The Dark Web and Why You Should Care

This Briefing is Proprietary and Competition Sensitive
What is the Dark Web

• The “Dark Web” is a part of the world wide web that requires special software to access.

• Much like the internet, the Dark Web is a network of websites, forums, and communication tools like email.

• What differentiates the Dark Web from the internet is that users are required to run a suite of security tools that help anonymize web traffic.
The Dark Web

• Though the name sounds ominous, the Dark Web did not hatch from some evil hacker lab.

• The Dark Web is simply a network of websites that require basic encryption technologies to be enabled before users can load content.

• These are the same technologies that protect passwords when users log on to bank portals and sites like Gmail and Facebook
What’s the Big Deal?

However……

- The Dark Web is used for both nefarious and reputable purposes.

- Criminals exploit the network's anonymity to sell
  - Personal Information
  - Banking information
  - Corporate information / access
  - Guns
  - Drugs
  - Human Trafficking
Examples of What is Sold

- Social Security number: $1
- Credit or debit card (credit cards are more popular): $5-$110
- Online payment services login info (e.g. Paypal): $20-$200
- Loyalty accounts: $20
- Subscription services: $1-$10
- Diplomas: $100-$400
- Driver’s license: $20
- Passports (US): $1000-$2000
- Medical records: $1-$1000*
- Customized Exploits - Varies
- A recent study by Carnegie Mellon researchers Soska and Christin has calculated that drug sales on the dark net total US$100M
• Consider the Ashley Madison hack. Vast amounts of account data, including real names, addresses and phone numbers ended up on the Dark Web.

• Exploits and attack code are complex to build from scratch. The dark web provides a marketplace that connects programmers with the needed skills with those with motivations to unleash them.

• Dr0p1t-Framework, a trojan that downloads other malware, and the Silent Word exploit, which converts a malicious .EXE file into an innocent-seeming .DOC or sale.
• Buyers of these exploits don't need to be master hackers themselves. There are guides on how to spread your malware, and also phishing and carding tutorials.“

• Dark Web paying corporate workers to leak info or for access
  – *staff at an unnamed bank were found to be helping hackers maintain a persistent presence on their corporate networks.*
Control Systems

• Control Systems (ICS, OT, SCADA) are used to run facilities like nuclear power stations, oil refineries and chemical plants, building automation, manufacturing and even airplanes so if cyber-criminals gained access to these networks, then the consequences could be lethal.
What’s on the “ClearNet” - Shodan Tool

• Simple search for devices running Modbus that are connected to internet in U.S.
Just found A Device

- Default credentials passwords
Known Data Breaches

• Known breaches
  – Equifax
  – Target
  – Macy’s
  – Atlanta city government systems down due to ransomware attack
  – Oregon tax agency employee copied personal data of 36,000 people
  – Kansas Department for Aging and Disability Services Notifies 11,000 Consumers About Breach of Protected Health Information
  – Officials: 2 ex-Florida Hospital employees stole, sold patient records

• And the lists goes on and on
How Do We Protect

• The bad guys know and are trained on current defensive tools and strategies

• Must be better than they are
  – Faster, Outside the Box thinking and solutions

• Machine Learning defensive solutions for companies

• Understand your “Digital Footprint” and do things to minimize it
Questions