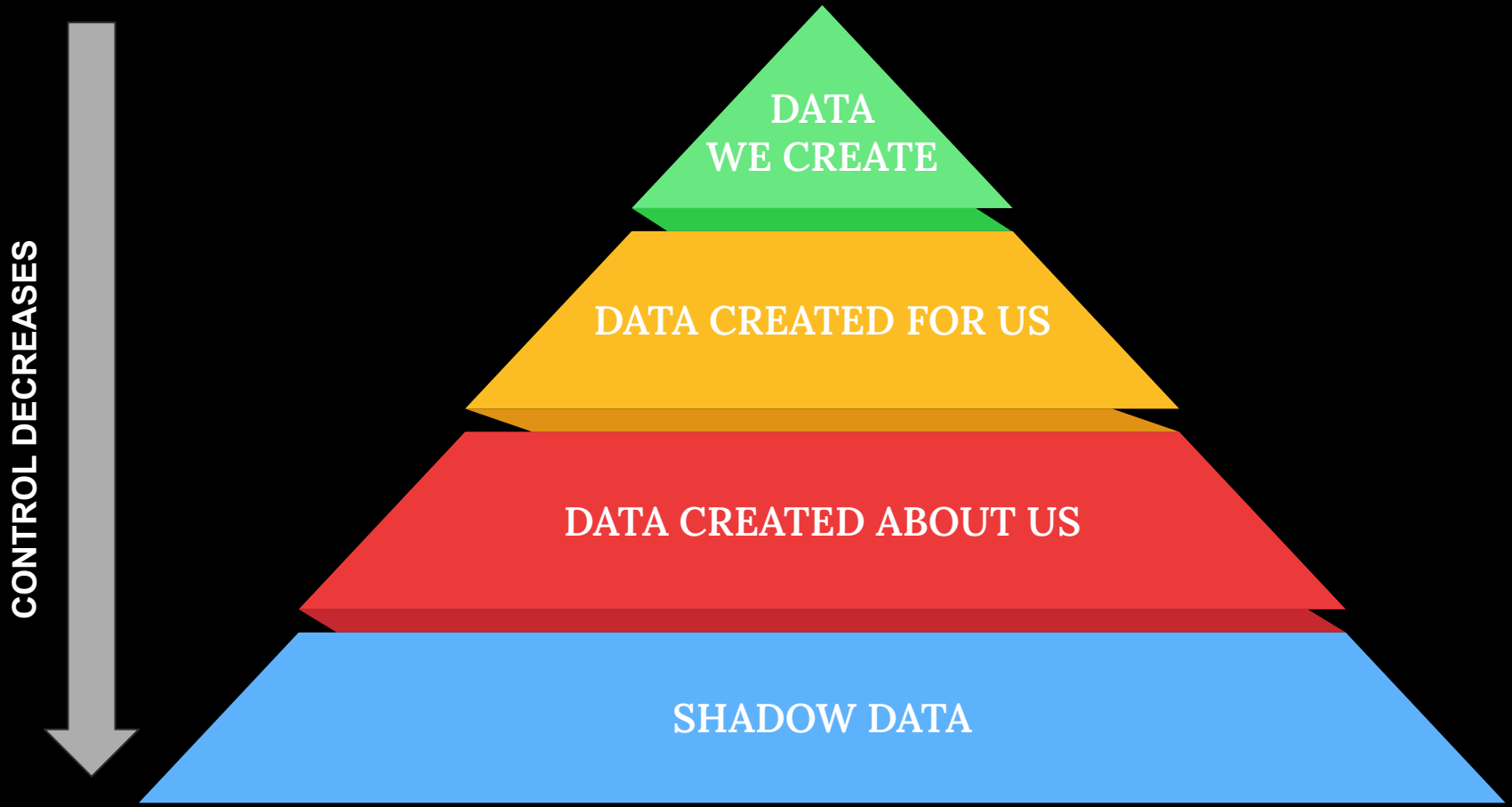


Black Hats & White Collars



https://www.splunk.com/en_us/blog/security/black-hats-white-collars-sec-edgar-database-hackers-revealed.html

Hierarchy of Data Bleed



Thank You!

kwestin@gmail.com
linkedin.com/in/kwestin
infosec.exchange/@kwestin
cybersecurity.io