



**Hacker Kitty...**



**Don't mess with him**

# Strategies on Securing you banks & enterprises. (From someone who robs banks & enterprises)



Police are searching for a man who reportedly took more than \$75,000 from a Walmart in Bristol while disguised as a Loomis armored truck driver Saturday morning.

# Who am I?



WeChat: JaysonStreet

# INTRO



Humans are terrible at risk management!

## Ebola virus cases in the United States

### Map of Ebola cases and infrastructure throughout the U.S.

Cases first diagnosed in U.S.	4 <sup>[note 1]</sup>
Cases evacuated to U.S. from other countries	7
Total cases	11 <sup>[note 2]</sup>
Deaths	2

4 more rows

[Ebola virus cases in the United States - Wikipedia](https://en.wikipedia.org/wiki/Ebola_virus_cases_in_the_United_States)

[https://en.wikipedia.org/wiki/Ebola\\_virus\\_cases\\_in\\_the\\_United\\_States](https://en.wikipedia.org/wiki/Ebola_virus_cases_in_the_United_States)

## Number of deaths for leading causes of death:

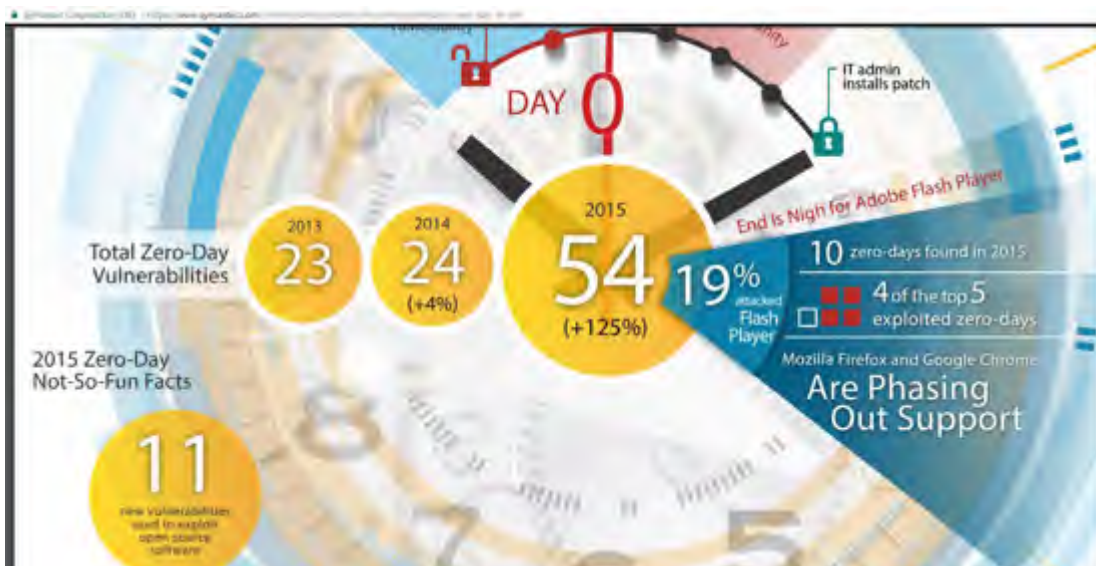
- Heart disease: 614,348
- Cancer: 591,699
- Chronic lower respiratory diseases: 147,101
- Accidents (unintentional injuries): 136,053
- Stroke (cerebrovascular diseases): 133,103
- Alzheimer's disease: 93,541
- Diabetes: 76,488
- **Influenza and Pneumonia: 55,227**
- Nephritis, nephrotic syndrome and nephrosis: 48,146
- Intentional self-harm (suicide): 42,773

Source: [Health, United States, 2015, Table 19](#) (Data are for 2014)

# INTRO



Humans are terrible at risk management!



## SQL injection has surfaced as the no. 1 attack in 2015

A new survey from Ponemon Institute finds that nearly 80 percent of enterprises say that their organization's portfolio of applications has become more vulnerable to attacks.



This vulnerability comes as more enterprises are relying on increasing numbers of applications to conduct their business; The survey found that 57 percent of enterprises have between 1000 and 5000 business applications in use throughout their organizations.

84 percent of respondents say the most common gateway attack experienced by their organization over the past 12 months is an SQL injection, followed by cross site scripting (23 percent of respondents) and cross site request forgery (at 18 percent).

# INTRO



Who do you really think poses the most danger to your enterprise?

Nation States? .... Not really unless you're building a nuclear centrifuge, building communication gear sold world wide, the Pope, etc... ;-)

**Stuxnet was work of U.S. and Israeli experts, officials say**

By Eliot Rubin and Amy Wittek

A damaging cyberattack against Iran's nuclear program was the work of U.S. and Israeli experts and proceeded under the secret orders of President Obama, who was eager to slow that nation's apparent progress toward building an atomic bomb without launching a traditional military attack, say current and former U.S. officials.

The origins of the cyberweapon, which outside analysts dubbed Stuxnet after it was inadvertently discovered in 2010, have long been debated, with most experts concluding that the United States and Israel probably collaborated on the effort. The current and former U.S. officials confirmed that long-standing suspicions Friday, after a New York Times report on the program.

The officials, speaking on the condition of anonymity to describe the classified effort code-named Olym Games, said it was first developed during the George W. Bush administration and was geared toward *damaging Iran's nuclear capabilities gradually while sowing confusion among Iranian scientists about the cause of mishaps at a nuclear plant.*

**TelecomsTech**

**The NSA hacked equipment from Cisco, Huawei, and Juniper**

By Ryan Davis  
25 August 2014, 3:04 pm  
comment

Categories  
SECURITY | Hacking | NSA | Privacy | Security

**Newsweek**

**NSA Accused of Peeping On The Pope**

An Italian magazine claims the NSA spied on the Vatican and Pope Francis with the complicity of Italy's authorities—but the Holy See denies the claim.

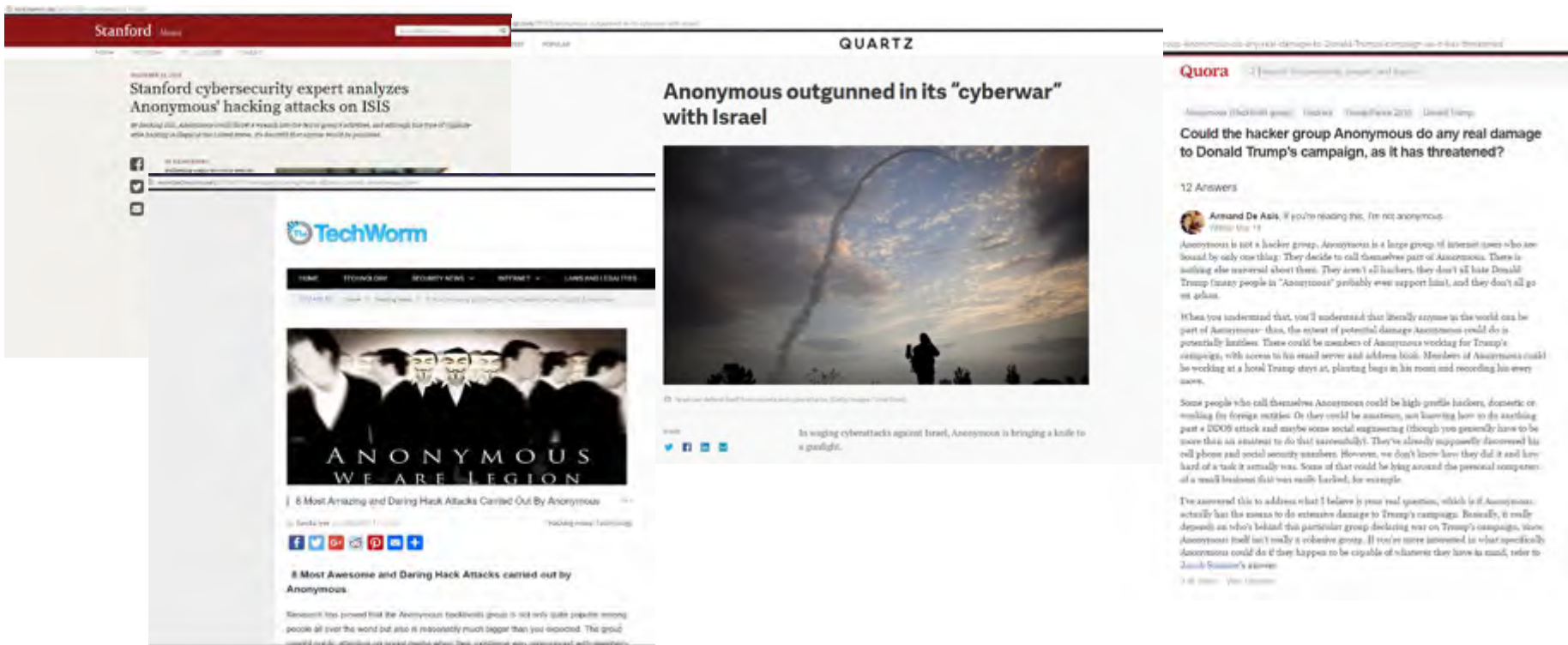
Nothing is sacred when it comes to espionage—not even the pope's privacy. At least that's what Italy's investigative Prosecco says in an investigation "exclusive" in which they lay out the widespread habit of wiretapping on Italians by the National Security Agency (NSA), including listening in on the Holy See.

# INTRO



Who do you really think poses the most danger to your enterprise?

L337 H4x0rs like Anonymous? .... Really, burning their 0-Day & tools (like LOIC) to take you down for the sake of justice and all that is righteous in the world!?!)



The collage consists of four overlapping screenshots:

- Stanford University:** Article titled "Stanford cybersecurity expert analyzes Anonymous' hacking attacks on ISIS".
- Quartz:** Article titled "Anonymous outgunned in its 'cyberwar' with Israel" featuring a dramatic image of a lightning bolt striking a silhouette against a cloudy sky.
- TechWorm:** Article titled "8 Most Amazing and Daring Hack Attacks Carried Out By Anonymous" featuring a group photo of individuals wearing Guy Fawkes masks.
- Quora:** A question "Could the hacker group Anonymous do any real damage to Donald Trump's campaign, as it has threatened?" with 12 answers.

# INTRO



Who do you really think poses the most danger to your enterprise?

Criminals? ..... Who though may not know everything about the tools they're using but know enough to make a lot of money by going after quantity not quality!

INVESTMENT BANKING | LEGAL/REGULATORY

## JPMorgan Chase Hacking Affects 76 Million Households

By JESSICA SILVER-GREENBERG, MATTHEW GOLDSTEIN and NICOLE PERLNOTH | OCTOBER 2, 2014 | 12:52 PM



The Manhattan headquarters of JPMorgan Chase, which securities filings revealed was attacked by hackers over the summer. (Reuters/Burton G. Meyer)

**Updated, 9:03 p.m.** | A cyberattack this summer on JPMorgan Chase compromised the accounts of 76 million households and seven million small businesses, a tally that dwarfs previous estimates by the bank and puts the intrusion among the largest ever.

The details of the breach — disclosed in a securities filing on Thursday — emerge at a time when consumer confidence in the

Front Page News Topics Magazines Research Directors Menu

## \$45 Million Global Cyber Bank Theft: Who Pays the Losses?

By Jessica Dye, Jim Finkle and Joseph Ax | May 15



Article 3 Comments

**REUTERS** In one of the biggest store \$45 million from credit card processors in 27 countries, U.S. |

The U.S. Justice Department accused eight men of the organization, and said seven of them, leader of the cell, was reported to have been in 27.

/alert/surveyetailers-risk-heavy-losses-just-one-cybersecurity-breach/

## Survey: Retailers Risk Heavy Losses From Just One Cybersecurity Breach

bbc News Spain Health Asia Earth Travel

NEWS

### Tesco Bank customers lose money to 'fraudsters'

Video - Business



Thousands of Tesco Bank current account customers appear to have been targeted by fraudsters, with some saying they have lost hundreds of pounds.

Customers have complained about money being withdrawn without permission, cards being blocked and being asked to pay through to the bank on the phone. U.S. |

a high price for any cybersecurity breach, with almost one in five consumers gain shop at a compromised chain even if the company later took steps to according to a report released Tuesday by auditing firm KPMG. 19 percent of respondents said they would never return to shop at a retail their personal information, while 49 percent said they would wait between three ring. KPMG said factors for determining whether consumers would return to an included offering a solid plan to prevent future attacks, a timely reach, and an agreement to cover losses. Retailers lagging behind financial and tech companies in both human and financial corporate executives, 58 percent of retailers said they employ a leader whose ity, compared with 85 percent at both financial and tech firms. Similarly, 45 ty have invested capital funds in information security, compared with 66 percent percent of tech companies.

state security focuses on financial and technology companies, hackers frequently's collected by retailers. On Aug. 18, clothing store chain Eddie Bauer said its infected with malware, enabling hackers to access customer payment card



# INTRO



## Literally don't become a Target of Cyber-Crime

More than 90 lawsuits have been filed against Target by customers and banks for negligence and compensatory damages. That's on top of other costs, which analysts estimate could run into the billions. Target spent \$61 million through Feb. 1 responding to the breach, according to its fourth-quarter report to investors. It set up a customer

The screenshot shows a CNN Money article. The header includes the CNN Money logo and navigation links for Business, Markets, Tech, Media, Personal Finance, Small Biz, and Luxury. The article title is "Target settles for \$39 million over data breach". The author is Ahiza Garcia (@ahiza\_garcia) and the date is December 2, 2015, 3:48 PM ET. The main content area is mostly blank with a small gear icon and the text "Click to play Adobe Flash Player". On the right side, there are social media sharing icons and a "Social Stream" section with three article teasers: "Meet the man who spent \$9 million on a license plate", "Getaway washing machines recalled because of explosion risk", and "The Simpsons renewed for an unprecedented 30th season". At the bottom, there is a red banner with the text "5 Stunning stats about Target" and a paragraph stating: "Target agreed to a \$39 million settlement with several U.S. banks on Wednesday over a data breach that affected roughly 40 million customers."

# INTRO



## Literally don't become a Target of Cyber-Crime

### 12 Email Attack on Vendor Set Up Breach at Target

The breach at Target Corp. that exposed credit card and personal data on more than 110 million consumers appears to have begun with a malware-laced email phishing attack sent to employees at an HVAC firm that did business with the nationwide retailer, according to sources close to the investigation.

Last week, KrebsOnSecurity reported that investigators believe the source of the Target intrusion traces back to network credentials that Target had issued to Fazio Mechanical, a heating, air conditioning and refrigeration firm in Sharpsburg, Pa. Multiple sources close to the investigation now tell this reporter that those credentials were stolen in an email malware attack at Fazio that began at least two months before thieves started stealing card data from thousands of Target cash registers.



Two of those sources said the malware in question was Citadel — a password-stealing bot program that is a derivative of the Zeus banking trojan — but that information could not be confirmed. Through a PR firm, Fazio declined to answer direct questions for this story, and Target has declined to comment, citing an active investigation.

In a statement (PDF) issued last week, Fazio said it was “the victim of a sophisticated cyber attack operation,” and further that “our IT system and security measures are in full compliance with industry practices.”

It's a measure of how common these crimes have become, and how conventional the hackers' approach in this case, that Target was prepared for such an attack. Six months earlier the company began installing a \$1.6 million malware detection tool made by the computer security firm FireEye, whose customers also include the CIA and the Pentagon. Target had a team of security specialists in Bangalore to monitor its computers around the clock. If Bangalore noticed anything suspicious, Target's security operations center in Minneapolis would be notified.

# Sharing Time!





# Attack 1



## Overview

[\[Redacted\]](#) is the first Lebanese mobile network owned by the Republic of Lebanon and managed by [\[Redacted\]](#) Telecom, Media and Technology (C [\[Redacted\]](#) capitalizes on the vast know-how and international expertise of OTMT in order to deliver quality and professional solutions to the mobile sector in Lebanon. On October 25, 201 [\[Redacted\]](#) became the first mobile operator to launch 3G+ mobile broadband services in Lebanon, and in another major technological achievement, the company was the first to commercially launch 4G-LTE services in the country on May 15, 2013. [\[Redacted\]](#) currently serves over 1.85 million subscribers and covers 99% of Lebanon

**Login**

Username:

Password:

**Sign in**

[Forgot Password?](#)  
[Forgot Username?](#)  
[Register](#)  
[Privacy Policy](#)

## [\[Redacted\]](#) Management Team

<a href="#">[Redacted]</a>	Chairman & CEO	<a href="#">View Profile</a>
<a href="#">[Redacted]</a>	Chief Commercial Officer	
<a href="#">[Redacted]</a>	Chief Technology Officer	
<a href="#">[Redacted]</a>	Chief Financial Officer	
<a href="#">[Redacted]</a>	Vice President, HR & Administration	
<a href="#">[Redacted]</a>	Chief Communications Affairs Officer	
<a href="#">[Redacted]</a>	Chief Corporate Strategy & Quality Officer	

My Mobile  
Communicate  
Press Releases



## [\[Redacted\]](#) Vision

To become the leading telecom operator in Lebanon by providing high quality innovative services within a dynamic environment for our employees.

## [\[Redacted\]](#) Mission

To increase [\[Redacted\]](#) market share by anticipating market's needs and providing the best telecommunication service while increasing value to our stakeholders.

# Attack 1



me:  
rd:  
n  
password?  
username?  
Policy

ile  
nicate  
leases

re  
NG



Chairman and CEO [redacted]

[redacted]

Chairman and CEO, [redacted]

[redacted] took the helm of [redacted] the first Lebanese mobile operator managed by [redacted] m, as its Chairman and CEO, since the beginning of 2010, putting his international experience at the service of the Lebanese Telecom sector, by introducing state-of-the-art technology, and bringing Lebanon back on the regional telecom map, through leading the introduction of the 3G+ technology that was first launched by [redacted] in Lebanon in October 2011 as well as the introduction of 4G-LTE technology which [redacted] was the first to launch in Lebanon in May 2013.

[redacted] is an experienced telecom executive with more than 18 years of field and operations experience. Mr. [redacted] started his career with France Telecom in Lebanon – Cellis, known currently as [redacted] where he was part of the initial team that built the first GSM network in Lebanon, before joining later on the [redacted] telecom Holding family back in 1999.

Since 1999, [redacted] has held several assignments within the [redacted] m Telecom Group's subsidiaries and its Holding, the latest before his current appointment was in September 2007, where he joined Mobinil - Egypt that has more than 30 million subscribers, as VP Technology in charge of both network and IT infrastructure. With the winning of the Management agreement of [redacted] m, in February 2009, and in addition to his position at Mobinil, [redacted] on the Board of MIC1-Lebanon and [redacted] m Lebanon.

Prior to Mobinil [redacted] was the CTO of Mobilink-Pakistan (an [redacted] m Telecom subsidiary) since June 2003, where he played a major role in building an infrastructure capable of handling more than 30 million subscribers in less than four years. Between 2000 and 2002 [redacted] was part of the team who built Sabafon's network in Yemen in the position of CTO managing both Technical and IT departments. Moreover, his role in business development between January 2002 and June 2003, as [redacted] Technical Director was substantial, where he worked on various projects and acquisitions in Africa and Asia. The work of [redacted] contributed to the growth [redacted] to over 120Msubs where he contributed directly to building an infrastructure capable of handling more than 60 million subscribers.

Mr. [redacted] holds a Master's degree in Telecommunications and Electrical Engineering

# Attack 1



Search bar: [redacted]

Web **Images** Maps Shopping More Search tools

About 6 results (0.40 seconds)

Image size: 163 x 245  
Find other sizes of this image: All sizes - Small

Best guess for this image: [redacted]  
[redacted] profiles | LinkedIn  
View the profiles of [redacted] [redacted] LinkedIn. There are 11 professionals named [redacted] [redacted] change ...

Visually similar images - Report images  
[redacted] [redacted] [redacted]

Pages that include matching images  
Asaad [redacted] anyinfo.aspx  
CEO, Assaad Kassis, Chief

[redacted] https://[redacted]  
163 x 245  
Com  
Gam

Lebanon Mob [redacted]  
www.[redacted]  
590 x 315  
curre  
and mobile ...

Wired For Action - BOLD [redacted]  
www.bold-r[redacted]  
165 x 115 -  
chairman an  
bullish mood

[redacted] on Lebanese Telecom Sector, 3G and Regulations  
www.ma[redacted]  
590 x 315  
still infra  
in Leban

Lebanon Telecom - MarcoPolis [redacted]  
www.ma[redacted]  
590 x 315  
benefits  
Lebanes

# Attack 1



CEO of @ [redacted] family member. Telecom Veteran & a Football extremist. I believe in the power of positive attitude, humor & Internet everywhere.

481 TWEETS   86 FOLLOWING   397 FOLLOWERS   Follow

### Tweets

 @tmdebanon غرفة التحكم المروري  
حملة RT : #منحط\_دركي\_لكل\_بيارة\_تاركونا\_الصور\_لنتشارك\_المساءلة  
@ [redacted] @ziad\_hawat @WajihAkkari @blackhawkinc @eleferiades

Retweeted by [redacted]

Expand

 **Mashable** @mashable 3 Jan  
The world's largest pyrotechnics show, ever: on.mash.to /19TYK7p pic.twitter.com/FnrwRSR2dy



# Attack 1



The image shows a screenshot of a Twitter post. At the top, there is a banner for the "GSMA MOBILE 360 SERIES · MIDDLE EAST" event. The banner features a green globe icon on the left and navigation arrows on either side. Below the banner, the Twitter interface shows a user profile picture (a white square), a redacted name, and the date "21 Oct". The tweet text reads: "Attending GSMA mobile 360 event in Dubai. 410m mobile connections in MENA and 90m mobile broadband users. pic.twitter.com/DmTywQ[redacted]". At the bottom of the tweet, there are icons for "Reply", "Retweet", and "Favorite", along with a "Flag media" option.

**GSMA**  
**MOBILE 360**  
**SERIES · MIDDLE EAST**

21 Oct

Attending GSMA mobile 360 event in Dubai. 410m mobile connections in MENA and 90m mobile broadband users. pic.twitter.com/DmTywQ[redacted]

Reply Retweet Favorite Flag media

# Attack 1



Santanu Biswas  
Director, eHealth Services, du



Patrik Regardh  
Head of Strategic Marketing,  
Ericsson



George Held  
VP, Commerce,  
Etisalat



Ali Asgharzadeh  
Chief Commercial Officer,  
Etisalat Afghanistan



Asif Aziz  
Group Director Marketing  
Products and Propositions,  
Expresso Telecom



Dan Warren  
Director of Technology, GSMA

# Attack 1



**Asif Aziz, Group Director Marketing Products and Propositions, Espresso Telecom**

Asif started his telecom journey at Orange UK, at a time when the industry was at its origins. Asif introduced innovative concepts that helped Orange capitalise on market growth and make it the fastest growing operator in the UK. This was followed by a period at Talk Talk, a leading alternative fixed line carrier, where Asif held various roles in Product Marketing, including the introduction of an MVNO service and finally progressing to head of business. Asif then joined Wanadoo plc as Managing Director for Products and Services. Asif led the integration of the Wanadoo into France Telecom and the successful rebrand to Orange. Asif was then given responsibility for all Data services and revenue for Orange. To gain broader experience Asif joined an African Mobile Operator and is now responsible for the international marketing activity of the Group, covering a number of African Countries.

# Attack 1



Dear ,

It was great seeing you again. As we discussed at GSMA Mobile 360 in Dubai this past October, here is the link to the MENA Telecom Alliance <http://menatelecomalliance.com>.

I hope you agree to be one of our board members and help with moving Lebanon forward to the future in technology.

Best Regards,

Asif Aziz

Group Director Marketing Products and Propositions, Espresso Telecom

(Sent from a mobile device)

# Attack 1



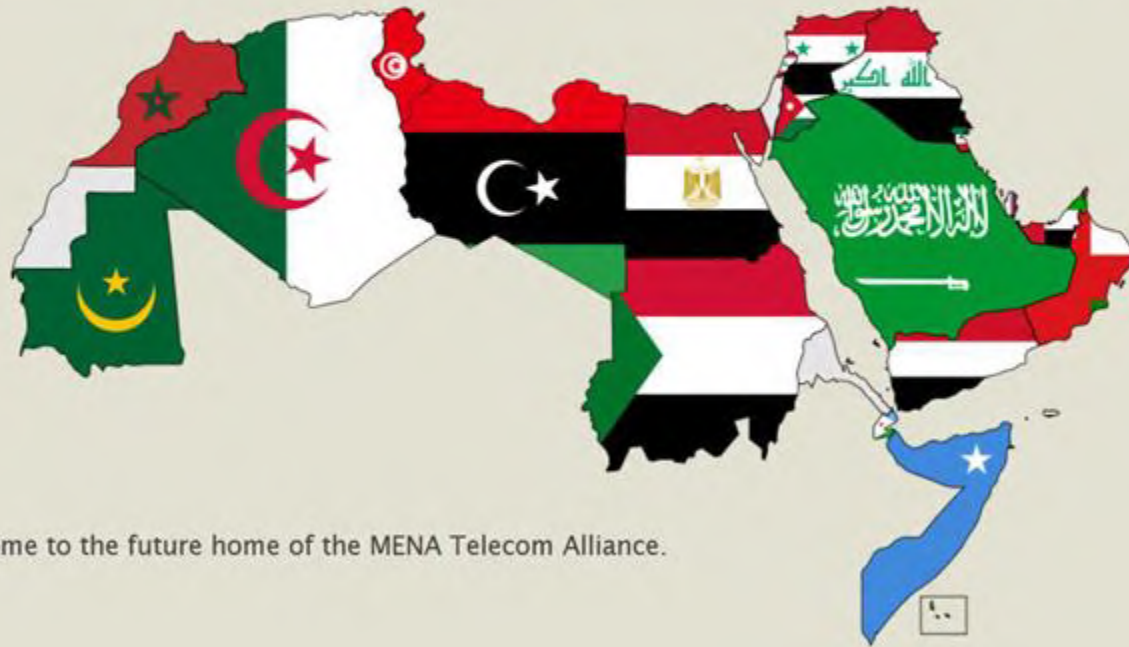
## MENA Telecom Alliance

Home

About Us

Contact

**UNDER CONSTRUCTION**



# Attack 1



BeEF 0.4.4.9-alpha | [Submit Bug](#) | [Logout](#)

Hooked Browsers

- Online Browsers
  - menatelecomalliance.com
    - 94.187.41.245
- Offline Browsers
  - 2012-12-08 19:00
  - 2012-12-08 19:00
  - 2012-12-08 19:00
  - 2012-12-08 19:00
  - 2012-12-08 19:00
  - 2012-12-08 19:00

Getting Started | Logs | **Current Browser**

**Details** | Logs | Commands | Rider | XssRays | Ipec

Category: **Browser (6 Items)**

Browser Name: Firefox	Initialization
Browser Version: 26	Initialization
Browser UA String: Mozilla/5.0 (Windows NT 6.3; WOW64; rv:26.0) Gecko/20100101 Firefox/26.0	Initialization
Browser Platform: Win32	Initialization
Browser Plugins: AVG SiteSafety plugin-v.17.3.0.49, Shockwave Flash-v.11.9.900.170, Google Update-v.1.3.22.3, Silverlight Plug-In-v.5.1.20913.0	Initialization
Window Size: Width: 1536, Height: 710	Initialization

Category: **Browser Components (14 Items)**

Flash: Yes	Initialization
VBScript: No	Initialization
PhoneGap: No	Initialization
Google Gears: No	Initialization
Silverlight: Yes	Initialization
Web Sockets: Yes	Initialization
QuickTime: No	Initialization
RealPlayer: No	Initialization
Windows Media Player: No	Initialization
Foxit Reader: No	Initialization
WebRTC: Yes	Initialization
ActiveX: No	Initialization
Session Cookies: Yes	Initialization
Persistent Cookies: Yes	Initialization

Category: **Hooked Page (5 Items)**

Page Title: Home	Initialization
------------------	----------------

Basic | Requester

# The Road Map of an Attack



# The Road Map of an Attack



Google largest bank portland maine

All News Images Maps Shopping More Search tools

About 358,000 results (0.97 seconds)

**Merger of Camden National and Bank of Maine creates ...**  
[www.pressherald.com/.../merger-of-camden-nation...](http://www.pressherald.com/.../merger-of-camden-nation...) Portland Press Herald  
Oct 16, 2015 - It is gaining branches in areas it previously did not cover, including Brunswick, Bath, Topsham, Falmouth, Saco and York. The acquisition of the Bank of Maine branch at 2 Canal Plaza in downtown Portland will significantly increase **Camden National's** exposure in Maine's largest market.

**Camden National plans to acquire The Bank of Maine - The ...**  
[www.pressherald.com/.../camden-national-bank-of-...](http://www.pressherald.com/.../camden-national-bank-of-...) Portland Press Herald  
Mar 30, 2015 - The acquisition, if successful, would significantly increase **Camden National's** presence in Portland, where The Bank of Maine is headquartered, and allow it to surpass Bangor Savings Bank as the largest Maine-based bank.

**Banks in Portland, Maine with Reviews & Ratings - YP.com**  
[www.yellowpages.com](http://www.yellowpages.com) Portland, ME Yellowpages.com  
Results 1 - 30 of 131 - Find 131 listings related to Banks in **Portland** on YP.com  
KeyCorp is one of the nation's **largest bank**-based financial services companies. ...

**The Maine 100 | PORTLAND MAGAZINE**  
[www.portlandmonthly.com/portmag/2010/09/the-maine-100-2/](http://www.portlandmonthly.com/portmag/2010/09/the-maine-100-2/)  
Sep 24, 2010 - In **Maine**, I think tourism is the big story of the year. You look at the ...  
People's United is the 22nd **largest bank** in America by deposits. It's the ...

**Proposed Merger Would Create Maine's Largest Bank ...**  
[news.mpbnet/post/proposed-merger-would-create-maines-largest-bank](http://news.mpbnet/post/proposed-merger-would-create-maines-largest-bank)  
Mar 30, 2015 - **CAMDEN, Maine** - The planned merger of two **banks** would create the **largest Maine-based bank** in the state. ... merger is successful, the **bank** will keep its headquarters in Camden, but keep some of its leadership in **Portland**.



# The Road Map of an Attack



BUSINESS

Posted October 16, 2015 Updated October 16, 2015

INCREASE FONT SIZE

## Merger of Camden National and Bank of Maine creates state's biggest community bank

The merger, Camden National Bank's largest purchase yet, is expected to be completed Friday.

BY J. CRAIG ANDERSON STAFF WRITER

[canderson@pressherald.com](mailto: canderson@pressherald.com) | [@JCraigAnderson](https://twitter.com/JCraigAnderson) | 207-791-6390

Share 2 Comments

The merger of The Bank of Maine into Camden National Bank will be completed Friday, creating Maine's largest community bank, with 64 branches, \$3.6 billion in assets and about 700 employees.

The combined bank will carry the Camden National brand. Customers will begin to see the transitioning of Bank of Maine's 24 branches to the new brand starting Monday. Their online and mobile banking also will shift automatically to Camden National.

"We're a different company come Monday morning," Camden National CEO Gregory Dufour said. The combined entity will incorporate the best aspects of the two community bank chains, he said.

As a result of the acquisition, Camden National is laying off 35 employees, about 5 percent of its combined workforce, Dufour said. It is also closing four Camden National branches – one in Gardiner, two in Augusta and one in Kennebunk – that are literally across the street or parking lot from each other. Signs at the closing branches will direct customers to the nearby branches.



BUSINESS

**USS Zumwalt so stealthy it uses special reflectors when it wants to be seen**



BUSINESS

**Jobs at risk in Legislature's decision on solar energy bill**



BUSINESS

**Week in review: Faster Cat, BIW stays busy and a new capital fund**



NEWS

**Trade specialists question science behind proposed export ban on lobsters**

# The Road Map of an Attack



Welcome to our redesigned website! Take a minute to explore a fresh new look, clear & concise content that responds to fit any device, and easy access to what you need—including a login to online banking on every page!



Online Banking [Login Help](#)

Login ID

Password

Login

Remember Me | [Forgot Password](#)

[I am a New User](#)  
[Consumer Enrollment](#)  
[Business Enrollment](#)

[LOCATIONS](#) | [CONTACT US](#) | [INVESTOR RELATIONS](#) | [SEARCH](#)

Products

## MONEY IN YOUR POCKET

Earn cash back on your everyday purchases.

Let Us Show You

[BANK](#) | [BORROW](#) | [LEARN](#) | [ABOUT](#)

What interests you today?

# The Road Map of an Attack

A screenshot of a web browser displaying the Camden National Bank website. The browser's address bar shows the URL 'https://www.camdennational.com'. The website has a blue header with a welcome message and a navigation menu. On the left, there is a login section with fields for 'Login ID' and 'Password', a 'Login' button, and links for 'Remember Me' and 'Forgot Password'. Below the login section are links for 'I am a New User', 'Consumer Enrollment', and 'Business Enrollment'. The main content area features a large image of a person's hands using a credit card at a payment terminal, with the text 'MONEY IN YOUR' and 'Earn cash back on your everyday p' overlaid. A blue button labeled 'Let Us Show You' is positioned below the text. At the bottom of the page, there is a navigation menu with links for 'BANK', 'BORROW', 'LEARN', and 'ABOUT', and a section titled 'What interests you today?'. Overlaid on the right side of the browser window is a window from 'TCPIPUTILS.com' showing IP lookup results for the IP address 147.202.127.203. The tool includes tabs for 'IPv4', 'IPv6', 'ISP', 'Domain', 'My IP', 'Premium', 'Options', and 'About'. The results show the IP address, location (Cedar Falls, Iowa, United States), registry (arn), network information (DNS servers, ASN number 14010, and ASN name Jack Henry & Associates, Inc.), and a search bar for other IP addresses.

Welcome to our redesigned website! Take a minute to explore a fresh new look, clear & concise content to fit any device, and easy access to what you need—including a login to online banking on every page.

Camden NATIONAL BANK

Online Banking [Login Help](#)

Login ID

Password

[Login](#)

Remember Me [Forgot Password](#)

[I am a New User](#)  
[Consumer Enrollment](#)  
[Business Enrollment](#)

LOCATIONS CONTACT US INVESTOR RELATIONS

## MONEY IN YOUR

Earn cash back on your everyday purchases

[Let Us Show You](#)

BANK BORROW LEARN ABOUT

What interests you today?

TCPIPUTILS.com

IPv4 IPv6 ISP Domain My IP Premium Options About

IPv4 root -> 147.8 -> 147.202.127.0/24 -> 147.202.127.203

type domain, IPv4/IPv6 or provider [Search](#)

### IP information 147.202.127.203

IP address	147.202.127.203
Location	Cedar Falls, Iowa, United States (US)
Registry	arn

### Network information

IP address	147.202.127.203
Reverse DNS (PTR record)	not available
DNS server (NS record)	ns1.teamnet.net (209.98.98.1) ns2.teamnet.net (86.254.98.138) ns3.teamnet.net (86.254.98.138)
ASN number	14010
ASN name (ISP)	Jack Henry & Associates, Inc.

# The Road Map of an Attack



Domains on 147.202.127.203

- fnb.com
- ffmbank.com
- westernbankwp.com
- ent.com
- wauchulastatebank.com
- incrediblebank.com
- citizensbanktn.com
- tlccu.org
- myfamilybusiness.com
- fhbank.com
- Domain Neighbors 147.202.127.203

Domains around 147.202.127.203

IP address	#domains
<a href="#">147.202.127.5</a>	9

# The Road Map of an Attack



Number of SPAM hosts on 147.202.127.0/24 0

SPAM tools **DNSBL 147.202.127.203**

### Blocklist lookup

Adult hosting listed ❌  
At least one domain hosted on this IP address is marked as containing adult content. [more info](#)

Hackers, Spyware, Botnets etc. not listed ✅

Open proxy not listed ✅

### Open TCP/UDP ports

Status well known TCP and UDP ports. Note: we do not perform any port scan but use data of the ZMap project.

Description	Protocol/Port	Status
HTTP	tcp80	Open ❌
HTTPS	tcp443	Open ❌
DNS	udp53	Closed ✅
Network Time Protocol (NTP)	udp123	Closed ✅
NetBIOS Name Service	udp137	Closed ✅
Session Initiation Protocol (SIP)	udp5060	Closed ✅

# The Road Map of an Attack



```
Domain Name: CAMDENNATIONAL.COM
Registry Domain ID: 2519393_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.activeregistrar.com
Registrar URL: http://www.activeregistrar.com
Updated Date: 2014-11-29T04:25:47Z
Creation Date: 1998-09-02T04:00:00Z
Registrar Registration Expiration Date: 2016-09-01T04:00:00Z
Registrar: Active Registrar, Inc
Registrar IANA ID: 1090
Domain Status: OK https://icann.org/epp#OK
Registry Registrant ID:
Registrant Name: David Ackley
Registrant Organization: Camden National Corporation
Registrant Street: 245 Commercial Street
Registrant City: Rockport
Registrant State/Province: ME
Registrant Postal Code: 04856
Registrant Country: US
Registrant Phone: +1.2072302329
Registrant Phone Ext:
Registrant Fax: +1.2072302033
Registrant Fax Ext:
Registrant Email: dackley@camdennational.com
Registry Admin ID:
Admin Name: David Ackley
Admin Organization: Camden National Corporation
Admin Street: 245 Commercial Street
Admin City: Rockport
Admin State/Province: ME
Admin Postal Code: 04856
Admin Country: US
Admin Phone: +1.2072302329
```

# The Road Map of an Attack



Google Camden National Bank

All Maps Apps News Shopping More Search tools

About 741,000 results (0.97 seconds)

**Camden National Bank - Banking the Way You Live Today ...**  
<https://www.camdennational.com/> - Camden National Bank -  
Camden National Bank offers innovative products and services that fit the way you live. We provide banking, mortgage, business loans, and more.

<b>Online Banking</b> With our online banking, your bank is always - or text all within ...	<b>Careers</b> Employees of Camden National Bank receive extensive ...
<b>Locations</b> Camden - Belfast - Orono - Portland - Rockland - Waterville ...	<b>Open a Personal Checking ...</b> At Camden National Bank, we offer the checking account products ...
<b>Personal</b> Welcome to personal banking at its best. Personal banking, like life ...	<b>Mobile Banking</b> Need help using online banking? Check out our Mobile Banking ...

[More results from camdennational.com »](#)

**Camden National Bank - Facebook**  
[www.facebook.com/CamdenMaine](http://www.facebook.com/CamdenMaine) - Camden, Maine - Local Businesses - Bank -  
Camden National Bank, Camden, Maine. 9799 likes - 94 talking about this. Camden National Bank is an independent, Maine-based community bank that has ...

**Camden National Bank - Android Apps on Google Play**  
<https://play.google.com/store/apps/details?id=com.camden3199android> -  
★★★★★ Rating: 3.5 - 179 votes - Free  
Bank from your mobile device and make more of your time yours with Camden National Bank's mobile banking app. Quickly and easily access your accounts ...

**Camden National Bank (@camdenational) | Twitter**  
<https://twitter.com/camdenational> -  
The latest Tweets from Camden National Bank (@camdenational). "Congrats to our own Ben Gray & his U16 Maine Moose on winning the 2016 U16 T2 ..

**Camden National Bank | LinkedIn**  
<https://www.linkedin.com/company/camden-national-corporation> - LinkedIn -

# The Road Map of an Attack



## Camden National Bank



Camden National Corporation, recently recognized by Forbes magazine as one of "America's Most Trustworthy Companies," is the holding comp... Show more

### Uploads



Camden National Bank: Hope@Home  
203 views · 4 weeks ago



Employee Appreciation Day 2016  
534 views · 1 month ago



Camden National Bank: Here, anywhere  
43,476 views · 5 months ago



Use Your Camden National Chip Card Everywhere!  
103 views · 6 months ago



Camden National Bank: Strength, Security and Stability  
42 views · 1 year ago




Secure and Reliable Banking with Camden National Bank  
69 views · 1 year ago



# The Road Map of an Attack






**Camden National Bank**  
Banking  
501-1000 employees

1,077 followers [Follow](#)

[Home](#)




Camden National Bank is a full-service community bank that's been supporting Maine's people and businesses since 1875. With advanced online and mobile banking solutions, a statewide network of 64 banking centers and 85 ATMs, and rewards for everyday banking, we offer smart solutions to fit your


[See more](#)

### Recent Updates

Camden National Bank Spring brings new things! We are now on Instagram and need some fresh new followers! Every Friday until May 6th we'll give a \$25 gift card to one random follower. All you have to do is follow @CamdenNational on Instagram!




### How You're Connected



6 second-degree connections  
369 Employees on LinkedIn

[See all](#)

### People Also Viewed



# The Road Map of an Attack

A screenshot of the Camden National Bank Twitter profile page. The header shows the bank's name in large blue letters and its anchor logo. Below the header, the profile name "Camden National Bank" and handle "@camdenational" are visible, along with location "Camden, Maine", website "camdenational.com", and "Joined November 2009". A tweet from 3 hours ago is displayed, mentioning a bowling event for youth mentoring. The tweet includes a photo of a group of people in blue shirts at a bowling alley.

**Camden National Bank**  
@camdenational

Camden, Maine  
camdenational.com  
Joined November 2009

TWEETS 604 FOLLOWING 233 FOLLOWERS 278 LIKES 140

Tweets Tweets & replies Media

**Camden National Bank** @camdenational · 3h  
Bowling to support #youthmentoring and @BBBSofMidMaine in the Midcoast this past weekend. #community

A group photo of approximately 15 people, mostly women, wearing blue polo shirts with the Camden National Bank logo. They are standing in a bowling alley. In the background, there are bowling lanes and a sign that says "Big Brothers Big Sisters" and "KLANDling".

# The Road Map of an Attack



Camden National Bank

Spring brings new things-check out our NEW website!

Camden National Bank

Learn More Like Message

Timeline About Photos Videos Likes

Search for posts on this Page

9,806 people like this

invite friends to like this Page

ABOUT

2 Elm St  
Camden, ME

(800) 860-8821

Ask for Camden National Bank's hours

Ask for Camden National Bank's price range

Typically replies within an hour  
Message Now

http://www.camdenational.com/

Status Photo / Video

Write something on this Page...

Camden National Bank added 10 new photos.  
4 hrs

Our Camden, Rockport and Rockland employees had a great time supporting Big Brothers Big Sisters of Mid-Maine this past weekend! Eleven teams took part in Bowl for Kids' Sake events at Oakland Park Bowling Lanes and Point Lookout Resort & Conference Center to raise funds for youth mentoring in our communities.

# The Road Map of an Attack




A screenshot of a Facebook post from the page 'Camden National Bank'. The post, dated 'Yesterday at 4:32pm', contains a video player and text: 'Spring brings new things! We are now on Instagram and need some fresh new followers! Every Friday until May 6th we'll give away a \$25 gift card to one random follower. All you have to do is follow @CamdenNationalBank'. A 'People Who Shared This' popup window is open, showing a share by 'Liz Ford Wyman' from 'Yesterday at 7:40pm'. The popup includes a 'Show Attachment' field and a 'Share' button. The background shows the Facebook interface with a 'Create Page' button, a 'Recent' list (2016-2011), and a list of users who liked the page: 'LAUGH loud SMILE big', 'Farnsworth Art Museum', and 'The Crooked Mile Cafe'. The main post image shows a blue anchor logo over a field of yellow daffodils.

# The Road Map of an Attack



**“WHAT DO YOU DO?”**

**I SAY,  
WHATEVER IT TAKES”**

 **Liz Ford Wyman** [Add Friend](#) [Message](#) [...](#)

[Timeline](#) [About](#) [Friends](#) [Photos](#) [More ▾](#)


DO YOU KNOW LIZ?


To see what she shares with friends, send her a friend request. [Add Friend](#)

**Intro**


- Works at Camden National Bank and Homemaker/Wife/Mom
- Studied Business at University of Maine
- Lives in Bath, Maine
- Married to Bert Wyman
- From Phippsburg, Maine

**Photos**



**Leslie Wyman**  
54 mins · 

Liz Ford Wyman



# The Road Map of an Attack



**I SAY, WHATEVER IT TAKES**

Liz Ford Wyman

Timeline About Friends Photos More

DO YOU KNOW LIZ?

To see what she shares with friends, send her a friend request.

About

To see what she shares with friends, send her a friend request.

**Overview**

- Work and Education
  - Works at Camden National Bank and Homemaker/Wife/Mom
    - Past J. Edward Knight and J Edward Knight Insurance
  - Studied Business at University of Maine
    - Past Morse High School and Morse High School
  - Lives in Bath, Maine
    - From Phippsburg, Maine - Lived in Bangor, Maine
  - Married to Bert Wyman
    - Married since October 22, 1994
- Places She's Lived
- Contact and Basic Info
- Family and Relationships
- Details About Liz
- Life Events

# The Road Map of an Attack














# The Road Map of an Attack



**Friends** [Add Friend](#)

[All Friends](#) [Recently Added](#) [Work](#) [College](#) [High School](#) [Current City](#) [Hometown](#) [Following](#)

Liz's friends who also work at Camden National Bank

 <p><b>Stephanie Patterson</b> Works at Camden National Bank</p> <a href="#">Add Friend</a>	 <p><b>Caitlin Bean</b> Vault Teller at Camden National Bank</p> <a href="#">Add Friend</a>
 <p><b>Dianne M Pottle</b> Bank Teller at Camden National Bank</p> <a href="#">Add Friend</a>	 <p><b>Derek Beaulieu</b> Banking Center Manager at Camden National Bank</p> <a href="#">Add Friend</a>
 <p><b>Holly C Sears</b> Branch Operations Supervisor at Camden National Bank</p> <a href="#">Add Friend</a>	 <p><b>Leslie Coffin Barter</b> Assistant Manager at Camden National Bank</p> <a href="#">Add Friend</a>
 <p><b>Edythe Morgan Dersham</b> Assistant branch manager at Camden National Bank</p> <a href="#">Add Friend</a>	 <p><b>Stephanie Purnell</b> Works at Camden National Bank</p> <a href="#">Add Friend</a>
 <p><b>Walter Reynolds</b> Partner at Self employed</p> <a href="#">Add Friend</a>	 <p><b>Zoe Simard</b> Works at Camden National Bank</p> <a href="#">Add Friend</a>
 <p><b>Keitha R Smith</b> Assistant Branch Manager at Camden National Bank</p> <a href="#">Add Friend</a>	

















# The Road Map of an Attack



**Friends** Add Friend

All Friends Recently Added Work College High School Current City Hometown Following

 <p><b>Rodney Leach</b> Linn Tech</p> <span>Add Friend</span>	 <p><b>Fred Brewer</b> Certified Public Accountant at William Brewer CPA</p> <span>Add Friend</span>
 <p><b>David Phillips</b> Morse High School</p> <span>Add Friend</span>	 <p><b>Marla Bouchard</b> Customer Service at Isamax Snacks Inc.</p> <span>Add Friend</span>
 <p><b>Larry Scott</b> University of Maine at Augusta Athletics</p> <span>Add Friend</span>	 <p><b>David Ater</b> Bath, Maine</p> <span>Add Friend</span>
 <p><b>Nick Merry</b> Assistant Chief at Wiscasset Fire Department</p> <span>Add Friend</span>	 <p><b>Stephanie Purnell</b> Works at Camden National Bank</p> <span>Add Friend</span>
 <p><b>Caroline Russell</b> Tufts University</p> <span>Add Friend</span>	 <p><b>Stephanie Patterson</b> Works at Camden National Bank</p> <span>Add Friend</span>
 <p><b>Stacy Simpson Frizzle</b> Executive Director at People Plus Maine</p> <span>Add Friend</span>	 <p><b>Holly C Sears</b> Branch Operations Supervisor at Camden National Bank</p> <span>Add Friend</span>
 <p><b>Richard Reed</b></p> <span>Add Friend</span>	 <p><b>Beverly Pye</b></p> <span>Add Friend</span>

# The Road Map of an Attack



The screenshot shows a Facebook profile for Holly C Sears. The profile picture is a woman with dark hair, smiling. The cover photo features a quote: "and do what you think is right for you." with the website "ilikeloquale.com" below it. The name "Holly C Sears" is displayed, along with "Add Friend" and "Message" buttons. Navigation tabs for "Timeline", "About", "Friends", "Photos", and "More" are visible. Below the profile, there are two "DO YOU KNOW HOLLY?" prompts, each with an "Add Friend" button. The "About" section is expanded to show an "Overview" of her work and education. Her work history includes "Branch Operations Supervisor at Camden National Bank" and "Past Pine State Trading and Juan Tio's Margarita's". Her education includes "Studied Dental Hygiene at University of Maine at Augusta" and "Past Carrabec High School". She is listed as living in Lewiston, Maine, having previously lived in Anson, Maine and Waterville, Maine. She is also shown to be in a relationship with Nick Maglione since January 23, 2016.

and do what you think is right for you.  
ilikeloquale.com

Holly C Sears

Add Friend Message

Timeline About Friends Photos More

DO YOU KNOW HOLLY?

To see what she shares with friends, send her a friend request.

Add Friend

About

To see what she shares with friends, send her a friend request.

Add Friend

**Overview**

Work and Education

Places She's Lived

Contact and Basic Info

Family and Relationships

Details About Holly

Life Events

Branch Operations Supervisor at Camden National Bank  
Past Pine State Trading and Juan Tio's Margarita's

Studied Dental Hygiene at University of Maine at Augusta  
Past Carrabec High School

Lives in Lewiston, Maine  
From Anson, Maine - Lived in Waterville, Maine

In a relationship with Nick Maglione  
In a relationship since January 23, 2016

# The Road Map of an Attack



 **Liz Ford Wyman** checked in to  Yankee Lanes Brunswick.  
April 2 at 8:41am · Brunswick, ME · 

BOWL FOR KIDS SAKE! 🎳



**Yankee Lanes Brunswick**  
Bar & Grill · Brunswick, ME ·  4,255 people checked in here 

 Share

  55

View 3 more comments

 **Liz Ford Wyman** We miss you Kelly Drouin Klaiber!! Mara Kane Pennell it was  
great to spend some time with you! Cecilia Smith see you soon!!

# The Road Map of an Attack



Email Format

Browse Domains

Search

Pricing

Login

Home > Domain > camdennational.com

Search for domains...

Want to directly email someone at **Camden National Corporation** but don't know their address? Maybe you just had an interview and didn't get a business card for a follow-up? Or you've got a name and nothing more from LinkedIn? Don't sweat it, we've got you covered.

Get the email address format for people working at

**camdennational.com**



Identified Name Formats Representative Email Addresses Export to Excel

high confidence

first\_initial last\_name e.g. JSmith@camdennational.com

low confidence

last\_name e.g. Smith@camdennational.com

first\_name last\_initial e.g. JohnS@camdennational.com

first\_name e.g. John@camdennational.com

last\_name first\_initial e.g. SmithJ@camdennational.com

# The Road Map of an Attack



Identified Name Formats

Representative Email Addresses

Export to Excel

rmquimby@camdenational.com

score 0 (found Sep 2013 - [www.uniontrust.com/contact](http://www.uniontrust.com/contact))

dfield@camdenational.com

score 0 (found Sep 2013 - )

cbredeau@camdenational.com

score 0 (found Sep 2013 - )

dgagne@camdenational.com

score 0 (found Sep 2013 - [www.uniontrust.com/contact](http://www.uniontrust.com/contact))

bkelley@camdenational.com

score 0 (found Sep 2013 - )

jbatchelder@camdenational.com

score 0 (found Aug 2013 - )

meldridge@camdenational.com

score 0 (found Sep 2013 - [www.uniontrust.com/contact](http://www.uniontrust.com/contact))

rlittlefield@camdenational.com

score 0 (found Jul 2013 - )

jparent@camdenational.com

score 0 (found Jul 2013 - )

gdufour@camdenational.com

score 0 (found Sep 2013 - )

driley@camdenational.com

score 0 (found Jul 2013 - [www.uniontrust.com/contact](http://www.uniontrust.com/contact))

njeffers@camdenational.com

score 0 (found Jul 2013 - )

crackliff@camdenational.com

score 0 (found Sep 2013 - )

slowell@camdenational.com

score 0 (found Aug 2013 - [www.uniontrust.com/contact](http://www.uniontrust.com/contact))

jdutson@camdenational.com

score 0 (found Jul 2013 - )

# The Road Map of an Attack



To [lizyman@camdenational.com](mailto:lizyman@camdenational.com)

CC [Holly C. Sears](#)

BCC

This has me worried.

Hello Liz,

After such a great day bowling on the 2nd I received a message from one of our customers who was also there for the event at Yankee Lanes. He said he really appreciated our community spirit and after the event felt moved to warn me of a protest he just heard about that was being planned for your branch by a bunch of Bernie Sanders supporters who will be marching in protest of what he calls Mrs. Clinton's love affair with banks & Wall Street! From the description of the protest on their website located here... <http://badlink.com> I am truly worried look at it yourself and please inform everyone at the branch to be prepared for this!!!

Regards,

Holly C. Sears

(Sent from a mobile device)

# INTRO



## ITWeb SECURITY

HOME | **OPINION** | IN DEPTH | PUBLICATIONS | SURVEYS | JOBS | SERVICES | EVENTS | VIDEO | ABOUT

BUSINESS | CHANNEL | COMPUTING | ENTERPRISE | FINANCIAL | HARDWARE | INTERNET | NETWORKING | SEC

VIRTUAL PRESS OFFICES™

COMPANY ZONES

Advertise on ITWeb

### Uptick in social media-based attacks

By Admire Moyo, ITWeb's senior news journalist  
Johannesburg, 31 Oct 2016

Cyber **criminals** are taking advantage of social media networks to spread malware and steal money from unsuspecting users.

This is one of the biggest findings in the Easy **Solutions** 2016 Fraud Beat report released on Friday. The report identifies the most recent and sophisticated cyber attacks impacting companies, financial institutions and consumers across the globe.

The digital revolution, led by users who are always connected to the internet through their smartphones, offers boundless financial opportunities for banks and businesses, says Easy Solutions. However, the **security** solutions vendor notes the digital revolution is also attracting the attention of cyber criminals for the same reasons.

There are over 80 million fake profiles on Facebook, Twitter and Instagram alone, and a large portion are used to launch social media attacks, the vendor notes.

Facebook announced it had surpassed a billion-and-a-half users at the end of last year, the report notes. Its user base would be the largest nation in the world if it were a country, even bigger than China.

Facebook estimates 2% of its 1.6 billion users are fake, which translates into more than 30 million counterfeit accounts. Twitter estimates about 5% of its profiles are fake, while Instagram approximates this number at around 8%.



The prevalence of social media has not gone unnoticed by cyber criminals.

#### See also

- Social media goes 'lite' in emerging markets
- Facebook Lite hits 100m users
- Social media attacks

# The Road Map of an Attack





# Be One With The Attacker




So what can we do?



# Attacker Recon



## INTELTECHNIQUES.com



MICHAEL BAZZELL  
OSINT TRAINER &  
PRIVACY CONSULTANT

Home Blog Forum Online Training Live Training Bio Privacy Links Books Contact

Open Source Intelligence Links (Updated January 01, 2016 at [IntelTechniques.com](http://IntelTechniques.com))  
**Free Newsletter and Video [HERE](#)**

- Custom Search Tools
- Training Guides
- Search Engines
- Facebook
- Google Plus
- Twitter
- Smaller Networks
- Maps
- Photos
- Archives
- People Engines
- Social Traffic
- Documents
- Businesses
- Auctions/Classifieds
- Dating/Meetups
- User Names
- Email Addresses
- Telephone Numbers

### Instant Access!

You can order your online video training package with any credit card right now and receive immediate access to the entire training! Click an option below to order today.

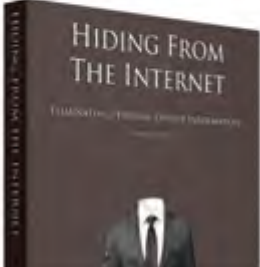
**ORDER NOW**  
\$399 FOR ONE MONTH

**ORDER NOW**  
\$999 FOR ONE YEAR

Contact Us to order by check or money order.

### New Privacy Guide

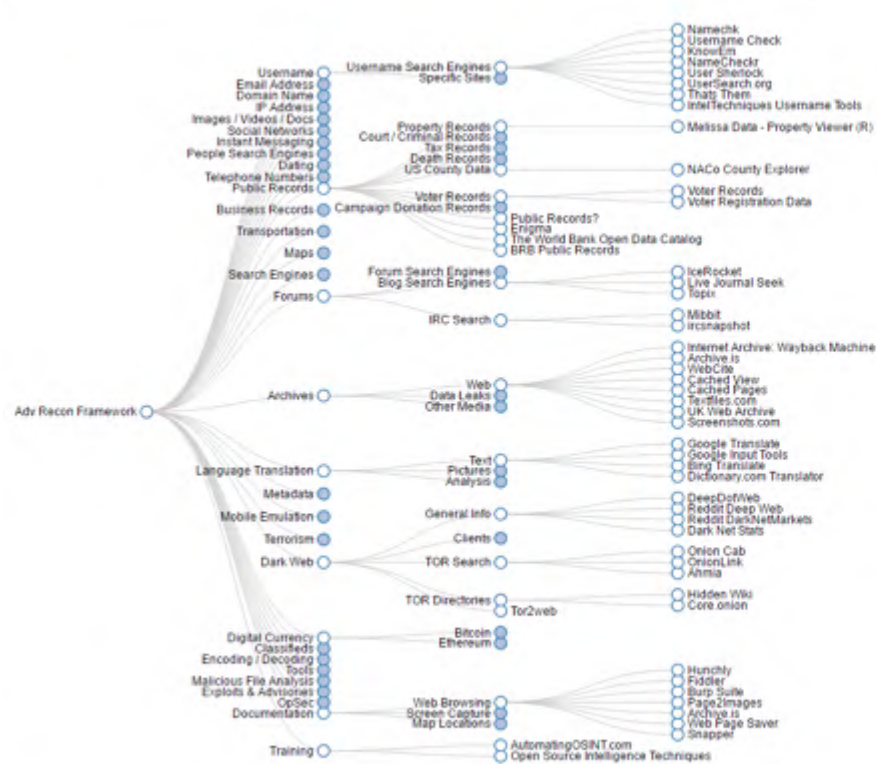
The Third Edition (2016) of my book on digital privacy is now available:



# Attacker Recon



## OSINT Framework



### Notes

OSINT framework focused on gathering information from free tools or resources. The intention is to help people find OSINT resources that return free information. Some of the sites included may require registration or offer more data for \$\$\$, but you should be able to get at least a portion of the available information for no cost.

# Attacker Recon



Shodan Exploits Scanhub Maps Blog Anniversary Promotion Settings Logout Buy ?

**SHODAN**  Search

Home Search Directory Data Analytics/ Exports Developer Center Labs

Popular Searches Recently Added Browse Tags

### Browse All Searches

#### Popular Searches

Date	Search	Description	Count	Tags
15 MAR 10	<b>Webcam</b>	best ip cam search I have found yet.	3035	webcam surveillance cams
13 JAN 12	<b>Netcam</b>	Netcam	837	netcam
6 FEB 12	<b>Cams</b>	admin admin	724	cam webcam
13 AUG 10	<b>dreambox</b>	dreambox	832	dreambox
14 JAN 10	<b>default password</b>	Finds results with "default password" in the banner; the named defaults might work!	305	router default password
20 JAN 10	<b>netgear</b>	user: admin pass: password	258	

#### Search the Directory

 Search

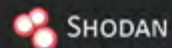
#### List All Searches By

- » Popularity
- » Recently Added

#### Popular Tags

webcam	60
scada	48
http	41
camera	40
router	40
ftp	38
test	35
cam	35
cisco	30
ssh	28

# Attacker Recon



Server: SQ-WEBCAM



Explore

Downloads

Reports

Enterprise Access

Contact Us

Exploits

Maps

Like 6,648

Download Results

Create Report

## TOP COUNTRIES



Lithuania	27
United States	26
Czech Republic	26
Hungary	21
Germany	21

## TOP SERVICES

HTTP	138
HTTP (8080)	25

Total results: 234

## --- VIDEO WEB SERVER ---

83.18.187.130

lvf130.intermetal.plnet.pl

Orange Polska

Added on 2018-02-28 08:50:01 GMT

Poland

Details

HTTP/1.1 200 OK

Connection: close

Cache-Control: no-cache

Server: SQ-WEBCAM

CONTENT-LENGTH: 2936

## --- VIDEO WEB SERVER ---

87.91.195.43

ip07-01-195-43.z195-0

XO Communications

Added on 2018-02-28

United States

Details



# Attacker Recon



The screenshot shows the IceChat 7.0 Alpha Build 082405 interface. The window title is "IceChat 7.0 Alpha Build 082405 - [#icechat [15] [+ Int 20] [QuakeNet]]". The menu bar includes "Main", "Options", "View", "DCC", "Server List", "Search", "Script Menu", "Window", and "Help". The toolbar contains various icons for actions like connect, disconnect, and search. The main chat area displays a log of messages, including topic changes and user join/quit events. A "Favorite Servers" list is visible on the left, and a "Nick List" is on the right. The "Buddy List" and "Favorite Channels" sections are at the bottom.

**Favorite Servers**

- irc.quakenet.org
- oslo.no.eu.undernet.org
- us.undernet.org
- irc.winbots.org
- irc.qeast.net
- amsterdam.nl.eu.underne
- irc.freenode.net
- irc.undernet.org
- powertech.no.eu.dal.net
- irc.qeast.net

**TOPIC:** Welcome to IceChat Support - IceChat 5.50 Released - IceChat 7 Alpha 082405 Released - www.icechat.net

**Nick List**

#icechat:15

@ Icebot	~IceBot@Ic
@ L	The.Bot@ig
@ madmn	~madmn@d
@ Snerf	icechat@Ice
+ ZeleD^BNC	zeled@bnc2
[gk]Joline	icechat5@A
aldorf	~icechat5@
c90368	~icechat5@
DanielBak	IceChat7@6
nukii	~icechat5@
Quaker	icechat5@2
rab3^bnc	rab3@frist.
Revanche	~icechat5@
TH3D4M4G3	~icechat5@
Uwana[OFF]	crAze@[LRF

[15:59.47] \* Icebot sets topic to: Resynchronizing Topic...

[15:59.48] \* Icebot sets topic to: Welcome to IceChat Support - IceChat 5.50 Released - IceChat 7 Alpha 082405 Released - www.icechat.net/forums/

[16:01.25] \* ssbmifreak (~icechat5@p508C0FF6.dip.t-dialin.net) Quit (Quit: The early bird may get the worm, but the second mouse gets the cheese)

[16:04.47] \* Icebot sets mode +I 17 for #icechat

[16:05.44] \* aldorf (~icechat5@dec-81-27-196-13.karneval.cz) has joined #icechat

[16:07.02] \* TH3D4M4G3 (~icechat5@p54ADE181.dip.t-dialin.net) has joined #icechat

[16:08.15] \* MDN (~icechat5@c189129.adsl.hansenet.de) has joined #icechat

[16:11.57] \* Guest\_419 (icechat5@69-169-98-71.ontrca.adelphia.net) has joined #icechat

[16:12.03] \* Guest\_419 (icechat5@69-169-98-71.ontrca.adelphia.net) has left #icechat

[16:12.13] \* xeQ (~icechat5@xds1-87-78-57-237.netcologne.de) has joined #icechat

[16:14.04] \* xeQ (~icechat5@xds1-87-78-57-237.netcologne.de) Quit (Quit: Not that there is anything wrong with that)

[16:14.13] \* MDN (~icechat5@c189129.adsl.hansenet.de) Quit (Signed off)

[16:14.44] \* xeQ (~icechat5@xds1-87-78-57-237.netcologne.de) has joined #icechat

[16:14.47] \* Icebot sets mode +I 20 for #icechat

[16:16.11] \* xeQ (~icechat5@xds1-87-78-57-237.netcologne.de) Quit (Quit: OUCH!!!)

[16:16.51] \* ShavingSheep (icechat5@207.90.221.180) has joined #icechat

[16:17.15] \* ShavingSheep (icechat5@207.90.221.180) has left #icechat

[16:17.19] \* nukii (~icechat5@xds1-87-78-57-237.netcologne.de) has joined #icechat


# Attacker Recon



Board index Wiki IRC Escrow



FAQ Search Register Login

(UPDATED) Visa Debit Card with IBAN, 4 currencies, Lowest Prices! Unlimited Stealth Paypal Accounts and How to Withdraw  
4 Sell - FRESH - CHEAP & GOOD cvv2 USA/Canada









It is currently Sat Mar 02, 2013 1:31 pm

View unanswered posts • View active topics

ADMINISTRATION	TOPICS	POSTS	LAST POST
 <b>Announcements</b> news, updates, and other need to know information regarding the site	44	423	by caeropore  Sat Mar 02, 2013 9:52 am

GENERAL	TOPICS	POSTS	LAST POST
 <b>Open Discussion</b> talk about anything that isn't relevant somewhere else. leave all introductions in the Introductions thread. news threads go in the News section. any posted here will be removed. Moderators: <b>l0v3h8</b> , <b>l0rax</b>	1406	9194	by Guest  Sat Mar 02, 2013 1:13 pm
 <b>News</b> if you have any recent news to share post it here. remember to cite source. Moderators: <b>l0v3h8</b> , <b>l0rax</b>	179	583	by caeropore  Sat Mar 02, 2013 8:43 am
 <b>Privacy</b> for discussions on cryptography, darknets, anti-forensics, and anything related to keeping LE off your back Moderator: <b>l0v3h8</b>	583	4145	by Guest  Sat Mar 02, 2013 11:08 am

# Attacker Recon



pastebin.com/sSame2Um



PASTEBIN

+ new paste

trends

API

tools

faq



PASTEBIN

+ new paste

trends

API

tools

faq

search...



Pastebin PRO Accounts AUTUMN SPECIAL! For a limited time only get 40% discount



china bins

RU\_SKIMMER OCT 29TH, 2013 615 NEVER

text 8.41 KB

```
3. 356829 CN JCB CREDIT
4. 356895 CN JCB CREDIT CHINA CONSTRUCTION BANK
5. 370246 CN AMEX CREDIT PEONY INDUSTRIAL AND COMMERCIAL BANK OF
6. 370247 CN AMEX CREDIT PEONY INDUSTRIAL AND COMMERCIAL BANK OF
7. 370285 CN AMEX CREDIT GREEN CHINA MERCHANTS BANK
8. 370286 CN AMEX CREDIT GOLD CHINA MERCHANTS BANK
9. 376343 TW AMEX CREDIT CLASSIC CATHAY PACIFIC
10. 376346 TW AMEX CREDIT GOLD AMERICAN EXPRESS TAIWAN
11. 376347 TW AMEX CREDIT
12. 376348 TW AMEX CREDIT
13. 376349 TW AMEX CREDIT
14. 376350 TW AMEX CREDIT
15. 376351 TW AMEX CREDIT
16. 376352 TW AMEX CREDIT
17. 376353 TW AMEX CREDIT
18. 376354 TW AMEX CREDIT
19. 400936 TW VISA CREDIT INFINITE CHINATRUST COMMERCIAL BAN
20. 400935 TW VISA CHANG HIA COMMERCIAL BANK, LTD.
21. 400937 CN VISA CREDIT CORPORATE T&E BOC CREDIT CARD (INTERNAT
22. 400938 CN VISA CREDIT CORPORATE T&E BOC CREDIT CARD (INTERNAT
23. 400939 CN VISA CREDIT CORPORATE T BOC CREDIT CARD (INTERNAT
24. 400940 CN VISA CREDIT CORPORATE T BOC CREDIT CARD (INTERNAT
25. 400941 CN VISA CREDIT CLASSIC BOC CREDIT CARD (INTERNATIONAL),
26. 400942 CN VISA CREDIT PREMIER BOC CREDIT CARD (INTERNATIONAL),
27. 400996 TW VISA MEGA INTERNATIONAL COMMERCIAL BANK
28. 402330 TW VISA CREDIT PLATINUM CATHAY UNITED BANK
29. 402325 CN VISA CHINA UNIONPAY CO., LTD.
30. 402334 TW VISA CREDIT CLASSIC AEON CREDIT CARD (TAIWAN) CO., LT
```

text 36.62 KB

raw download clone embed report print

```
3. ADD ME FOR MORE DEALS WITH ANY BIN OF YOURS
4. CONTACT
5. 660206082
6. dumps_great@yahoo.com
7. 356829 CN JCB CREDIT
8. 356895 CN JCB CREDIT CHINA CONSTRUCTION BANK
9. 370246 CN AMEX CREDIT PEONY INDUSTRIAL AND COMMERCIAL BANK OF CHINA
10. 370247 CN AMEX CREDIT PEONY INDUSTRIAL AND COMMERCIAL BANK OF CHINA
11. 370285 CN AMEX CREDIT GREEN CHINA MERCHANTS BANK
12. 370286 CN AMEX CREDIT GOLD CHINA MERCHANTS BANK
13. 376343 TW AMEX CREDIT CLASSIC CATHAY PACIFIC
14. 376346 TW AMEX CREDIT GOLD AMERICAN EXPRESS TAIWAN
15. 376347 TW AMEX CREDIT
16. 376348 TW AMEX CREDIT
17. 376349 TW AMEX CREDIT
18. 376350 TW AMEX CREDIT
19. 376351 TW AMEX CREDIT
20. 376352 TW AMEX CREDIT
21. 376353 TW AMEX CREDIT
22. 376354 TW AMEX CREDIT
23. 400936 TW VISA CREDIT INFINITE CHINATRUST COMMERCIAL BAN
24. 400935 TW VISA CHANG HIA COMMERCIAL BANK, LTD.
25. 400937 CN VISA CREDIT CORPORATE T&E BOC CREDIT CARD (INTERNAT
26. 400938 CN VISA CREDIT CORPORATE T&E BOC CREDIT CARD (INTERNAT
27. 400939 CN VISA CREDIT CORPORATE T BOC CREDIT CARD (INTERNAT
28. 400940 CN VISA CREDIT CORPORATE T BOC CREDIT CARD (INTERNAT
29. 400941 CN VISA CREDIT CLASSIC BOC CREDIT CARD (INTERNATIONAL),
30. 400942 CN VISA CREDIT PREMIER BOC CREDIT CARD (INTERNATIONAL),
31. 400996 TW VISA MEGA INTERNATIONAL COMMERCIAL BANK
32. 402330 TW VISA CREDIT PLATINUM CATHAY UNITED BANK
33. 402325 CN VISA CHINA UNIONPAY CO., LTD.
34. 402334 TW VISA CREDIT CLASSIC AEON CREDIT CARD (TAIWAN) CO., LT
```



# If All Else Fails!



www.360.com

中文版 Global

登录 注册



电脑软件 手机软件 360商城 安全理赔 个人服务 企业服务 游戏 社区



搜一下

## 360儿童机器人

解决陪孩子的小问题 TA更擅长

999元

立即抢购

智能硬件

360直杀套装  
安全上网的“黄金组合”  
360“全部保护您的电脑安全”

360商城  
新潮前卫的智能硬件  
还可申请免费试用

免费试用  
免费试用智能硬件  
查看全方位试用报告

### 最新动态

更多>>



360云盘关于延长下载结束日期的公告  
自360云盘发布转型公告后，因大量用户集中下载，虽然我们及时进行了带宽调配，但仍有不少用户反映下载网速慢等问题。详情>>

- 周鸿祎：大数据将会是未来科技的灵魂
- 360分身大师获“最佳新人奖”各应用市场表现优异
- 360浏览器推出“春运抢票日历”让老百姓安心回家
- 360Q5 Plus获中国手机设计与应用创新最高天酷奖
- 小编推荐：如何将360云盘内容快速转移到其他云盘

### 快速下载

更多>>

- 安全卫士
- 手机卫士
- 安全浏览器
- 手机助手
- 杀毒
- 360商城
- 免费WiFi
- 云盘手机版

### 360安全软件

#### 360安全卫士

杀木马 防欺诈 免病毒 防钓鱼

下载 论坛

#### 360杀毒

全网防杀 超病毒库 轻巧快速

下载 论坛

### 360商城

## 有我的地方就是电影院

坚果智能家庭影院

价格给力



# Create A Submarine Not A Wall

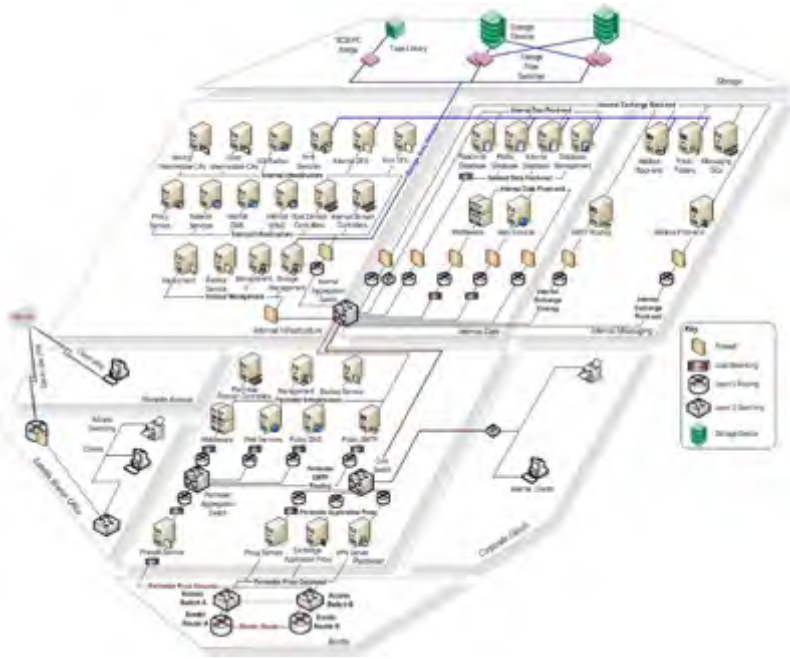


THIS.....

.....NOT THIS!

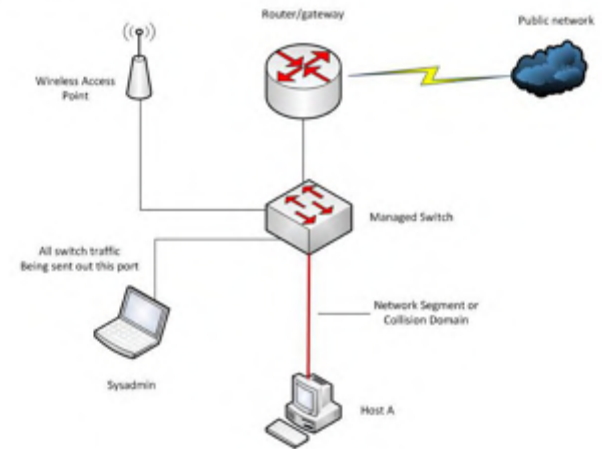


# Create A Submarine Not A Wall



THIS.....

Simple network diagram



.....NOT THIS!

# A Mubix Moment



WPAD

Make a null route (to 127.0.0.1 IPV4 ::1 IPV6) DNS entry for WPAD

Make a null route (to ::1 IPV6) DNS entry for WPADWPADWPAD

Disable NetBios resolution domain wide.



# A Mubix Moment



## Evil Canary

1. Create user called "DomainAdmin\_TMP"
2. Put password in the description.
3. Add to Domain Admins Group!
4. Under Logon Hours set to ZERO!!!
5. Set an alert ANY time that account tries to logon!

Published Certificates | Member Of | Password Replication | Dial-in | Object  
Security | Environment | Sessions  
Remote control | Remote Desktop Services Profile  
Personal Virtual Desktop | COM+ | UNIX Attributes | Attribute Editor  
General | Address | Account | Profile | Telephones | Organization

User logon name:  
DomainAdmin\_TMP

User logon name (pre-Windows 2000):

Logon Hours...

Unlock account

Account options:

- User must change password at next logon
- User cannot change password
- Password never expires
- Store password using reversible encryption

Account expires:

Never

End of: 12 September 2012

OK Cancel Apply Help

# A Mubix Moment

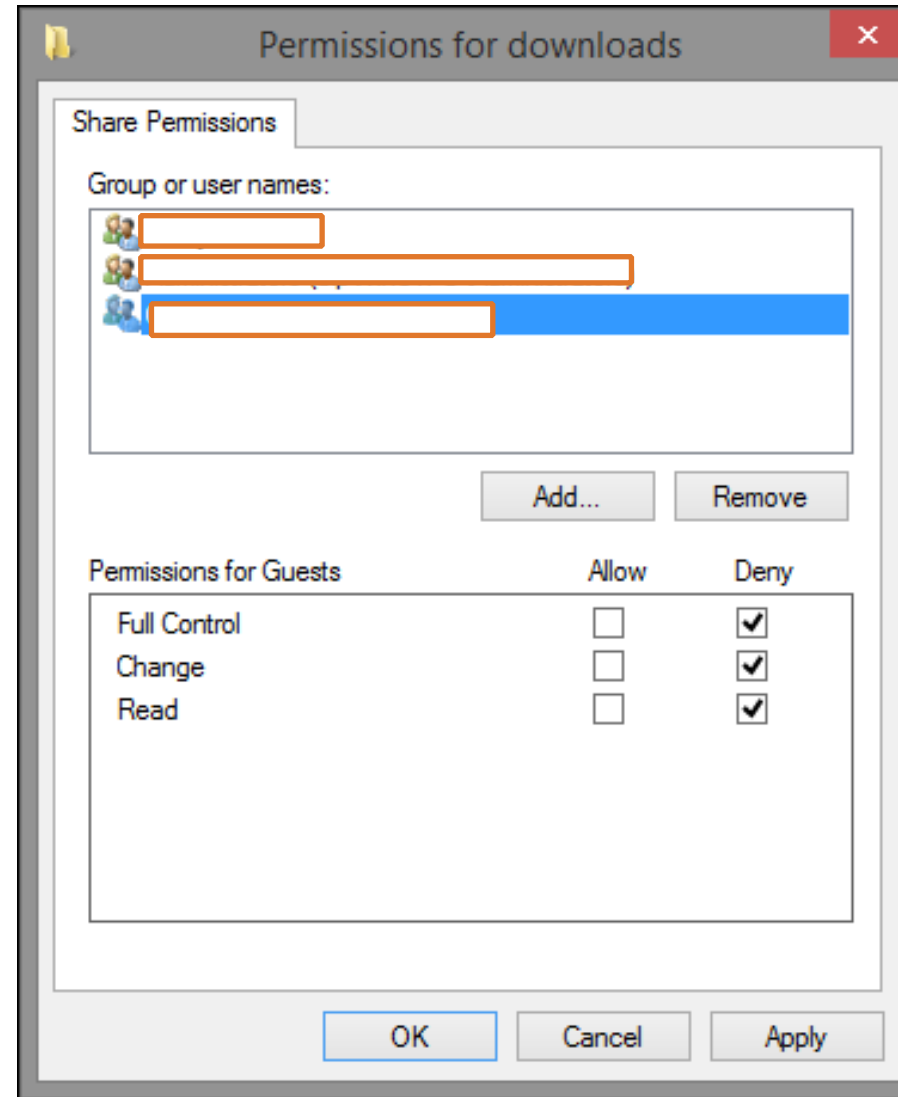


Evil Canary

Make a public share called

“Password Audit 2015” inside create  
a EXLS file about 4 MB but

“Everyone: Deny” permission.



# A Mubix Moment



Rob Fuller

Twitter @mubix

Blog – <http://www.room362.com>

Wiki – <http://pwnwiki.io>

Full video located here....

<https://www.youtube.com/watch?v=VqcDjPUXPIw>

# A Few Last Tricks & Traps



1. Code names on your who is contact information.
2. 1X1 pixel gif going to a link that alerts you.
3. User agent strings should also alert you.
4. Control the countries that can see you if you can.
5. Add triggers/false leads on your job listings.
6. Web Developers should be building good code!!!  
(Which it makes it more secure)



# Social Media Devices



HP  
Chromebook  
...  
**\$193.99**  
\$199.00  
Office Depot



Dell Latitude  
E6400 14.1" ...  
**\$139.99**  
PCLiquidatio...



Dell  
Chromeboo...  
**\$298.99**  
\$384.69  
Office Depot



Dell Latitude  
D830 15" Co...  
**\$174.99**  
PCLiquidatio...



Toshiba  
Toshiba CB3...  
**\$299.99**  
Toshiba



Asus EeeBook  
X205TA-DH...  
**\$207.55**  
Newegg.com



ASUS Laptop  
X551MAV-E...  
**\$269.99**  
Newegg.com



Android 4.2  
988 Netboo...  
**\$79.59**  
GearBest

# A Few Last Tricks & Traps



LAST but NOT Least!!!!

**Create teachable moments for your employees  
before a real attacker does!!!**

# A Few Last Tricks & Traps



The image displays multiple screenshots of the WiFi Pineapple management interface, showing various reports and data tables. The interface is titled "WiFi Pineapple - Management - kismet" and includes tabs for "Intelligence Report", "PassAP", "Karma", and "Karma Log".

The "Intelligence Report" tab is the primary focus, displaying a table of detected devices. The table columns are: IP Address, IP Address, hostname, and SSID. The data is as follows:

IP Address	IP Address	hostname	SSID
78.91.11.111	172.16.42.212	OPINION-000	Unknown
10.117.118.201	172.16.42.176		Mariposa
60.111.72.88.18.14	172.16.42.217	android-61276003004678	WiFiFi
80.140.80.70.14.11	172.16.42.180	android-65714791377767	WiFiFi
74.64.62.62.97.45	172.16.42.187	ADP	WiFiFi
80.140.80.70.14.11	172.16.42.176	android-61276003004678	Unknown
84.118.62.68.4.19	172.16.42.210	iPhone	WiFiFi
60.111.72.88.18.14	172.16.42.180	android-65714791377767	The 1624

Other screenshots show the "Karma" tab with a table of detected devices, the "PassAP" tab, and the "Karma Log" tab. The "Karma" tab table is as follows:

IP Address	IP Address	hostname	SSID
78.91.11.111	172.16.42.156	Lajpote/iPhone	WiFiFi
80.140.80.70.14.11	172.16.42.206	Robe-iPhone	WiFiFi
10.41.79.80.88.89	172.16.42.167	Lindsey	Unknown
80.140.80.70.14.11	172.16.42.157	Monica	Unknown
40.81.72.79.20.41	172.16.42.227	android-61181111	WiFiFi
79.118.90.30.19	172.16.42.240	robocorp1	WiFi-PUB-1
02.44.71.30.85.81	172.16.42.171	android-42075018360428	WiFiFi
78.91.11.111	172.16.42.207	WiFi-iPhone	WiFiFi
1.8.76.41.38.11.8	172.16.42.188	wifi-wifi/iPhone	Monica
80.140.80.70.14.11	172.16.42.175	Sacks-iPhone	Target-Suave Wi-Fi
90.118.71.45.18.41	172.16.42.190	android-178006871287962	Monica
80.140.80.70.14.11	172.16.42.244	iPhone	PassAP
71.22.49.53.45.86	172.16.42.233	android-6c81181111	WiFiFi
172.16.79.42.58.28	172.16.42.186	android-64261208878679	Old-Suave
80.25.88.80.70.12	172.16.42.255	WiFi-iPhone	Target-Suave Wi-Fi
70.48.42.70.12.80	172.16.42.162	Shaw-Wi-iPhone	Greenbud-IPUB-1
80.140.80.70.14.11	172.16.42.103	android-40276003004678	Monica
44.80.84.50.110.82	172.16.42.186	WiFi-iPhone 2	PassAP
10.20.48.07.90.30	172.16.42.242	WiFi-iPhone 2	Target-Suave Wi-Fi
18.75.41.81.80.47	172.16.42.179	Suring	WiFiFi
80.140.80.70.14.11	172.16.42.179	android-61276003004678	Robe-iPhone

# A Few Last Tricks & Traps



WiFi Pineapple Dashboard Statistics:

- UPTIME: 0 hours, 7 minutes
- CLIENTS CONNECTED: 42
- SSIDS IN POOL: 283
- 92% CPU USAGE
- 236 SSIDS ADDED THIS SESSION

WiFi Pineapple Clients Page:

MAC Address | IP Address | SSID | Hostname | Kick Client

MAC Address	IP Address	SSID	Hostname	Kick Client
0c3e9854e111	172.16.42.223	WLAN	Angela's-Phone	Kick
d4948fbd8066	172.16.42.162	United_Wi-Fi	David's-Phone	Kick
68dbca7cc0e68	172.16.42.138	JSACONFERENCE	D'AmenasPhone6	Kick
006171cc4132	172.16.42.209	United_Wi-Fi	iPhone	Kick
48437ceb3590	172.16.42.236	pdwRf	No Hostname	Kick
e6508b649e90	172.16.42.246	dlink	android-23947d12d5c181f	Kick
d0a63794910d	No IP	United_Wi-Fi	No Hostname	Kick
9131c31d295f	172.16.42.179	Bolingo Hotspot	TatsuKasiPhone2	Kick
5871572e0e17	172.16.42.247	PANERA	ArthursPhone2	Kick
d0335e1ef051	No IP	OuterNET	No Hostname	Kick
6418e172805f	No IP	Bolingo Hotspot	No Hostname	Kick
4c0bbe213b54	No IP	HotelLobby	No Hostname	Kick
24da9b070eef	No IP	JSACONFERENCE	No Hostname	Kick
4c348889809d	172.16.42.167	mckorporate	ASGG543003M	Kick
265aeb484b61	172.16.42.121	AWG-WiFi	No Hostname	Kick
80be06e1208c	No IP	van der Valk	No Hostname	Kick
e0b526dfe1d3	172.16.42.225	Admins_Club	Retse-Fort	Kick
50cc8bba911e	No IP	JSACONFERENCE	No Hostname	Kick

# Remember your employees are your asset not a liability!!



## Observant employee foils robbery attempt at Hampton bank

HOSTED WITH THE EMBROIDERY 2 SHOP BY [eScrips](#) | [Twitter](#) | [Facebook](#) | [LinkedIn](#) | [Google+](#)

### Man arrested after bank employee foils robbery

[Daily News](#) | [@nydailynews](#) | [www.nydailynews.com](#) | [www.dailymail.com](#) | [www.fox.com](#)



Frankle police say, a bank employee's quick actions foiled a robbery attempt that led to one man's arrest.

Rocky Vance, 35, of Franklin is charged with aggravated robbery and is being held on a \$100,000 bond, said Frankle police in a media release.

On Thursday, a Pittsfield bank employee rushed to lock the door at the 2040 Providence Parkway location as a man wearing a heavy coat, carrying a backpack and pulling a duffel bag over his face, walked toward the patron side.



Video: Wanderlust



By [Ron Zeitlinger](#) | [The Jersey Journal](#)

[Follow on Twitter](#)

on August 16, 2016 at 12:55 PM, updated August 16, 2016 at 1:03 PM

[Print](#)

[Email](#)

A quick-thinking 7-Eleven employee thwarted a robbery early this morning by locking himself in a back office when the thief demanded cash, Jersey City police said.

## Alert Panera employee foils ID theft ring in MT

Gang suspected of bilking restaurant patrons in several states.

BERNARD HARRIS Staff | Apr 8, 2008 | [0](#)

[f](#) [t](#) [e](#) [i](#)

A group of theft suspects who are believed to have been stealing credit cards from restaurant patrons in several states was caught leaving the Panera Bread cafe in Manheim Township Monday night.

Two women and one man were arrested. A second man fled the shopping center parking lot and abandoned his car nearby, Manheim Township police reported.

## Peoria pharmacy employee foils robbery attempt

Posted: Jun 17, 2014 6:51 PM CDT

Updated: Jul 01, 2014 6:51 PM CDT

By [Phil Benson](#) | [CONNECT](#)

PEORIA, AZ (CBS5) - Peoria police are trying to track down a man who attempted to rob narcotic pills from a grocery store pharmacy.



# Now let' s learn from others

Discussion and Questions????

Or several minutes of uncomfortable silence it' s your choice.



This concludes my presentation Thank You



# LINKS as you LEAVE

<http://pwnieexpress.com/jaysonstreet>

WeChat jaysonstreet

Twitter @jaysonstreet

# Company Info



**pwn** (pōn) **v. pwned** - tr. Slang. **1.** To own in the sense of defeat: *Don't get pwned by network hackers.* **2.** To beat someone or something by a wide margin, usually in relation to a game.

## Security Assessment for Remote Sites & Wireless

- Closes huge gap in security infrastructure
- Founded 2010
- Boston HQ & Vermont Research Lab
- Financing: \$5.1 million Series A (July 2013)
- Over 1000 accounts globally, 600 Enterprises, & Partner Channel
- Recognition and Awards

Forbes

NETWORKWORLD

engadget

WIRED

FOX & friends

PCWorld

