WEAPONIZING OSINT

WHAT YOU DON’T KNOW CAN HURT YOU....
OUTLINE OF THE TALK

Idea
Research
Prevention
IDEA:
PASSIVE
THREAT
LANDSCAPE
ATTACK PATH

01
The Goal is to only use passive methods of collection. With that intel, create a ransom style attack

02
We will review different information that might be able to be used against a target

03
We will not have time to review all options. The threat is based on the level of detail and the target its being used against
What can we use that is public
How best to use it
Best places to find it
What else can we find that might be damaging
- Business cards
  - Already have a name
  - Email
  - Phone number
  - Employed
ATTACKER PATH

- News articles
  - Who is a (B)(M)illionaire
  - Top 30 under 30
  - Local papers are your friend

Several Missouri, Kansas residents land on Forbes' billionaires list
- Social Media
  - Facebook
  - Twitter
  - Instagram
  - Location based Check ins (foursquare)
  - Linkedin
PHONE ATTACK

- Everything is tied to the phone
  - Locating business that use it
  - Wait
  - Bring recording device
  - Profit....
- Attacking Companies
  - Subdomain (Dorks)
  - Basic employee recon (Socmint)
  - Public record (Employee and Company)
  - Court Doc Search (C level and Business)
  - Vulnerable system (Censys and Shodan)
  - C level search (Deep Dive for Shadows)
ATTACKER PATH

- Pastebin
  - Bots that scrape pastebin:
    - @leak_scavenger
    - @pastebinleaks
    - Pastebin searches
  - Automating the process - IFTTT
- If an email, password or username is on multiple breaches...
- Medical Records
  - Drugs cost money
  - What do you want people not to know?
  - STD, Illness, genetic traits etc
ATTACKER PATH

- DeepDarkScaryFear Web
  - Data breaches
  - Most of this intel is going to be online in clear web
  - If you are on the Darkweb anyway, pay someone to do the heavy lifting
• Namibia
  • Turning waste water into drinking water
  • No other source of water in the area
  • Been doing this for over 50 years
  • What if we told them we could take it away? (IoT)
Contact

Wingoc or Windhoek Goreangab Operating Company
(Pty) Ltd
P.O. Box 2103
Windhoek
Namibia

<table>
<thead>
<tr>
<th>Thomas Honer</th>
<th>Siegfried Mueller</th>
<th>Rene Mertens</th>
</tr>
</thead>
<tbody>
<tr>
<td>General Manager</td>
<td>Technical Manager</td>
<td>Operations Manager</td>
</tr>
<tr>
<td><a href="mailto:thomas@wingoc.com.na">thomas@wingoc.com.na</a></td>
<td><a href="mailto:sgi@wingoc.com.na">sgi@wingoc.com.na</a></td>
<td><a href="mailto:renem@wingoc.com.na">renem@wingoc.com.na</a></td>
</tr>
</tbody>
</table>

Phone number
+264(0)61272083

www.citescada.tk
2a02:4780:dead:bae8::1
- **Time**
  - What will you hold valuable in 5 years, 10 years 15 years?
  - Where will you be?
  - Will you be making more money? Own more property? Have more systems online?
  - Remember you are just another line of code to the webscrapers…
PREVENTION
STOPPING AN ATTACK BEFORE IT STARTS
What are you worth to an attacker?
- Physical Value
- Digital Value
- Professional Value (also Future Value)
Why is this important?
- You cannot build a fence without knowing your property lines
- What are your vulnerable surfaces?
- Who is leaking all your data?
PREVENTION

- Start to flex the muscle
  - Google Voice
  - Sudo (coming soon for Android?)
  - Sideline/Burner/FLYP
PREVENTION

- Social Media Accounts
  - Determine the level of oversharing
  - Make sure you are assisting others
  - Make sure the privacy setting are at least up to date
PREVENTION

- Disinformation
- Love the lie...
- Number of marketing sites will help you
- Flex the muscle, don’t break the law
THANK YOU

5150RESEARCH@PROTONMAIL.COM