INTSIGHTS
Defend Forward™

Turning the Tables: Putting Threat Intel to Work Against Attackers

Etay Maor, Chief Security Officer

Hi

- Chief security officer, Intsights
  - IBM Executive security advisor
  - RSA Head of cyberthreats research lab
- Adj Prof at Boston College
- Started my career in high school… not in a good way

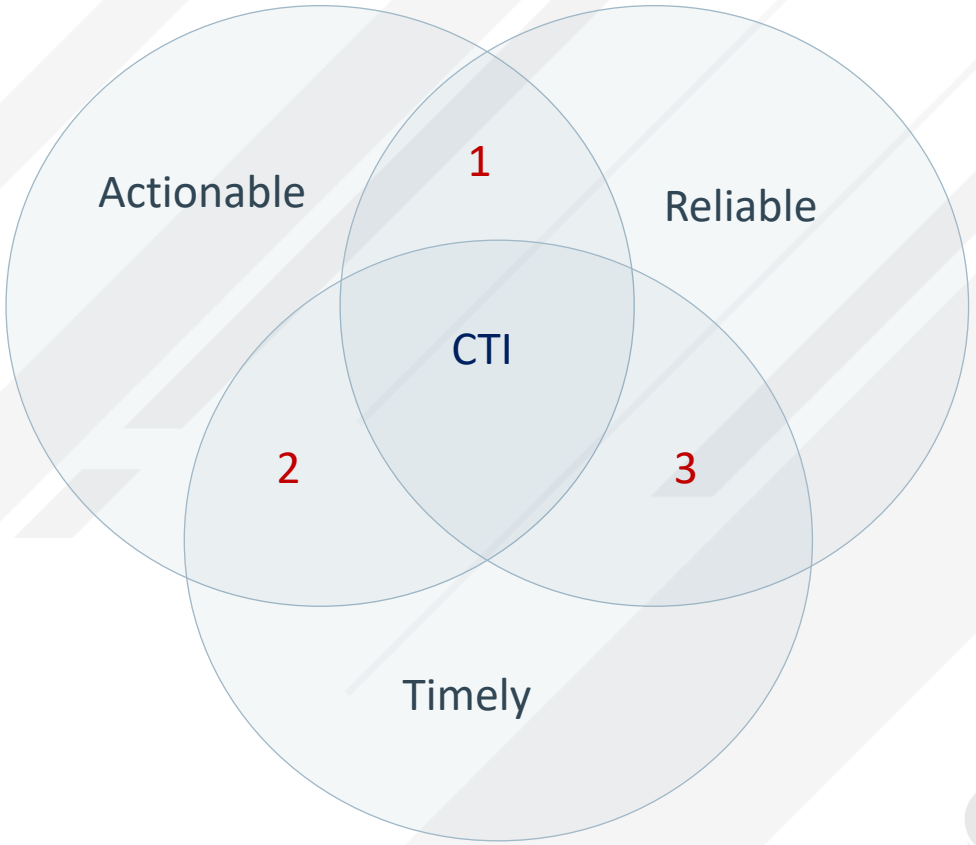
CTI is an ART

1 - Not Timely? Old news, attack already happened.

2 – Not Reliable? Fake news, false positives are coming.

3 – Not Actionable? Just a feed, data overload.

Holistic & Tailored



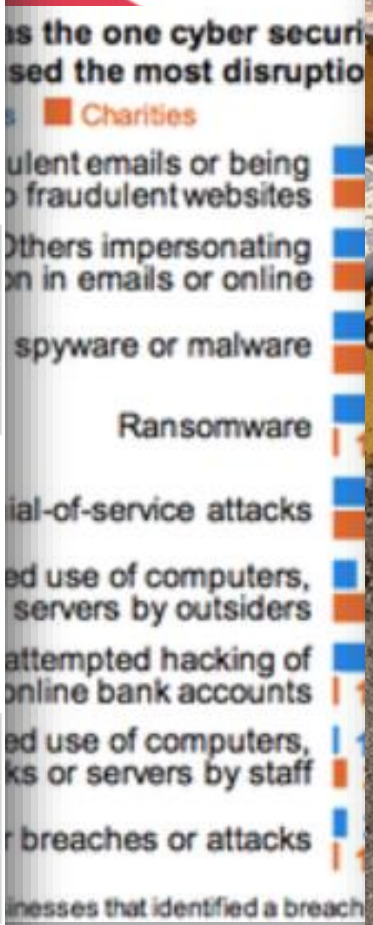
Who Is Targeted More These Days?

- People
- Processes
- Technology

The Two Reasons For Every Breach

Initial Access
9 techniques

- Drive-by Compromise
- Exploit Public-Facing Application
- External Remote Services
- Hardware Additions
- Phishing (0/3)
  - Spearphishing Attachment
  - Spearphishing Link
  - Spearphishing via Service
- Replication Through Removable Media
- Supply Chain Compromise (0/3)
- Trusted Relationship
- Valid Accounts (0/3)
  - Default Accounts
  - Domain Accounts
  - Local Accounts



OSINT is EASY

Simple OSINT

BOSTON COLLEGE

Researching Target Affiliates

- According to the website, [redacted] partners with 2 institutions to [redacted] and to do research on Advancing state of the art discoveries:
    - Karolinska Institutet and Karolinska University Hospital – Advancing state of the art discoveries with mRNA Therapeutics™ to treat serious diseases
    - Institut Pasteur – For the discovery and development of drugs and vaccines for infectious diseases using the mRNA Therapeutics™ platform

Biopharma | Government | Foundations | Research Institutes

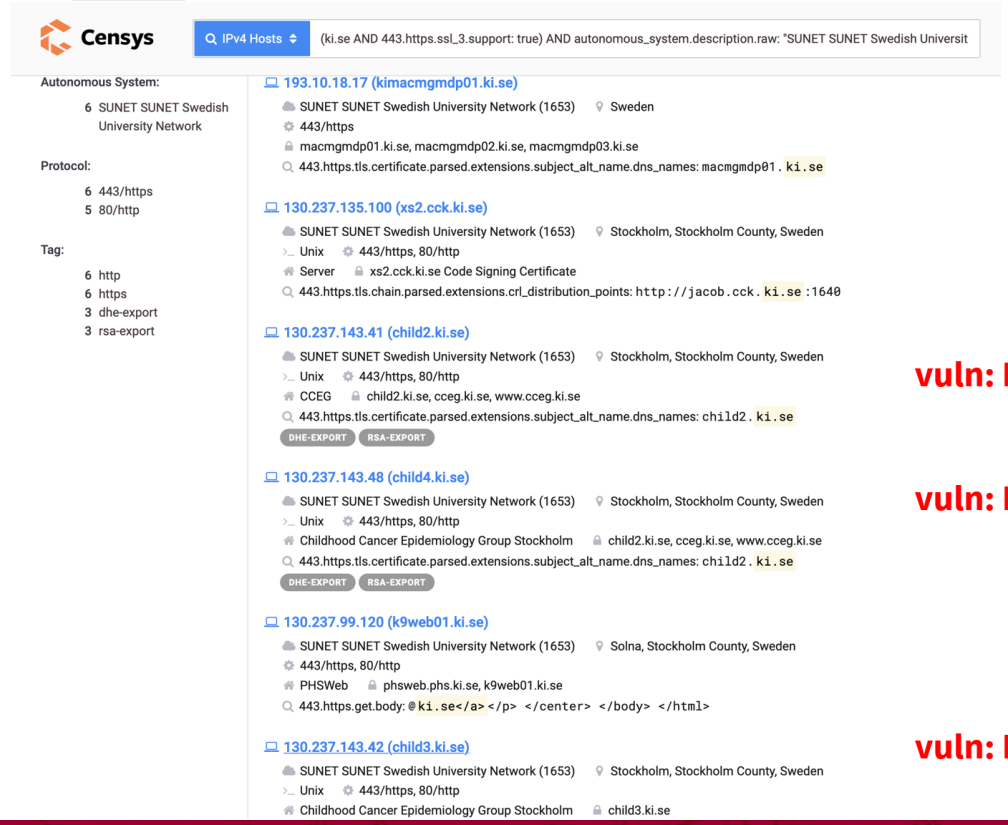
Karolinska Institutet

KAROLINSKA Universitetssjukhuset

Institut Pasteur

Simple OSINT

Some Karolinska servers are vulnerable...



vuln: Poodle

vuln: Poodle

vuln: Poodle, Logjam, FREAK

vuln: Poodle, Logjam, FREAK

vuln: Poodle

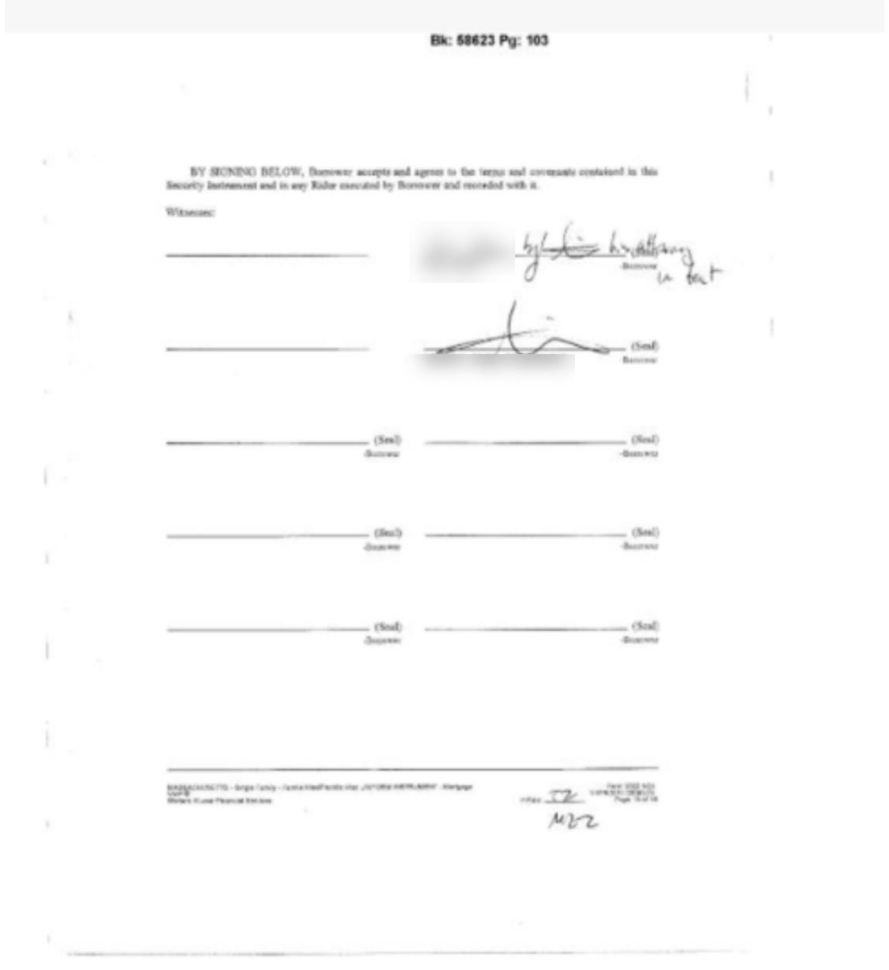
vuln: Poodle, Logjam, FREAK

Simple OSINT

Potential Targets

Simple OSINT

Open Source Investigations



Bk: 58623 Pg: 103

BY SIGNING BELOW, Borrower accepts and agrees to the terms and covenants contained in this Security Instrument and in any Rider executed by Borrower and recorded with it.

Witnesses:

(Seal) Borrower

(Seal) Borrower

(Seal) Borrower (Seal) Borrower

(Seal) Borrower (Seal) Borrower

(Seal) Borrower (Seal) Borrower

MBB

Bk: 58623 Pg: 88

Executed as a **SEALED** instrument, UNDER THE PAINS AND PENALTIES OF PERJURY, this 28 day of February, 2012.

COMMONWEALTH OF MASSACHUSETTS

Norfolk, ss February 28, 2012

On this 28 day of February, 2012, before me, the undersigned notary public, personally appeared [redacted] proved to me through satisfactory evidence of identification, which were _____ to be the person whose name is signed on the preceding or attached document, and acknowledged to me that he/she signed it voluntarily for its stated purpose.

(official signature and seal of notary)

My Commission Expires: 10/2/17

Simple OSINT

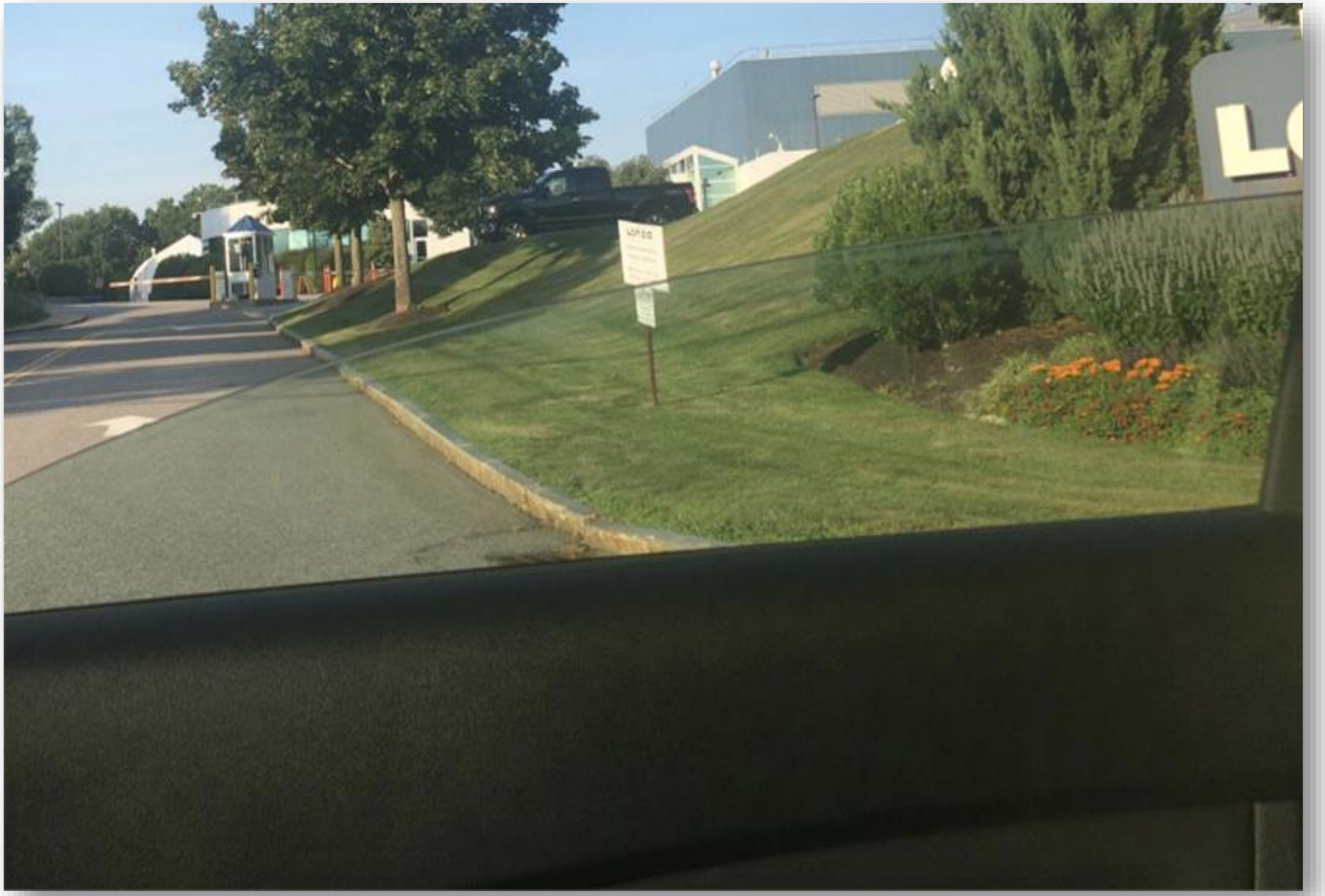
[redacted] (Detailed)

- Has a favorite hobby that is baking gingerbread houses
- She bakes a massive gingerbread house for [redacted]
- She starts shopping and preparing this house in mid to late October
- She shops at two stores every year
  - [redacted] in Marlborough
  - [redacted] in Kittery
- Emails:
  - [redacted]@aol.com
  - [redacted]@comcast.net

[redacted] Hospital

Simple OSINT

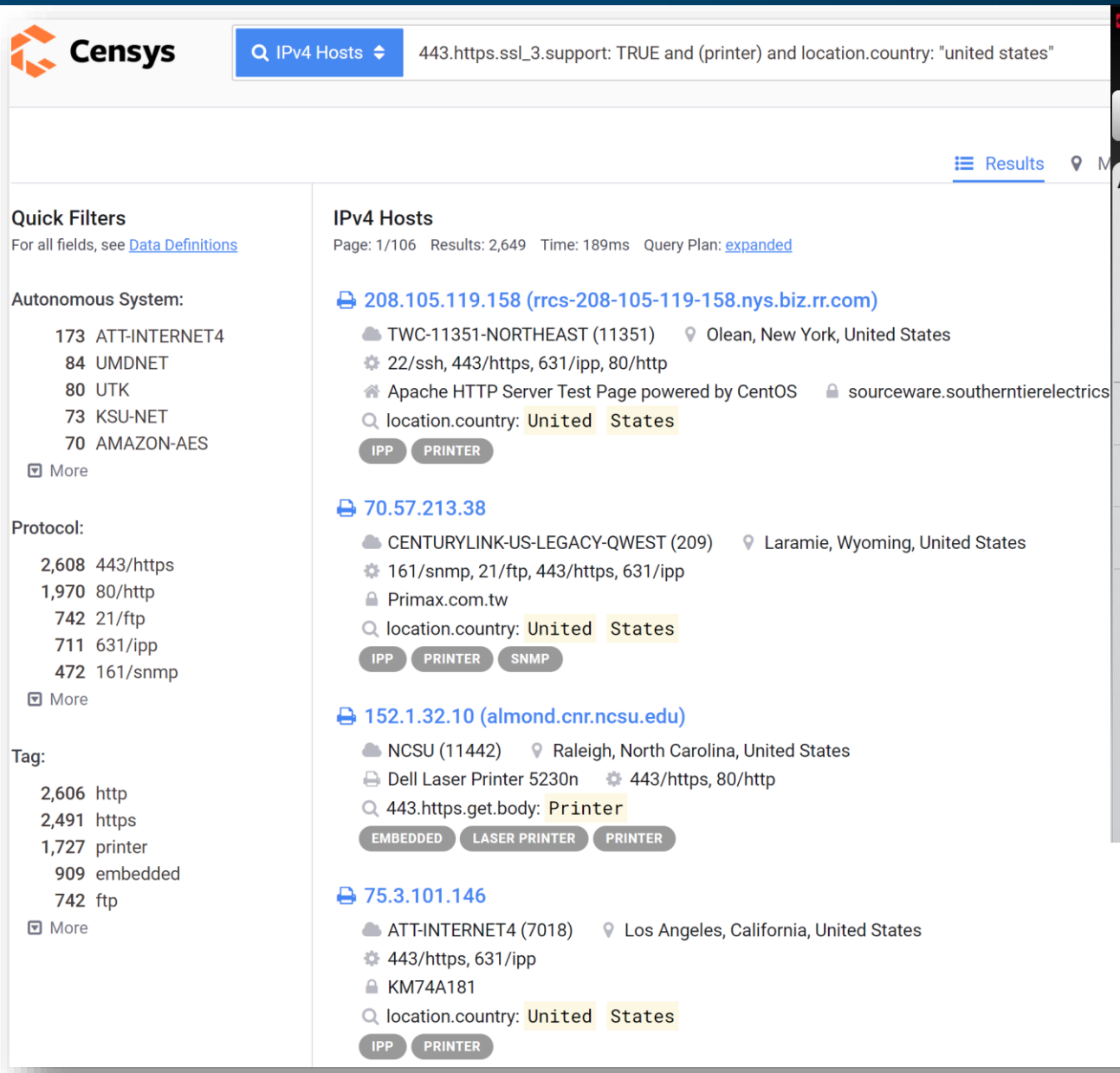
Simple OSINT

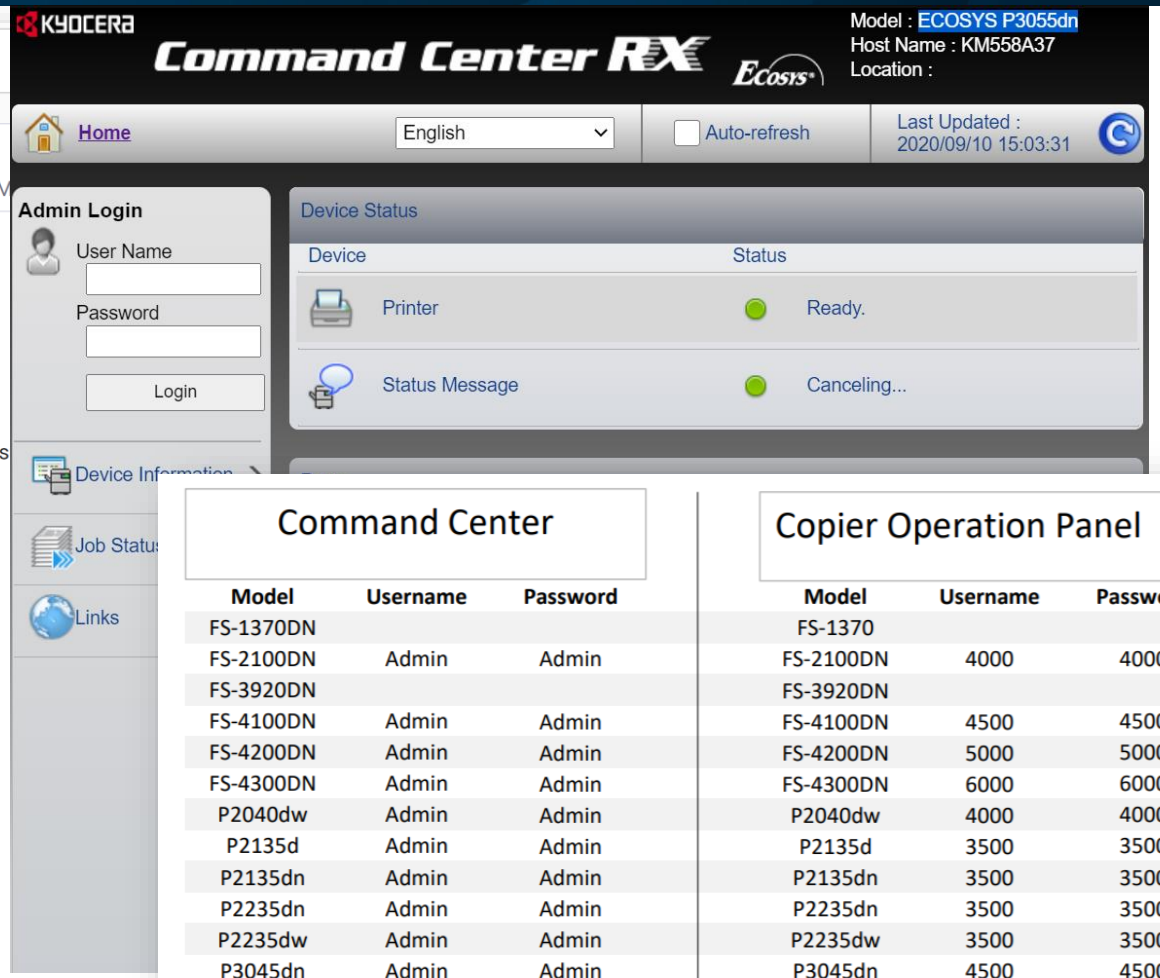


“Home” Office

Router Brand	Login IP	Username	Password
3Com	http://192.168.1.1	admin	admin
Belkin	http://192.168.2.1	admin	admin
BenQ	http://192.168.1.1	admin	admin
D-Link	http://192.168.0.1	admin	admin
Digicom	http://192.168.1.254	admin	michelangelo
Digicom	http://192.168.1.254	user	password
Linksys	http://192.168.1.1	admin	admin
Netgear	http://192.168.0.1	admin	password
Sitecom	http://192.168.0.1	sitecom	admin
Thomson	http://192.168.1.254	user	user
US Robotics	http://192.168.1.1	admin	admin

“Home” Office





Command Center

Model	Username	Password
FS-1370DN		
FS-2100DN	Admin	Admin
FS-3920DN		
FS-4100DN	Admin	Admin
FS-4200DN	Admin	Admin
FS-4300DN	Admin	Admin
P2040dw	Admin	Admin
P2135d	Admin	Admin
P2135dn	Admin	Admin
P2235dn	Admin	Admin
P2235dw	Admin	Admin
P3045dn	Admin	Admin
P3050dn	Admin	Admin
P3055dn	Admin	Admin
P3060dn	Admin	Admin
FS-9530dn		
FS-1028MFP		admin00
FS-1030MFP		admin00
FS-1035MFP		admin00

Copier Operation Panel

Model	Username	Password
FS-1370		
FS-2100DN	4000	4000
FS-3920DN		
FS-4100DN	4500	4500
FS-4200DN	5000	5000
FS-4300DN	6000	6000
P2040dw	4000	4000
P2135d	3500	3500
P2135dn	3500	3500
P2235dn	3500	3500
P2235dw	3500	3500
P3045dn	4500	4500
P3050dn	5000	5000
P3055dn	5500	5500
P3060dn	6000	6000
FS-9530dn		
FS-1028MFP	2800	2800
FS-1030MFP	3000	3000
FS-1035MFP	3500	3500

Oversharing On GITHUB

Uber data breach from 2016 affected 57 million riders and drivers

Darrell Etherington @etherington / 5:20 pm EST • November 21, 2017 Comment

The report says the attack occurred because attackers managed to gain login credentials for an Uber Amazon Web Services account using a private GitHub site maintained by Uber engineers.

BBC Sign in | News | Sport | Reel | Worklife | Travel | Future | M

NEWS

Home | Video | World | US & Canada | UK | Business | Tech | Science | Stories | Entert

Technology

Chinese hotel group investigates possible leak of millions of guests' data

29 August 2018 Share

Scotiabank source code, credentials found open on GitHub: news report

Howard Solomon @howarditwc
Published: September 19th, 2019

Oversharing On GITHUB

CapitalOne

Responsible Disclosure (Shared) <responsibledisclosure@capitalone.com>

[External Sender] Leaked s3 data

[redacted]

Wed, Jul 17, 2019 at 1:25 AM

To: "responsibledisclosure@capitalone.com" <responsibledisclosure@capitalone.com>

Hello there,

There appears to be some leaked s3 data of yours in someone's github / gist:

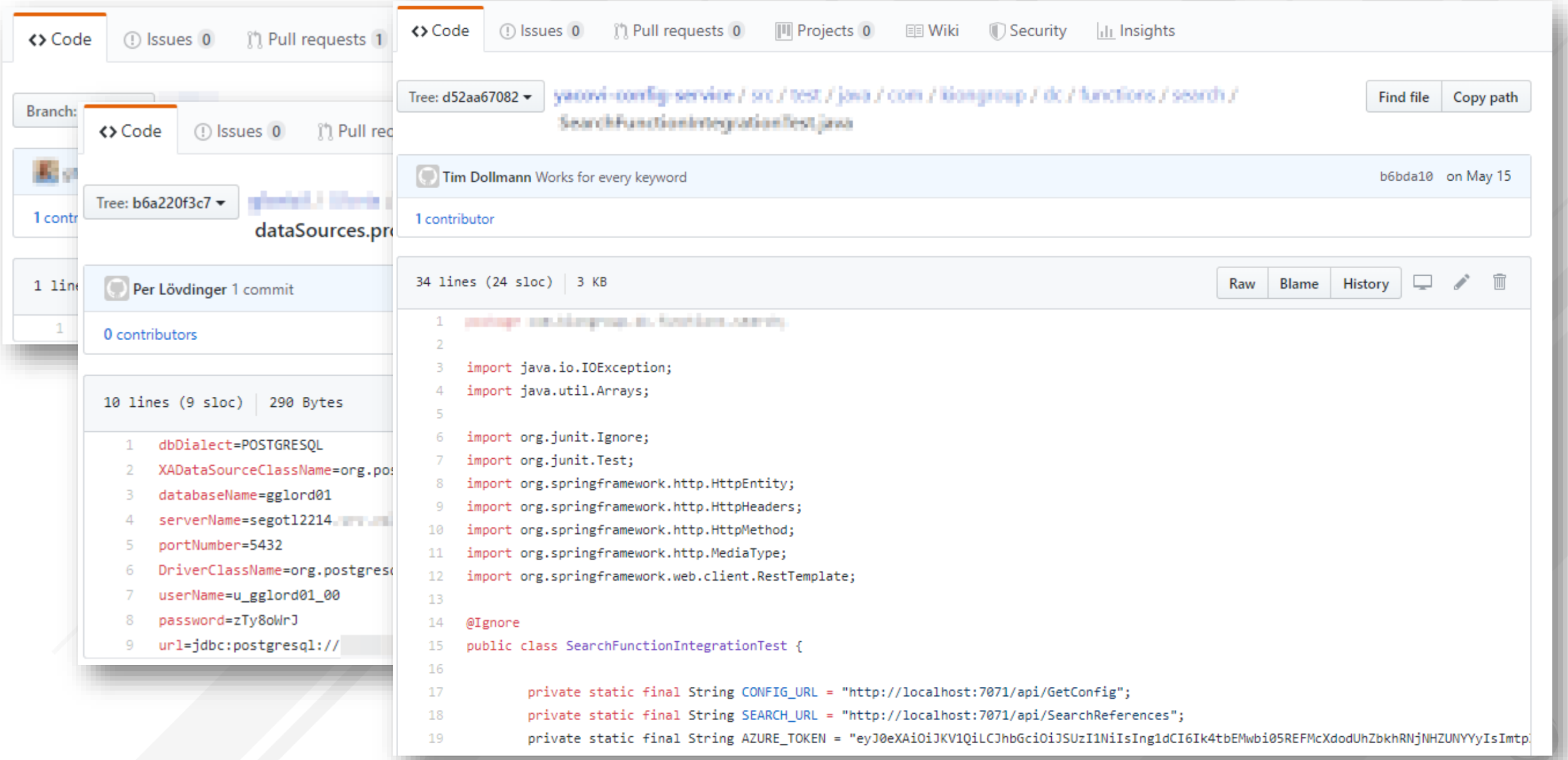
https://gist.github.com[redacted]

Let me know if you want help tracking them down.

Thanks,

[redacted]

Or Just Search GitHub...



INTSIGHTS
Defend Forward™

For Sale

Domain Admins

SlayerFrom_K
килобайт
●●

JS

Платная регистрация
1
29 публикаций
Регистрация
05.07.2019 (ID: 94 114)
Деятельность
хакинг / hacking

Опубликовано: В среду в 13:01

Предлагаю доступ в корпоративную сеть компании, один из лидеров мировой судостроительной промышленности.
Revenue - 12.5 billion $
Сотрудников ~ 33 000
Доступ :
1) domain admins
2) 50 000 уникальных пар логин/пароль к учетным записям сотрудников в доменах
3) ~ 20 000 корпоративных ящиков

Наше предложение - 15 btc
Работаем только через гаранта данного форума
Связь в ЛС форума, далее в jabber

+ Цитата

smogger
байт
●

S

Платная регистрация
0
1 публикация
Регистрация
07.08.2020
(ID: 107 151)
Деятельность
хакинг / hacking

Опубликовано: 3 минуты назад

Access Type: Domain Admin
Industry: Cyber Security, Homeland Security, SCADA Services
Location:Israel
Price: $3200
Host in the network : 300+

+ Цитата

RCE Vul, RDP/VNC

RCE at *** Bank

Автор: Ferb, 6 сентября в [Доступы] - FTP, shell'ы, руты, sql-inj, БД, дедики

Подписаться 1

Создать тему | Ответить в тему

Ferb
байт

Платная регистрация
0
3 публикации
Регистрация
24.08.2020
(ID: 107 681)
Деятельность
хакинг / hacking

Опубликовано: 6 сентября (изменено)

Жалоба

Price: $10,000 USD (UNITED, STATES, DOLLAR)
I am selling a vulnerability that allows ***RCE, you can get a reverse shell at the bank***.
You can contact me via XMPP[1] or e-mail[2].
Be direct in negotiation.

This bank is very good for you to hack, steal and in the end earn good money. I recommend that you read this Phineas Fisher guide[3]
Come talk to me and I will show you the proof of this vulnerability.

Come talk to me and I will share details like(bank name) and show you the proof of this vulnerability.
[1] ghostfalcon@jabbim.ru
[2] jestersnc@protonmail.com
[3] https://dl.packetstormsecurity.net/papers/attack/hackback-bankrobbing.txt

Изменено 6 сентября пользователем Ferb

\+ Цитата

Z

Продажа брут RDP/VNC

Автор: zone, 19 июня в [Доступы] - FTP, shell'ы, руты, sql-inj, БД, дедики

Подписаться 1

Создать тему | Ответить в тему

zone
байт

Z

Платная регистрация
0
6 публикаций
Регистрация
06.04.2020
(ID: 102 372)
Деятельность
хакинг / hacking

Опубликовано: 19 июня

Жалоба

В наличии брученные внц и рдп
По локациям юса и европа
рдп от 10$
vnc от 20$

Оплата в бтс

Jabber: stopware@jabber.ru

\+ Цитата

Bank Accounts

Sell 20 400 BA US

Author: GREAT , Sunday at 15:54in Auctions

GREAT
gigabyte

Seller
7
156 posts
Registration
17.04.2019 (ID: 92 204)
Activities
other / other

Posted: Sunday at 15:54

Selling 20,400 lines of US Bank Account

Format:
ROUTING NUMBER, ACCOUNT NUMB

Start: $ 10,000
Step: $ 5,000
Blitz: $ 20,000

Quote

Корзина

Accounts

CardShop › Accounts

Update Support: Chat us directly from shop contact support:

USA Info User+Pass + AN/RN | USA Bank Info User+Pass + AN/RN +Name | User+Pass/random balance | USA Fullz Info | USA Email Access Logs
PayPal Info | Bill pay Logs | Australia Bank | Spamming Tools | USA DL | Canada Bank Logs | Direct Deposit Logs | Germany Bank
Credit Card Section.

NEW UPDATE

2020-08-10
Added to TD bank AN/RN + Name 24 accounts

2020-08-09
Added to Chase User+Pass + AN/RN 4 accounts
Added to Asbhwawaii AN/RN 8 accounts
Added to Citi Bank 1 accounts

2020-08-08
Added to PayPal Info 22 accounts

2020-08-07
Added to Asbhwawaii AN/RN 10 accounts

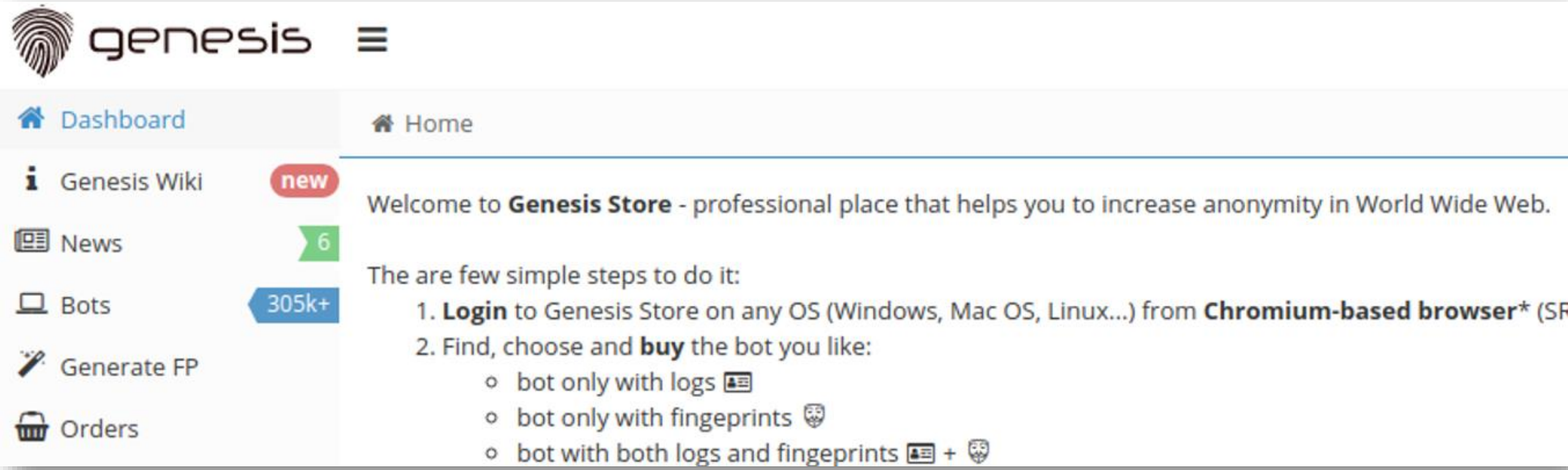
2020-08-05
Added to fairwindsCU Email Access 3 accounts
Added to Vystar AN/RN 8 accounts

2020-08-04
Added to TD bank AN/RN + Name 1 accounts
Added to Chase User+Pass + AN/RN 4 accounts
Added to TD Canada Logs AN/RN + Name 2 accounts

Список товаров

Баланс	Название	Цена $	
23130	Balance = 23130.3	70.00	Купить
4251	Balance = 4251.77	30.00	Купить
93125	Balance = 93125.63	90.00	Купить
54	Balance = 54.26	10.00	Купить
4025	|Balance = 4025.48|	30.00	Купить
3359	Balance = 3359.16	25.00	Купить
23714	Balance = 23714.96	60.00	Купить
50991	Balance = 50991.38	100.00	Купить
25847	Balance = 25847.3	50.00	Купить
5128	Balance = 5128.88	30.00	Купить
14234	Balance = 14234.74	70.00	

Identity Markets Booming



INTSIGHTS
Defend Forward™

Social Engineering

Meet Robin Sage

Home Profile Connections Jobs Interests Search…

Robin Sage

Cyber Threats Analyst at the
Naval Network Warfare Command

Norfolk, CT | Cyber Threats Analyst

Current	Naval Network Warfare Command
Age	25 years old
Education	Massachusetts Institute of Technology

Connect Send InMail

300+
connections

IRL

ANDY GREENBERG 07.27.17 10:00 AM

MEET MIA ASH, THE FAKE WOMAN IRANIAN HACKERS USED TO LURE VICTIMS

SECUREWORKS

MIA ASH IS a 30-year-old British woman with two art school degrees, a successful career as a photographer, and plenty of friends—more than 500 on Facebook, and just as many on

ET CISO.in
From The Economic Times

News | Whitepapers | CISO Mind Speak | CISO Wall | Interviews | CISO TV | Brand Solutions

Vulnerabilities • Mobility Threats • ETCISO Annual Summit 2020 • Email Security • Cyberwarfare • Digital Se

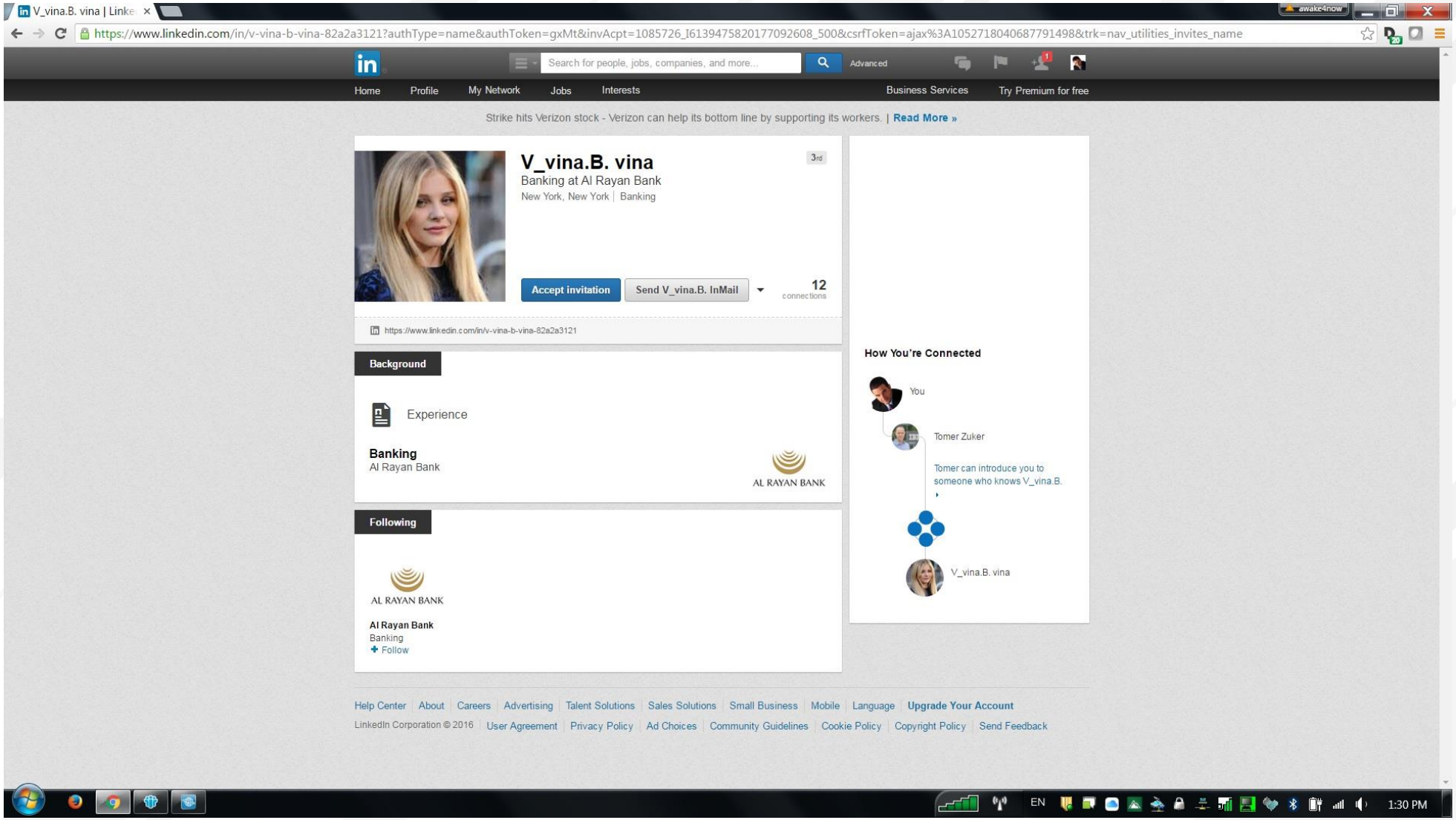
IT Security News / Latest IT Security News / Vulnerabilities

Cyber spies use LinkedIn to hack European defence firms: Report

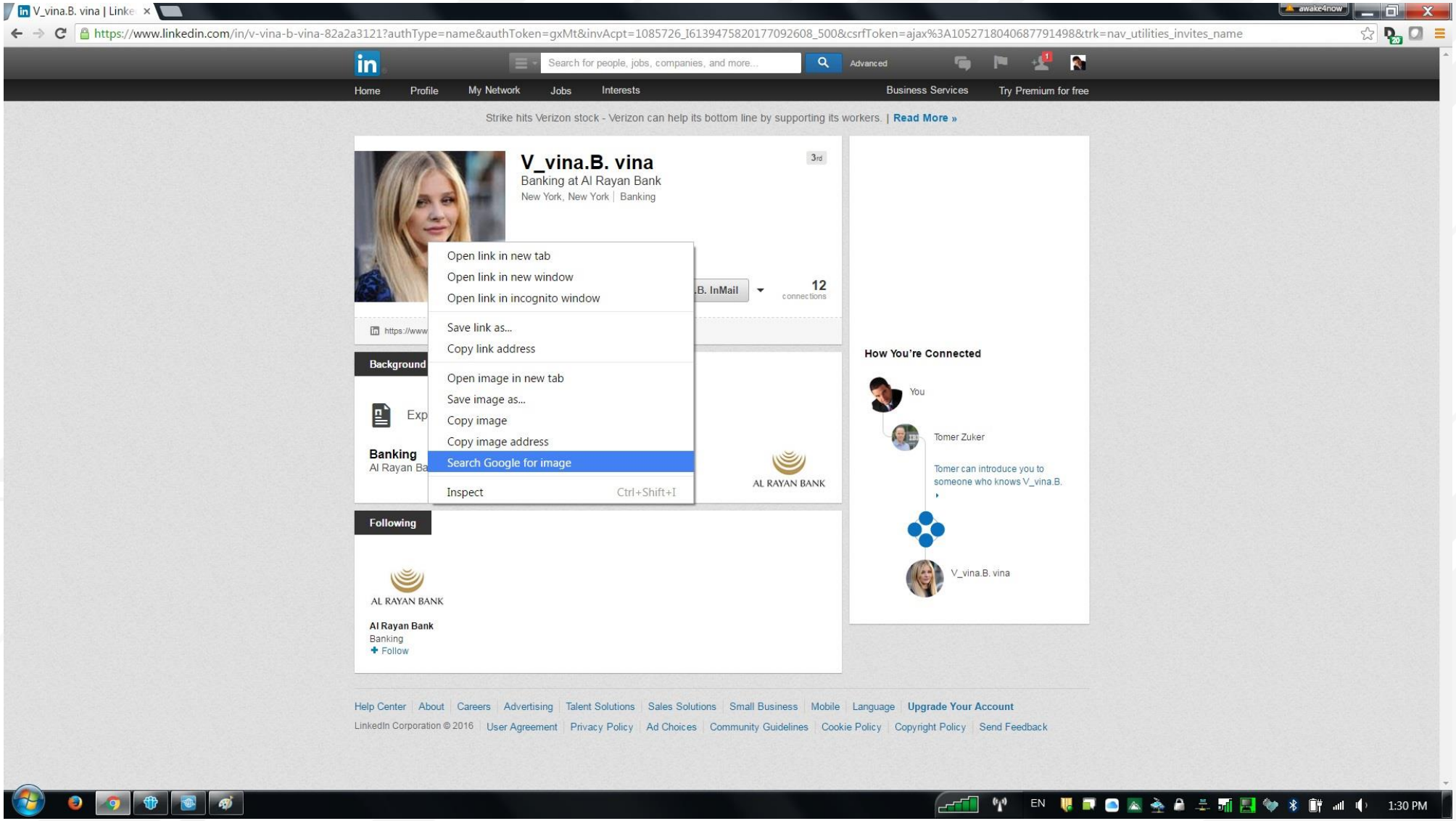
sThe attackers used LinkedIn's private messaging feature to send documents containing malicious code which the employees were tricked into opening, said Jean-Ian Boutin, ESET's head of threat research.

Reuters • June 18, 2020, 11:07 IST

My LinkedIn


V_vina.B. vina | Linke
https://www.linkedin.com/in/v-vina-b-vina-82a2a3121?authType=name&authToken=gxMt&invAcpt=1085726_I6139475820177092608_500&csrfToken=ajax%3A1052718040687791498&trk=nav_utilities_invites_name
Search for people, jobs, companies, and more...
Advanced
Home
Profile
My Network
Jobs
Interests
Business Services
Try Premium for free
Strike hits Verizon stock - Verizon can help its bottom line by supporting its workers. | Read More »
V_vina.B. vina
3rd
Banking at Al Rayan Bank
New York, New York | Banking
Accept invitation
Send V_vina.B. InMail
12
connections
https://www.linkedin.com/in/v-vina-b-vina-82a2a3121
Background
Experience
Banking
Al Rayan Bank
AL RAYAN BANK
Following
AL RAYAN BANK
Al Rayan Bank
Banking
+ Follow
How You're Connected
You
Tomer Zuker
Tomer can introduce you to someone who knows V_vina.B.
V_vina.B. vina
Help Center | About | Careers | Advertising | Talent Solutions | Sales Solutions | Small Business | Mobile | Language | Upgrade Your Account
LinkedIn Corporation © 2016 | User Agreement | Privacy Policy | Ad Choices | Community Guidelines | Cookie Policy | Copyright Policy | Send Feedback
EN
1:30 PM

My LinkedIn


V_vina.B. vina | Linke
https://www.linkedin.com/in/v-vina-b-vina-82a2a3121?authType=name&authToken=gxMt&invAcpt=1085726_I6139475820177092608_500&csrfToken=ajax%3A1052718040687791498&trk=nav_utilities_invites_name
Search for people, jobs, companies, and more...
Advanced
Home
Profile
My Network
Jobs
Interests
Business Services
Try Premium for free
Strike hits Verizon stock - Verizon can help its bottom line by supporting its workers. | Read More »
V_vina.B. vina
Banking at Al Rayan Bank
New York, New York | Banking
3rd
Open link in new tab
Open link in new window
Open link in incognito window
Save link as...
Copy link address
Open image in new tab
Save image as...
Copy image
Copy image address
Search Google for image
Inspect
Ctrl+Shift+I
.B. InMail
12
connections
Background
Banking
AL RAYAN BANK
Following
AL RAYAN BANK
Al Rayan Bank
Banking
+ Follow
How You're Connected
You
Tomer Zuker
Tomer can introduce you to someone who knows V_vina.B.
V_vina.B. vina
Help Center | About | Careers | Advertising | Talent Solutions | Sales Solutions | Small Business | Mobile | Language | Upgrade Your Account
LinkedIn Corporation © 2016 | User Agreement | Privacy Policy | Ad Choices | Community Guidelines | Cookie Policy | Copyright Policy | Send Feedback
EN
1:30 PM

My LinkedIn

V_vina.B. vina | Linke | Chloe Grace Moretz

deadline.com/2014/07/tale-of-the-princess-kaguya-chloe-grace-moretz-release-date-804430/

DEADLINE | HOLLYWOOD FILM 'Tale Of The Princess Kaguya' Sets English-Language Voice ...

Of Tomorrow' Regulars Exit | Week's Top Trends & More | Brothers Dream Big | The High Castle' Top Spot

'Tale Of The Princess Kaguya' Sets English-Language Voice Cast, October Release Date

by The Deadline Team
July 15, 2014 9:07am

- FILM
- NEWS
- CHLOE GRACE MORETZ
- GKIDS
- THE TALE OF THE PRINCESS KAGUYA

What's Hot on Deadline

1. 'The Blacklist' Creator On Finale's Shocking Twists, the Fallout &...
2. 'DC's Legends Of Tomorrow': Ciara Renée To Depart
3. 'Nashville': #BringBackNashville Movement Is Growing
4. 'The Man In The High Castle' Showrunner Frank Spotnitz Exits...
5. 'Neighbors 2' Parties Harder Than 'Angry Birds' & 'Nice Guys' In...
6. 'The Blacklist' Finale Surprise: Look Who's Back!
7. 'DC's Legends Of Tomorrow': Wentworth Miller Exits As Regular...
8. Sara Ramirez Exits 'Grey's Anatomy' After 10 Seasons
9. Netflix's 'Gilmore Girls' Revival Gets Official Title
10. 'Personal Shopper' Director Olivier Assayas On The Wonders Of Working...

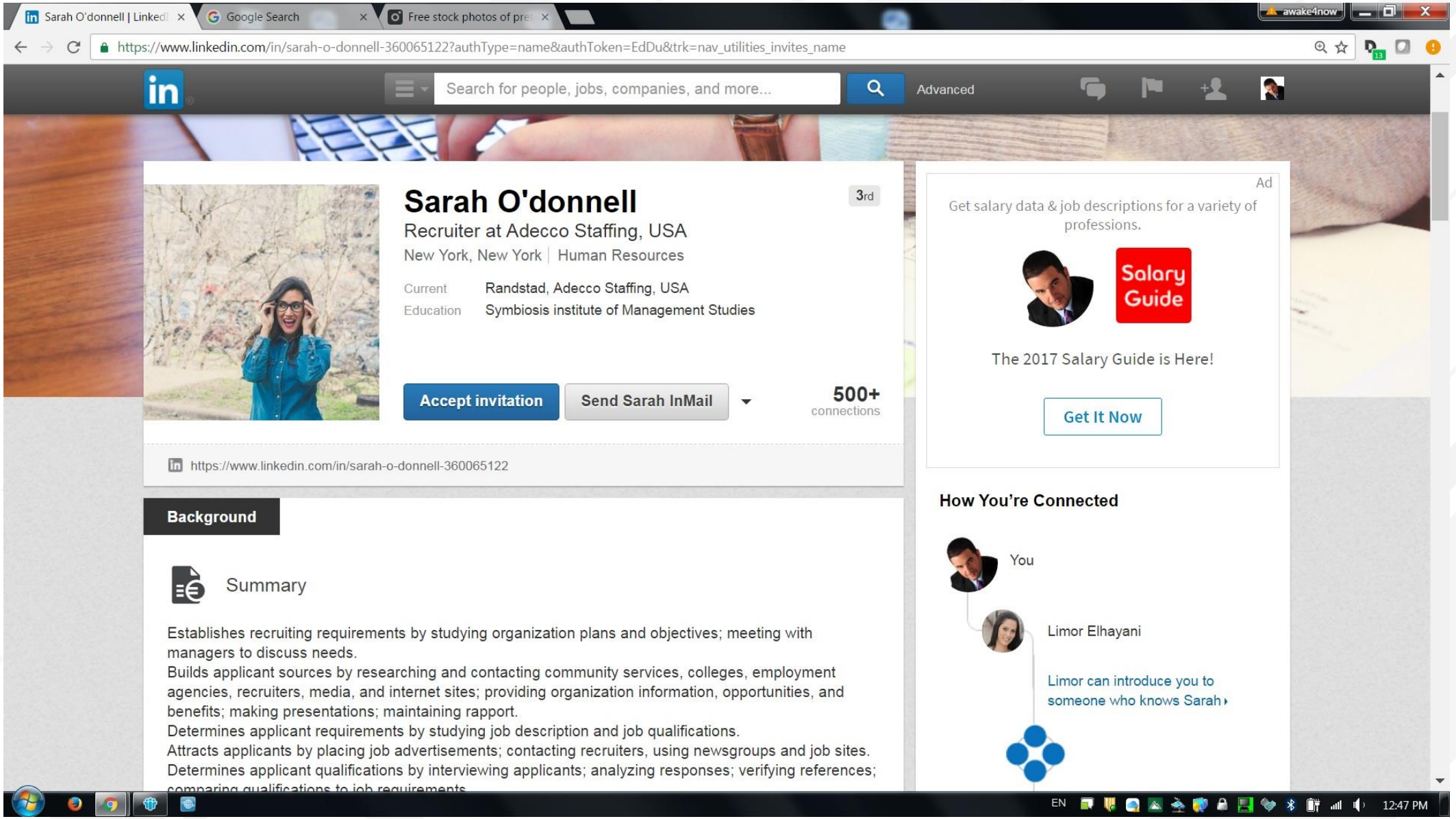
EXCLUSIVE: Chloe Grace Moretz will voice the title character in *The Tale Of The Princess Kaguya*, the latest animated pic from Studio Ghibli, the company co-founded by Japan animation icons Hayao Miyazaki and Isao Takahata. James Caan, Mary Steenburgen, Darren Criss, Lucy Liu, Beau Bridges, James Marsden, Oliver Platt and Dean Cain also have signed up for the film, which GKIDS acquired in March to release in the U.S. The indie distributor, which has four Best Animated Feature nominations since 2010, has set an October 17 release date timed to maximize awards-season play.

Takahata (*Grave Of The Fireflies*) directed *Kaguya* in his helming effort in in 14 years, and the pic based on the an ancient Japanese folk story the Tale of the Bamboo Cutter played strong in Japan when it was released there in November . The plot: Found inside a shining stalk of bamboo, a tiny girl grows into an exquisite young lady, raised by an old bamboo cutter and his wife. From the countryside to the grand capital city, even unseen she enthralls all who encounter her, including five noble suitors. Ultimately however she must face her secret fate.

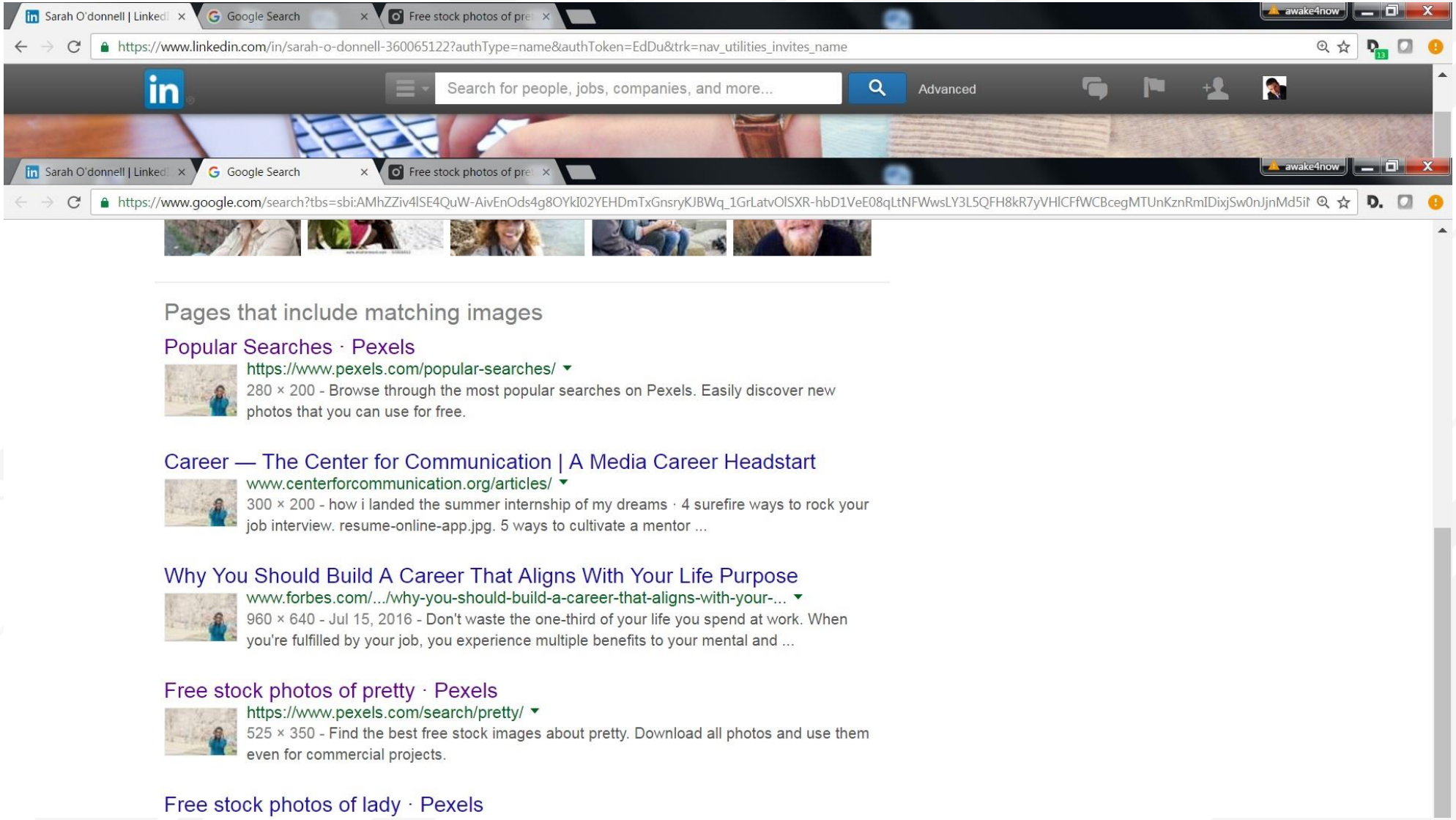
Studio Ghibli and Geoffrey Wexler are producing the English-language version of the pic with Frank Marshall of

EN 1:31 PM

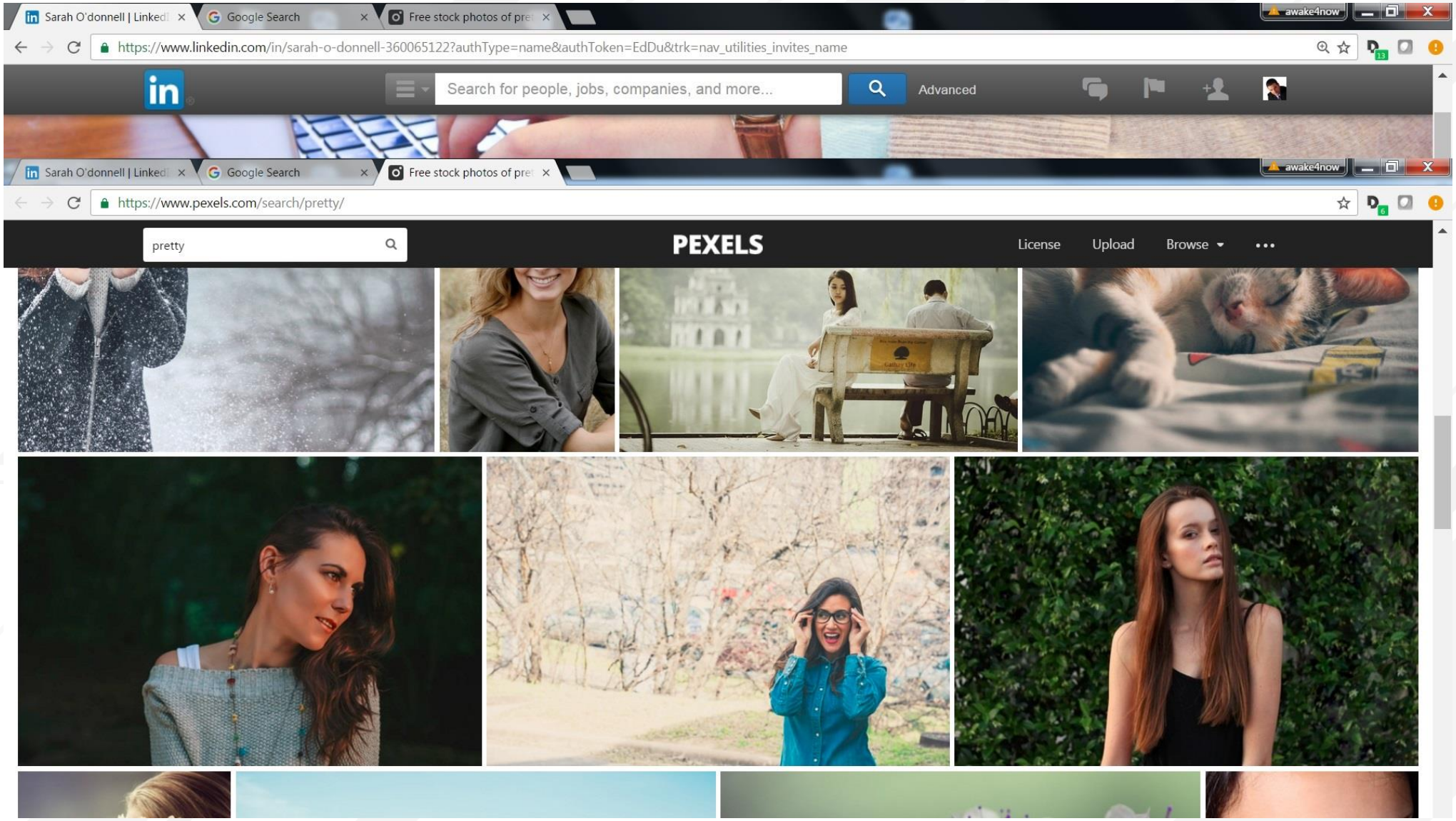
My LinkedIn


Sarah O'donnell | Linked
Google Search
Free stock photos of pre
https://www.linkedin.com/in/sarah-o-donnell-360065122?authType=name&authToken=EdDu&trk=nav_utilities_invites_name
Search for people, jobs, companies, and more...
Advanced
Sarah O'donnell
3rd
Recruiter at Adecco Staffing, USA
New York, New York | Human Resources
Current Randstad, Adecco Staffing, USA
Education Symbiosis institute of Management Studies
Accept invitation
Send Sarah InMail
500+
connections
https://www.linkedin.com/in/sarah-o-donnell-360065122
Background
Summary
Establishes recruiting requirements by studying organization plans and objectives; meeting with managers to discuss needs.
Builds applicant sources by researching and contacting community services, colleges, employment agencies, recruiters, media, and internet sites; providing organization information, opportunities, and benefits; making presentations; maintaining rapport.
Determines applicant requirements by studying job description and job qualifications.
Attracts applicants by placing job advertisements; contacting recruiters, using newsgroups and job sites.
Determines applicant qualifications by interviewing applicants; analyzing responses; verifying references;
Ad
Get salary data & job descriptions for a variety of professions.
Salary Guide
The 2017 Salary Guide is Here!
Get It Now
How You're Connected
You
Limor Elhayani
Limor can introduce you to someone who knows Sarah
EN
12:47 PM

My LinkedIn


Sarah O'donnell | Linked
Google Search
Free stock photos of pre
awake4now
https://www.linkedin.com/in/sarah-o-donnell-360065122?authType=name&authToken=EdDu&trk=nav_utilities_invites_name
Search for people, jobs, companies, and more...
Advanced
https://www.google.com/search?tbs=sbi:AMhZZiv4lSE4QuW-AivEnOds4g8OYkI02YEHDmTxGnsryKJBWq_1GrLatvOlSXR-hbD1VeE08qLtNFWwsLY3L5QFH8kR7yVHlCFfWCBcegMTUnKznRmIDixjSw0nJjnMd5iI
Pages that include matching images
Popular Searches · Pexels
https://www.pexels.com/popular-searches/
280 × 200 - Browse through the most popular searches on Pexels. Easily discover new photos that you can use for free.
Career — The Center for Communication | A Media Career Headstart
www.centerforcommunication.org/articles/
300 × 200 - how i landed the summer internship of my dreams · 4 surefire ways to rock your job interview. resume-online-app.jpg. 5 ways to cultivate a mentor ...
Why You Should Build A Career That Aligns With Your Life Purpose
www.forbes.com/.../why-you-should-build-a-career-that-aligns-with-your-...
960 × 640 - Jul 15, 2016 - Don't waste the one-third of your life you spend at work. When you're fulfilled by your job, you experience multiple benefits to your mental and ...
Free stock photos of pretty · Pexels
https://www.pexels.com/search/pretty/
525 × 350 - Find the best free stock images about pretty. Download all photos and use them even for commercial projects.
Free stock photos of lady · Pexels

My LinkedIn


Sarah O'donnell | Linked
Google Search
Free stock photos of pre
awake4now
https://www.linkedin.com/in/sarah-o-donnell-360065122?authType=name&authToken=EdDu&trk=nav_utilities_invites_name
Search for people, jobs, companies, and more...
Advanced
Sarah O'donnell | Linked
Google Search
Free stock photos of pre
awake4now
https://www.pexels.com/search/pretty/
pretty
PEXELS
License
Upload
Browse

My LinkedIn

Sarah O'donnell | Linked | Recruiter Job Description

hiring.monster.com/hr/hr-best-practices/recruiting-hiring-advice/job-descriptions/recruiter-job-description-sample.aspx

Monster.com | OFCCP Info | Contact Monster | Security Center | Help

MONSTER

Sign In

Home | Products | Solutions | Resource Center | Success Stories

Home / Recruiting & Hiring Advice / Job Descriptions / Recruiter Job Description Sample

Search Resource Center

Recruiter Job Description Sample

This recruiter sample job description can assist in your creating a job application that will attract job candidates who are qualified for the job. Feel free to revise this job description to meet your specific job duties and job requirements.

Recruiter Job Responsibilities:

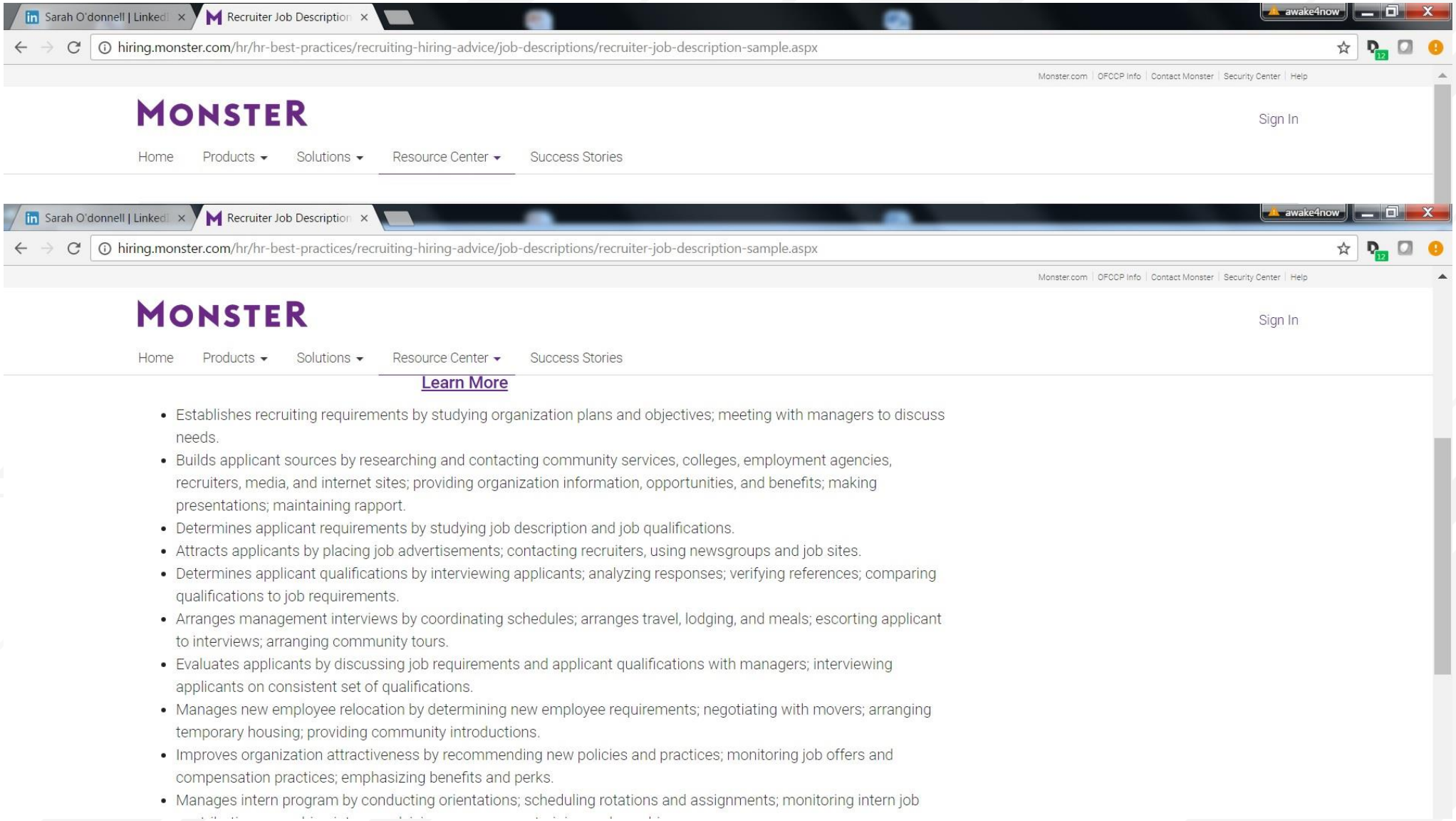
Achieves staffing objectives by recruiting and evaluating job candidates; advising managers; managing relocations and intern program.

Recruiter Job Duties:

- Establishes recruiting requirements by studying organization plans and objectives; meeting with managers to discuss needs.
- Builds applicant sources by researching and contacting community services, colleges, employment agencies, recruiters, media, and internet sites; providing organization information, opportunities, and benefits; making presentations; maintaining rapport.

EN 12:49 PM

My LinkedIn


Sarah O'donnell | Linked
Recruiter Job Description
awake4now
hiring.monster.com/hr/hr-best-practices/recruiting-hiring-advice/job-descriptions/recruiter-job-description-sample.aspx
Monster.com | OFCCP Info | Contact Monster | Security Center | Help
MONSTER
Sign In
Home
Products
Solutions
Resource Center
Success Stories
Learn More
• Establishes recruiting requirements by studying organization plans and objectives; meeting with managers to discuss needs.
• Builds applicant sources by researching and contacting community services, colleges, employment agencies, recruiters, media, and internet sites; providing organization information, opportunities, and benefits; making presentations; maintaining rapport.
• Determines applicant requirements by studying job description and job qualifications.
• Attracts applicants by placing job advertisements; contacting recruiters, using newsgroups and job sites.
• Determines applicant qualifications by interviewing applicants; analyzing responses; verifying references; comparing qualifications to job requirements.
• Arranges management interviews by coordinating schedules; arranges travel, lodging, and meals; escorting applicant to interviews; arranging community tours.
• Evaluates applicants by discussing job requirements and applicant qualifications with managers; interviewing applicants on consistent set of qualifications.
• Manages new employee relocation by determining new employee requirements; negotiating with movers; arranging temporary housing; providing community introductions.
• Improves organization attractiveness by recommending new policies and practices; monitoring job offers and compensation practices; emphasizing benefits and perks.
• Manages intern program by conducting orientations; scheduling rotations and assignments; monitoring intern job

INTSIGHTS
Defend Forward™

Ransomware Review

Maze Group ROI?

Maze Team official press release. June 22, 2020

Maze Team is working hard on collecting and analyzing the information about our clients and their work. We also analyzing the post attack state of our clients. How fast they were able to recover after the successful negotiations or without cooperation at all.

Today we would like to tell some words about the cost of non-cooperation and about our clients who were trying to recover all the information themselves. Looking ahead all those attempts were more close to suicide than to recovery.

So the company was attacked and the files were blocked and encrypted. What are the worst mistakes the company can made?

Maze Locker can't be decrypted without the help of Maze Team. A few companies we are not going to name were trying to decrypt the files with the help of side organizations. Those organizations are well known security companies. That happened at the end of 2019 and they are still waiting for a solution. As we know, compared to the first offer of Maze Team, those companies already paid two and a half times more money. One of those companies already spend four times more trying to decrypt the files themselves. And we guarantee that it would take them years to wait until decryption.

But encrypting files is not the main risk. If the company have chosen to make a long pause in its operations this is the company's right. But sometimes companies can't understand the risk of information leak, especially the private information. We are specializing in client's private information, financial information, databases, credit card data, NDA documents and all the company's researches.

Usually that kind of information leaks will lead for multimillion losses, fines and lawsuits. And don't forget about the lost profit and falling of the stock price.

As we know from the reports of our clients the average recovery costs are about $60M. We have never asked for amounts even close to those.

According to our statistics the loss from lawsuits and fines varies from $18M to $47M. As we know from one of our clients, in one week he loosed $12M while his files were in open access. For large companies the average lost if about $50M-60M after the publication of private data. A few very large companies have lost from $250M to $350M.

While hiring the negotiators from the side, especially the those who work on government, and listening to what they tell you, try to think are they really interested in solving your problems or they are just thinking about their own profit and ambitions of the government agency they belong to. They can't minimize your loss or eliminate the data breach. You'll pay from your own pocket.

Ransomware: Customer Service

07/26/2020 00:24:03

Support

Hello! Can I help you?

You

07/27/2020 03:27:33

Hello? What do we need to do to get our data deleted from your servers and unlock our files?

07/27/2020 07:43:08

Support

Hello !

You have 30.000 infected and locked devices from different countries.
Our price is consists of two services, decryption software and deleting all downloaded data from our servers.
If you need both of them you have to pay 10.000.000$ in Bitcoins, before the timer on main page will ends.
As a bonus we will provide you with the details about how we breach your security perimeter and give you recommendations about improving security measures to help your admins avoid such issues in future!

07/27/2020 07:43:35

Support

For sure we understand your worries about this deal, that's why we will decrypt two your random files for Free, just to prove that our decryptor is working properly!

Ransomware: Customer Service (Cont.)

You

07/27/2020 17:47:17

So in your message that you left us, you mentioned a "very SPECIAL PRICE" if we reached out to you within 2 days, which we did. There's no way that $10M is a "very SPECIAL PRICE" right?

07/27/2020 18:07:05

Support

This price isn't a Special price, correct! However it is a standard amount for company of your size and it's probably much cheaper than lawsuits expenses, reputation loss caused by leakage.

Yes we did offered a special price and you are eligible for it, so if you are ready to process the payment promptly, we can make a step forward to your direction and give you a discount.

Ransomware: Customer Service (Cont.)

I appreciate the discount and kind words here, but to be honest, we were hoping for something that we actually have available cash for. I completely understand that this is a business for you, but right now I'm tasked with trying to keep our business afloat. In all honesty, $8M puts us in a spot where we would need to double current revenue to keep our doors open. We were willing to get you $3.7M potentially today if we could have found common ground. I don't mean to belittle you and your team's work here, I'm just trying to help prevent further layoffs on our side.

07/27/2020 18:31:25

07/27/2020 18:48:03

Support

We appreciate your offer, but understand us too, this is the market and you have been offered an adequate price. unfortunately, the amount you offered is not enough to close our deal with you, we gave you 20% not because we are ready to bargain heavily, but because we see your business spirit and immediately gave you a good discount, we can offer 5% discount more and payment by installments. For example for $4M you will get the Decryptor and after you will pay the rest amount, we will delete all the private Data.

Ransomware: Customer Service (Cont.)

07/28/2020 00:47:12

Here are the list of recommendations to avoid such a things in future:
- Turn off local passwords
- Force end of administrators sessions
- In group policy set up wdigest value to "0", If the UseLogonCredential value is set to 0, WDigest will not store credentials in memory.
- Update passwords every month !
- Check the granted privileges for users, to make them maximum reduced privileges and access only to exact applications.
- In most cases there would enough standard windows software like an Applocker.
- Approve to run only necessaries applications ONLY.
- Don't count on the Anti-Virus, there is no one AV that really helps, they can be useful only in long-term infections, if hackers for some reasons didn't attack in short time.
- Install Endpoint Detection and Response security (EDR) and teach the IT-admin to work with it.
- For huge companies we suggest at least 3 system administrators working 24 hours, maximum 4 admins working 3 shifts for 8 hours per day, that would be enough.

Ransomware: Customer Service (Cont.)

You

07/28/2020 00:51:17

Thank you for all of this in a very timely manner

07/28/2020 00:53:29

Support

You are welcome it's a pleasure to work with professionals. If there will be any questions, please feel free to ask

07/28/2020 01:23:07

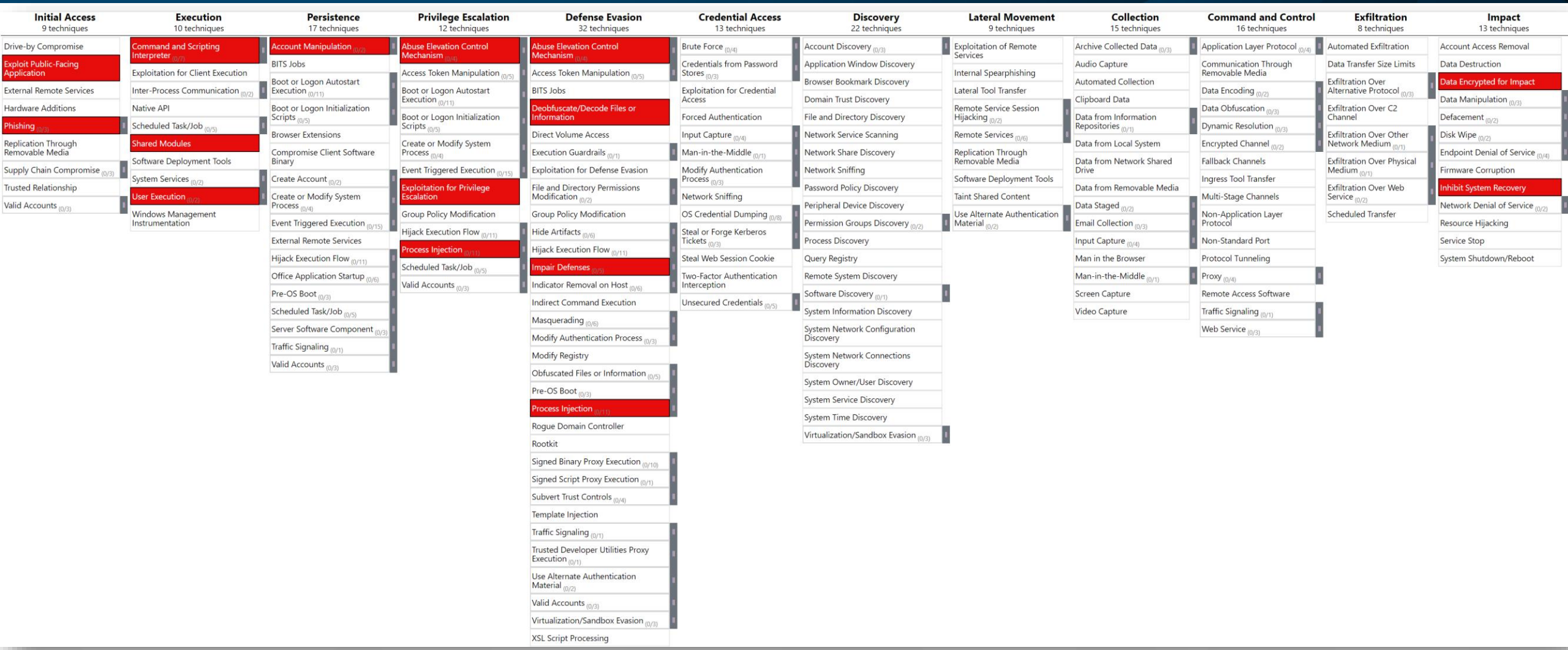
Support

Please confirm that you wrote down all important information from this Chat, so we could clear it. However we will keep the chat room and will be here for your support if necessary

INTSIGHTS
Defend Forward™

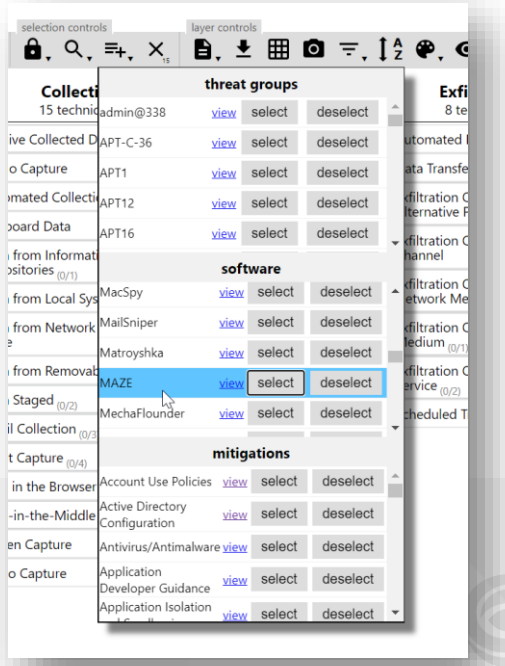
The Take Aways

Understand the Threat - Sodinokibi



Understand the Threat - Maze

Initial Access 9 techniques	Execution 10 techniques	Persistence 17 techniques	Privilege Escalation 12 techniques	Defense Evasion 32 techniques	Credential Access 13 techniques	Discovery 22 techniques	Lateral Movement 9 techniques	Collection 15 techniques	Command and Control 16 techniques	Exfiltration 8 techniques	Impact 13 techniques
Drive-by Compromise	Command and Scripting Interpreter (1/7)	Account Manipulation (0/2)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Brute Force (0/4)	Account Discovery (0/3)	Exploitation of Remote Services	Archive Collected Data (0/3)	Application Layer Protocol (1/4)	Automated Exfiltration	Account Access Removal
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Credentials from Password Stores (0/3)	Application Window Discovery	Internal Spearphishing	Audio Capture	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
External Remote Services	Inter-Process Communication (0/2)	Boot or Logon Autostart Execution (0/11)	Boot or Logon Autostart Execution (0/11)	BITS Jobs	Exploitation for Credential Access	Browser Bookmark Discovery	Lateral Tool Transfer	Automated Collection	Data Encoding (0/2)	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Hardware Additions	Native API	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Deobfuscate/Decode Files or Information	Forced Authentication	Domain Trust Discovery	Remote Service Session Hijacking (0/2)	Clipboard Data	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Phishing (0/3)	Scheduled Task/Job (0/5)	Browser Extensions	Create or Modify System Process (0/4)	Direct Volume Access	Input Capture (0/4)	File and Directory Discovery	Remote Services (0/6)	Data from Information Repositories (0/1)	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Event Triggered Execution (0/15)	Execution Guardrails (0/1)	Man-in-the-Middle (0/1)	Network Service Scanning	Replication Through Removable Media	Data from Local System	Encrypted Channel (0/2)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Supply Chain Compromise (0/3)	Software Deployment Tools	Create Account (0/2)	Exploitation for Privilege Escalation	Exploitation for Defense Evasion	Modify Authentication Process (0/3)	Network Share Discovery	Software Deployment Tools	Data from Network Shared Drive	Fallback Channels	Exfiltration Over Web Service (0/2)	Endpoint Denial of Service (0/4)
Trusted Relationship	System Services (0/2)	Create or Modify System Process (0/4)	Group Policy Modification	File and Directory Permissions Modification (0/2)	Network Sniffing	Network Sniffing	Taint Shared Content	Data from Removable Media	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Valid Accounts (0/3)	User Execution (0/2)	Event Triggered Execution (0/15)	Hijack Execution Flow (0/11)	Group Policy Modification	OS Credential Dumping (0/8)	Password Policy Discovery	Use Alternate Authentication Material (0/2)	Data Staged (0/2)	Multi-Stage Channels		Inhibit System Recovery
	Windows Management Instrumentation	External Remote Services	Process Injection (1/11)	Hide Artifacts (0/6)	Steal or Forge Kerberos Tickets (0/3)	Peripheral Device Discovery		Email Collection (0/3)	Non-Application Layer Protocol		Network Denial of Service (0/2)
		Hijack Execution Flow (0/11)	Scheduled Task/Job (0/5)	Hijack Execution Flow (0/11)	Steal Web Session Cookie	Permission Groups Discovery (0/2)		Input Capture (0/4)	Non-Standard Port		Resource Hijacking
		Office Application Startup (0/6)	Valid Accounts (0/3)	Impair Defenses (1/5)	Two-Factor Authentication Interception	Process Discovery		Man in the Browser	Protocol Tunneling		Service Stop
		Pre-OS Boot (0/3)		Indicator Removal on Host (0/6)	Unsecured Credentials (0/5)	Query Registry		Man-in-the-Middle (0/1)	Proxy (0/4)		System Shutdown/Reboot
		Scheduled Task/Job (0/5)		Indirect Command Execution		Remote System Discovery		Screen Capture	Remote Access Software		
		Server Software Component (0/3)		Masquerading (0/6)		Software Discovery (0/1)		Video Capture	Traffic Signaling (0/1)		
		Traffic Signaling (0/1)		Modify Authentication Process (0/3)		System Information Discovery			Web Service (0/3)		
		Valid Accounts (0/3)		Modify Registry		System Network Configuration Discovery					
				Obfuscated Files or Information (1/5)		System Network Connections Discovery					
				Pre-OS Boot (0/3)		System Owner/User Discovery					
				Process Injection (1/11)		System Service Discovery					
				Rogue Domain Controller		System Time Discovery					
				Rootkit		Virtualization/Sandbox Evasion (0/3)					
				Signed Binary Proxy Execution (0/10)							
				Signed Script Proxy Execution (0/1)							
				Subvert Trust Controls (0/4)							
				Template Injection							
				Traffic Signaling (0/1)							
				Trusted Developer Utilities Proxy Execution (0/1)							
				Use Alternate Authentication Material (0/2)							
				Valid Accounts (0/3)							
				Virtualization/Sandbox Evasion (0/3)							
				XSL Script Processing							



Understand the Threat - Maze

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact
11 items	34 items	62 items	32 items	69 items	21 items	23 items	18 items	13 items	22 items	9 items	16 items
External Remote Services	Command-Line Interface	Valid Accounts	Valid Accounts	Valid Accounts	Credential Dumping	Account Discovery	Remote Desktop Protocol	Data from Network Shared Drive	Commonly Used Port	Data Compressed	Data Encrypted for Impact
Valid Accounts	PowerShell	Modify Existing Service	Process Injection	Obfuscated Files or Information	Credentials in Files	Domain Trust Discovery	Remote File Copy	Data Staged	Remote File Copy	Exfiltration Over Alternative Protocol	Service Stop
Spearphishing Attachment	Scripting	New Service	New Service	Scripting	LLMNR/NBT-NS Poisoning and Relay	File and Directory Discovery	Pass the Ticket	Data from Local System	Standard Application Layer Protocol	Automated Exfiltration	Inhibit System Recovery
Drive-by Compromise	Service Execution	Create Account	Access Token Manipulation	Code Signing	Brute Force	Permission Groups Discovery	Windows Admin Shares	Audio Capture	Remote Access Tools	Data Encrypted	Account Access Removal
Exploit Public-Facing Application	Rundll32	.bash_profile and .bashrc	Accessibility Features	Disabling Security Tools	Account Manipulation	Remote System Discovery	Windows Remote Management	Automated Collection	Standard Cryptographic Protocol	Data Transfer Size Limits	Data Destruction
Hardware Additions	User Execution	Accessibility Features	AppCert DLLs	Indirect Command Execution	Bash History	Network Share Discovery	AppleScript	Clipboard Data	Communication Through Removable Media	Exfiltration Over Command and Control Channel	Defacement
Replication Through Removable Media	Windows Remote Management	Account Manipulation	AppInit DLLs	Masquerading	Credentials from Web Browsers	System Owner/User Discovery	Application Deployment Software	Data from Information Repositories	Connection Proxy	Exfiltration Over Other Network Medium	Disk Content Wipe
Spearphishing Link	AppleScript	AppCert DLLs	Application Shimming	Modify Registry	Credentials in Registry	System Network Configuration Discovery	Component Object Model and Distributed COM	Data from Removable Media	Custom Command and Control Protocol	Exfiltration Over Physical Medium	Disk Structure Wipe
Spearphishing via Service	CMSTP	AppInit DLLs	Bypass User Account Control	Process Injection	Exploitation for Credential Access	Application Window Discovery	Exploitation of Remote Services	Email Collection			Endpoint Denial of Service
	Compiled HTML File	Application Shimming	DLL Search Order Hijacking	Redundant Access	Forced	Browser Bookmark Discovery					Firmware Corruption
	Component Object Model and Distributed COM	Authentication	Dylib Hijacking	Deobfuscate/Decode Files or Information							Network Denial of Service
				File Deletion							

INTSIGHTS
Defend Forward™

I Mean, REALLY IN THE OPEN

Securing Passwords … On National TV

Securing Passwords … On National TV

Securing Passwords ... On National TV

Securing Passwords… During A Site Visit

Jeffrey Wong, the Hawaii Emergency Management Agency's current operations officer, shows computer screens monitoring hazards at the agency's headquarters in Honolulu on Friday. Hawaii is the first state to prepare the public for the possibility of a ballistic missile strike from North Korea. | AP

ASIA PACIFIC

Hawaii first U.S. state to prepare for 'unlikely' North Korea missile threat

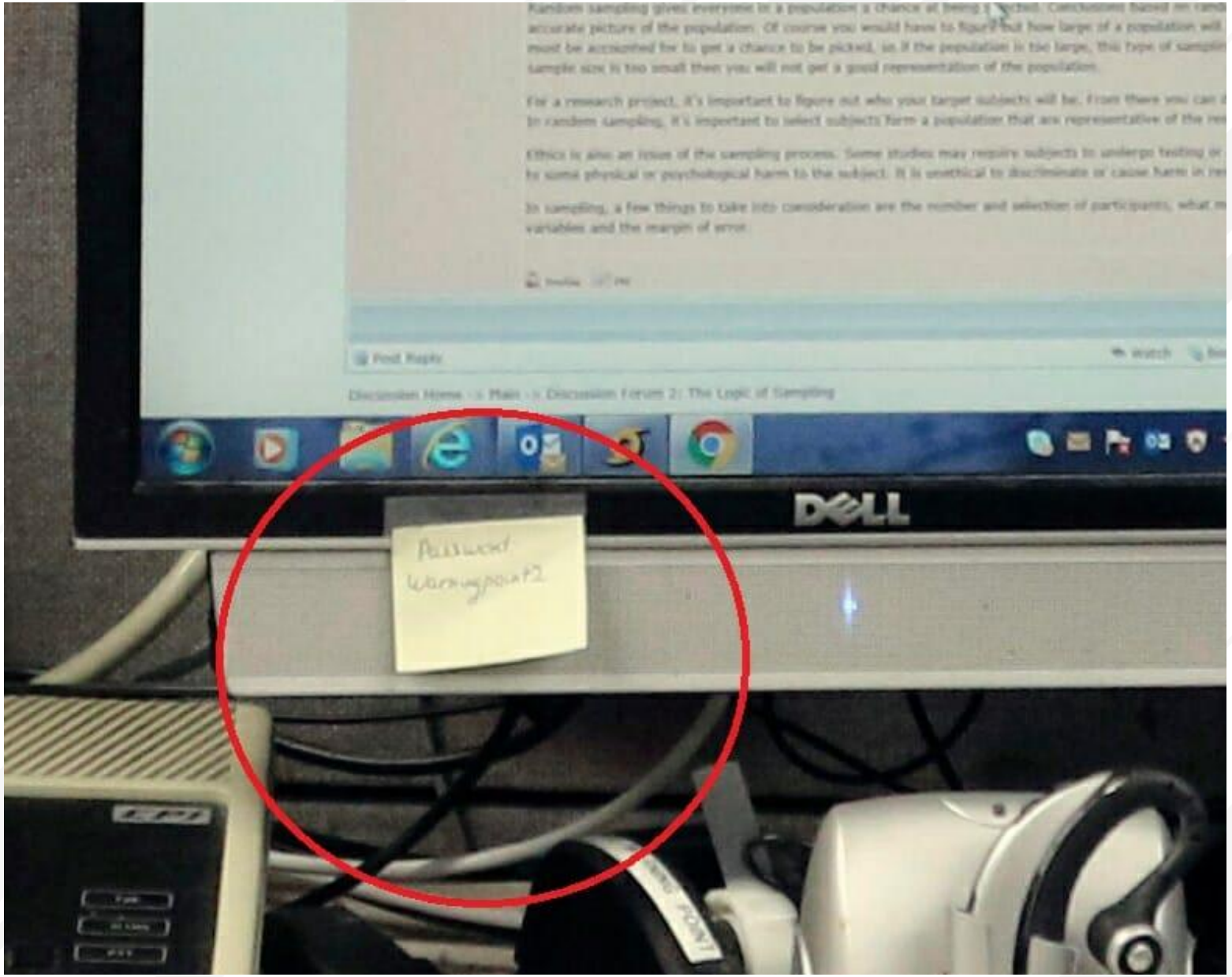
AP, STAFF REPORT

HONOLULU – Hawaii is the first state to prepare the public for the possibility of a ballistic missile strike from North Korea.

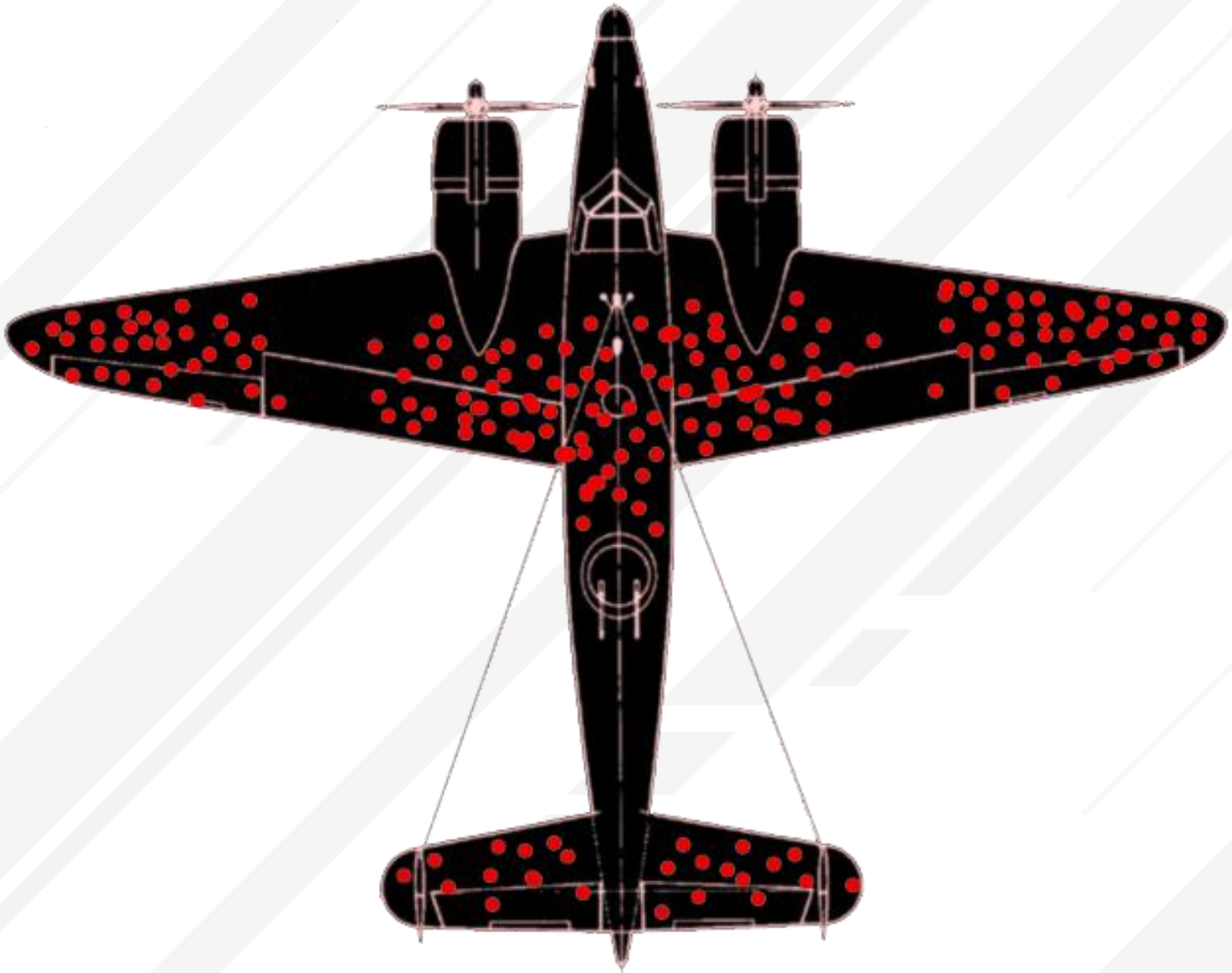
JUL 22, 2017

ARTICLE HISTORY

Securing Passwords… During A Site Visit



The Bias




INTSIGHTS
Defend Forward™
Thank You
Questions?