

LOW HANGING FRUIT

OFFENSIVE OSINT FOR DEFENSE

@BOSINTBLANC

WHOAMI?

- Background in Desktop Support, SOC/IR and lover of all things OSINT. Currently employed as a lead intelligence analyst with threat intelligence firm DarkTower.
- 2nd place finish with team Dwayne “the sock” Johnson in Tracelabs Global Search Party.
- Case Tracking & Statistics Lead with NCPTF.

@BOSINTBLANC

DISCLAIMER:

- Nothing in this presentation represents the views of my employers or organizations I am associated with past, present or future.
- DO NOT DO CRIMES. Do OSINT for good.

@BOSINTBLANC

CREDIT WHERE ITS DUE

- GOOGLE Hacking by Johnny Long has be a huge inspiration to me.
- OSINTDOJO.COM has provided a path for OSINT learning. @sinwindie is one of the best OSINTers out there in my opinion.

@BOSINTBLANC

From Facebook to LinkedIn, data-scraping leaks proliferate

The incentives and opportunities for harvesting valuable personal information have multiplied

Clubhouse Joins Facebook and LinkedIn as Target of Data Scraping; Cumulative One Billion User Profiles Have Been Leaked

Facebook Responds To Data Leak – Says, ‘Data Not Hacked, But Scraped’

@BOSINTBLANC

A COUPLE QUESTIONS FOR YOU.

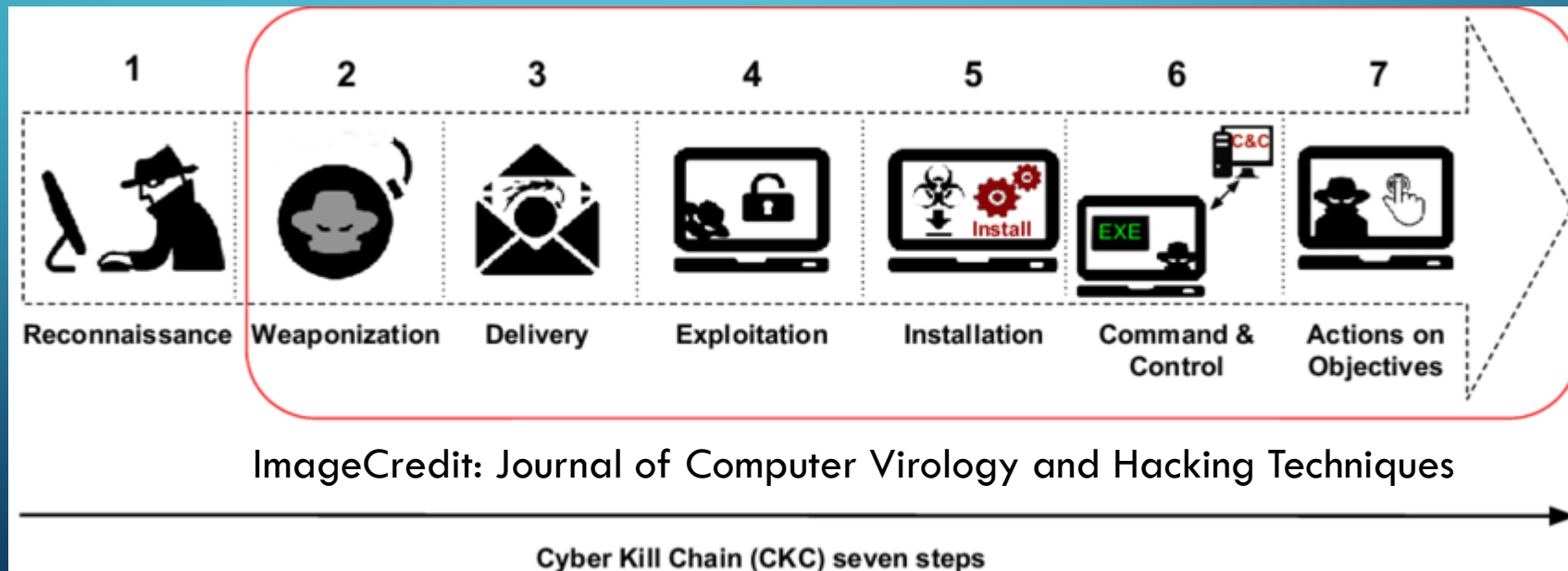
- How much damage could someone do to an organization using only a Google search?
- What do Facebook, LinkedIn, and Clubhouse have in common?

THE STAGES OF FINDING LOW HANGING FRUIT

- Stage 1: Rationale and Methodology.
- Stage 2: Conduct the investigation
- Stage 3: Lessons learned and closing thoughts.

STAGE 1 : WHY MAP AN OSINT ATTACK SURFACE?

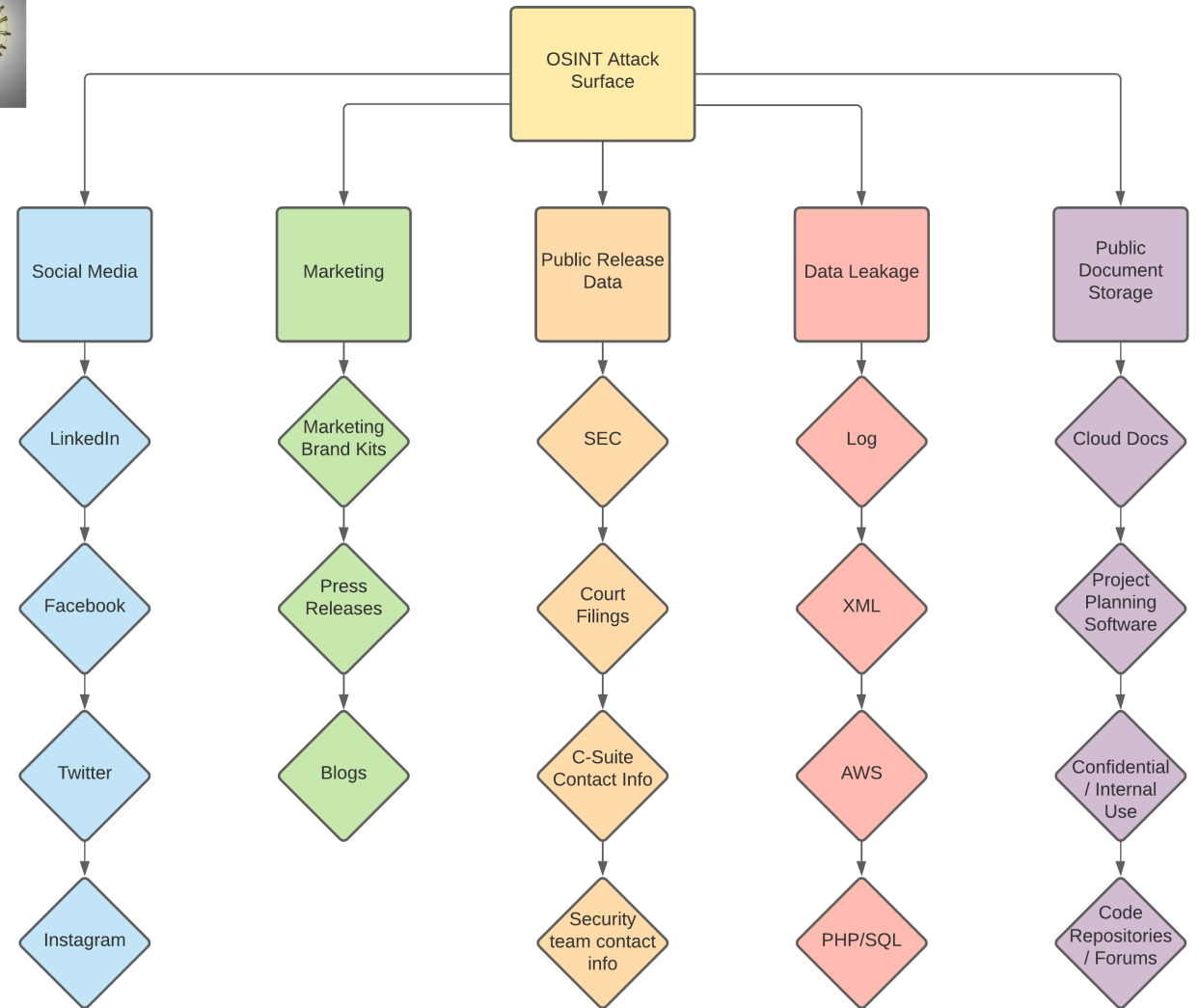
- Blue teams spend almost 100 % of their time in sections 2-7 of the kill chain.
- Red teams may gain additional insight in tech stack, organizational structure and culture and additional avenues of exploitation.



STAGE 1: TAKE AIM.

@BOSINTBLANC

@BosintBlanc



STAGE 1: WOULD YOU LIKE TO PLAY A GAME?

- I chose a company off the Fortune 500 list at random. For the purposes of this presentation I am calling them Big Financial Company or BFC.
- I performed passive intelligence gathering on their OSINT attack surface.
- For the entire enterprise I will only use Google. No tools and no active methods. Since this company has not granted me permission I only click things which are distinctly public domain.

STAGE 2: LET THE HUNT BEGIN!

- Social Media
 - Often great to start with:
 - Development Team
 - IT Security Team
 - IT Leadership
 - Executives

@BOSINTBLANC

STAGE 2: CASH ME OUTSIDE

- Searching `site:linkedin.com "BFC" & "information security"` gets us a list of BFC's security staff.

site:linkedin.com [redacted] & "information security"

About 10,600 results (0.47 seconds)

[https://www.linkedin.com/\[redacted\]](https://www.linkedin.com/[redacted]) - [redacted]
Washington D.C. Metro Area - [redacted]
Experience - Director, **Information Security**, Architecture, Assurance and Advisory - Director
Security Architecture, [redacted]

[https://www.linkedin.com/\[redacted\]](https://www.linkedin.com/[redacted]) - [redacted]
Washington D.C. Metro Area - Director, Information Security Transformation [redacted]
[redacted] Experienced **Information Security** Executive. [redacted]
Baltimore. Washington D.C. Metro [redacted]

[https://www.linkedin.com/\[redacted\]](https://www.linkedin.com/[redacted]) - **Information Security Professional** - [redacted]
Washington D.C. Metro Area - Information Security Professional [redacted]
View [redacted] profile on LinkedIn, the world's largest professional community. [redacted]
has 2 jobs listed on their profile. See the complete profile on ...

[https://www.linkedin.com/\[redacted\]](https://www.linkedin.com/[redacted]) - **Director, Information Security** - [redacted] ...
Washington D.C. Metro Area - Director, Information Security - [redacted]
View [redacted] profile on LinkedIn, the world's largest professional community. [redacted] has
1 job listed on their profile. See the complete profile on LinkedIn ...

[https://www.linkedin.com/\[redacted\]](https://www.linkedin.com/[redacted]) - **Information Security Associate** - [redacted]
Washington D.C. Metro Area - Information Security Associate - [redacted]
View [redacted] profile on LinkedIn, the world's largest professional community. [redacted] has
1 job listed on their profile. See the complete profile on ...

STAGE 2: CASH ME OUTSIDE

- The first three security people's profiles give me no valuable information. The 4th we hit something interesting.



Information Security, Senior Technical Lead at [REDACTED]

Information Security Manager

Full-time

- Management of all day-to-day team operations pertaining to Access Certification, responsible for execution of corporate-wide periodic access reviews for Privileged infrastructure access as well high-risk applications using **SailPoint IdentityIQ**.
- Management of all day-to-day team operations pertaining to Access Management, responsible for the operational support and user access provisioning of approximately 150+ high-risk business applications and 12 core infrastructure platforms.
- Managed all daily operations and access governance activities for identities and accounts, privileged account access, and role and entitlement management.
 - Partner with IT Risk Management team and liaise with 2nd/3rd LOD, maintaining relationships and providing visibility of program.
 - Work with our risk partners to support issue management using risk assessments to resolve severity of issues, partnering with process owners for the timely development and execution of remediation action plans.
- Review, assessment, benchmark and development of issue remediation action plans for IT programs and technologies within IAM.
 - Implement policies, standards, and processes for **IAM** in support of alignment with overall Enterprise strategy and compliance.
 - Provided advisory services to business and technology teams concerning IAM security controls and responded to internal, external and SOX audits and regulator requests.
- Identified gaps/risks in user Joiner-Mover-Leaver processes and created and enhanced IAM processes, automating them where possible to remove manual work that lead to errors of omission and commission.
- Major stakeholder and active participation with IAM Solutioning for successful implementation of newly deployed **SailPoint IIQ**.
 - Strategic management planning for future state Project Releases in support of capability deployments for **IAM** Transformation.
- Development, communication and execution of new Enterprise-wide strategy for **Privileged Access Management (PAM)**.

see less

STAGE 2: NOW THAT'S PIVOTING

- Unfamiliar with Sailpoint I search information on it. Turns out to be an IAM software.

@BOSINTBLANC

SailPoint IdentityIQ®

Find your hidden security risks.

If you don't know who has access to your applications and data, you probably have security and compliance gaps you haven't even thought about.

With IdentityIQ at the center of your enterprise, you can [control access to every file and application across your hybrid IT environment](#) by employees, partners, contractors — even bots.

Keep up with the complexity and speed of business.

Combine SailPoint [Predictive Identity™](#) with IdentityIQ to unleash AI-driven capabilities that help you see and do more. Our [Access Modeling](#), [Access Insights](#) and [Recommendations](#) provide greater intelligence and efficiency by keeping access policies up-to-date, and let you know if access is safe or risky.

Learn more



See IdentityIQ in action



Get an identity solution built to scale with your business



Find out how to secure access to data stored in files



Learn how to govern access to AWS



Control and secure access to your SAP systems



STAGE 2: NOW THAT'S PIVOTING2

- I search site:bfc.com inurl:identityiq
- This returns the subdomain of their IAM portal.
- One of the most interesting hits is the success page of the password reset.

@BOSINTBLANC

The screenshot shows a Google search interface with the query 'site:bigfinancialcompany.com inurl:identityiq'. The search results are filtered to show only the domain 'bigfinancialcompany.com'. The results list several pages related to SailPoint IdentityIQ, including login, forgot username, forgot password, and success pages. The search results are as follows:

- Access Manager for e-Business Login**
Username : Forgot your username? Password : Forgot your password? © **[REDACTED]**
Questions? Call 1-800 ...
- SailPoint IdentityIQ - [REDACTED]**
Forgot Username. Email Address. Confirm Email Address. © **[REDACTED]**. Terms of Use · Privacy Policy.
- SailPoint IdentityIQ [REDACTED]**
SailPoint Logo. Reset Password. Username. Forgot Username? © Copyright 2019 SailPoint Technologies - All rights reserved.
- SailPoint IdentityIQ**
[REDACTED] Seller/Service Number *. Institution Name *. First Name *. Middle Name. Last Name *. Phone Number *. Email Address *. User Title *.
- SailPoint IdentityIQ**
Debt Auction Registration. First Name *. Last Name *. User Title *. Dealer Firm Name *.
[REDACTED] [REDACTED] ...
- SailPoint IdentityIQ**
Success! If found, your username will be sent to the e-mail entered. © **[REDACTED]** Terms of ...

STAGE 2: WHOOPSY

- Brand guides should be behind a login. (opinion don't @ me)
- Yes threat actors can get this other ways but why make it easy?

@BOSINTBLANC

"Big Financial Company" "brand" guide

× | 🔊 🔍

🔍 All 📰 News 🖼️ Images 🛒 Shopping 📺 Videos ⋮ More ⚙️ Settings 🛠️ Tools

About 381,000 results (0.66 seconds)

██████████ > About ⋮
Lender Guide to Using Our Brand - ██████████
This **Guide** was created to help ██████████ lenders learn how to incorporate the new name into their businesses, whether in conversation with their ...

██████████ > Lenders ⋮
██
██████████ Multifamily Seller/Service**r Guide (Guide)** forms, commonly used underwriting forms, and other forms and documents are listed below. Access the ...

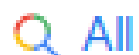
██████████ > marketing-materials PDF ⋮
██
Jan 1, 2020 — Please refer to the following marketing and branding **guidelines** when ... https://
██████████ /create/**brand-elements/** ...

██████████ > working-with-us > overview ⋮
Origination & Underwriting Overview - ██████████ ...
Whether you're a veteran lender or **brand** new to the business ██████████ has the ... **Guide**
Bulletin 2020-17 Temporary Purchase and Refinance Eligibility ...

██████████ > pdf > 062916guide PDF ⋮
██
Jun 29, 2016 — This is a PDF of the ██████████ Single-Family Seller/Service**r Guide** ... AllRegs
brand ("AllRegs") and which posts the **Guide** under license ...

STAGE 2: IS PUBLIC “CONFIDENTIAL”?

BigFinancialCompany filetype:pptx "internal use"



All



News



Shopping



Maps



Images



More

Settings

Tools

About 1 results (0.35 seconds)

[Redacted] › Chapter PPT



Slide 1

Property/Casualty. State Page – Exhibit of Premiums & Losses. New Line 29 for reporting of International business. Previously treated as a write-in. Created crosscheck problems.

STAGE 2: IS PUBLIC “CONFIDENTIAL”?

- Looking for filetype:pdf I noticed a number of things hosted with a title that led me to believe BFC’s doc service is leaking somewhere.

site:[redacted] intitle:print[redacted] "confidential"

About 329 results (0.37 seconds)

[redacted] > mbs > data PDF

print[redacted] file - [redacted]

Dec 5, 2017 —\$520,064,655. \$181,704,308. \$106,851,483 \$1,960,205,130. (1) Includes all loans in [redacted] is the named special servicer, ...

[redacted] _assets > docs > stacr_2... PDF

[redacted] - [redacted]

[redacted] — a brief and non-exhaustive summary of which is included under “— Claiming the De Minimis Exemption” below. As discussed under “Risk Factors — Investment Factors and Risks ...

[redacted] > mbs > data PDF

print[redacted] file - [redacted]

Feb 6, 2019 — primary servicing functions with respect to the underlying mortgage loans sub-serviced by [redacted] may delegate its duties to agents or subcontractors so long as the related ...



[redacted] > mbs > data PDF







print[redacted] file - [redacted]

Oct 25, 2018 — . The principal compensation to be paid to the master servicer with respect to its master servicing activities will be a servicing fee consisting of a master servicing fee, all or a portion of ...



STAGE 2: IS PUBLIC “CONFIDENTIAL”?


- Searching
various
presentation
formats almost
always proves
valuable.

BigFinancialCompany filetype:pptx "confidential" ×  



 All  News  Images  Maps  Videos  More Settings Tools


About 49 results (0.53 seconds)




 > February_Exhibits PPT 



Home Sales have been picking up - 


have been picking up. Home Sales have been picking up. 2012. 2013. 2014. 2015. 2016. 2017. 2018F. 2019F. 2020F. Home Sales have been picking up. Home Sales have been ...



 > uploads > 2019/11 > L... PPT 



ATTENTION: Apply Data Classification Label - 

 Confidential. 2. 2. Agenda. Overview of  What are the different Services in ; Understanding the Risk ...


 Serve_Carpenter PPT 

PowerPoint Presentation - Council for A  ..

2. Title III of the  authorizes  "Provide stability in the secondary market for residential mortgages;" "respond appropriately to the ...

 > wp-content > uploads > 2018/07 PPT 

PowerPoint Presentation



STAGE 3: LESSONS LEARNED

- Misconfigurations cause undesired information to be shared.
- Knowing your OSINT attack surface allows you to structure your defense and understand where your low hanging fruit lies and thus better structure your defense to compensate.
- Worst case you find nothing / best case your team are heroes.

STAGE 3: ONE LAST BOW

- Google alerts provide a easy and FREE monitoring for data leakage.
- This is not a vendor talk so I want recommend anyone specific but will say know when you need help.
- OSINT Attack Surface mapping looks differently at different security maturity levels.

THANK YOU

- Twitter: @Bosintblanc
- Email: osintholmes@protonmail.com
- Discord: BosintBlanc

