LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF INFORMATION SECURITY

The Dark Web and Cybercrime

07/23/2020

Report #: 202007231300

Agenda

- Dark Web Background
  - What is the Dark Web?
  - What is Tor?
  - Is the Dark Web Synonymous with Crime?
  - What Kind of Criminal Activity Occurs on the Dark Web?
  - What Sites Exist on the Cybercriminal Dark Web?
  - Forums vs Markets
  - The Life Cycle of Stolen Data
- Case Study
  - Incident Overview
  - Site Overview
  - Actor Overview
  - Incident Timeline
  - Sample Data Overview
  - Incident Takeaways

Slides Key:

Non-Technical: managerial, strategic and high-level (general audience)

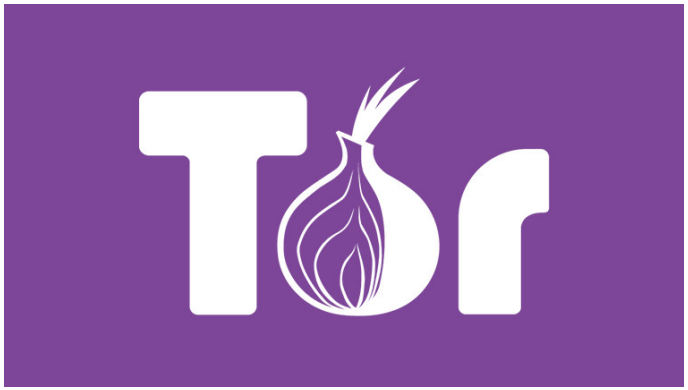
Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

What is the Dark Web?

- Technically, overlay networks that use the Internet and require specific software or credentials to access.
- Surface web: indexed by Google, does not require special software or credentials to access
  - HHS.gov
- Deep web: not indexed by Google, requires special software or credentials to access:
  - HHS's internal SharePoint, a bank account portal
- Dark web: requires Tor Browser, may require additional credentials, all Tor urls end in .onion
  - Dread (dark web forum), dreadditevelidot[.]**ONION**
  - **Note: do not attempt to visit this site on a corporate network**

What is Tor?

- Created by the U.S. Naval Research Lab in 1995
- The Tor Project (nonprofit) created in 2006
- Privacy focused internet browsing and site hosting
- Route traffic through multiple nodes and encrypt at every step of the way
  - Layers of encryption are compared to an onion, hence **T**he **O**nion **R**outer and the top level domain **.onion**



Is the Dark Web Synonymous with Crime?

- Many people use the dark web for totally legitimate reasons – political dissidence, private communication, etc
- Many people also use the dark web because of the cybercriminal communities that thrive there
  - Silk Road (and Silk Road 2.0, 3.0, etc), Alphabay, Hansa, Dream, etc
- Many of those cybercriminal communities also use surface web sites or other privacy focused hosting solutions (I2P, etc.)
  - Colloquially, “the dark web” sometimes refers to cybercriminal communities that use these other methods
  - For example, some security researchers would consider the surface web (.com) site Raid Forums or RAID to be part of the dark web even though it is not a .onion

What Kind of Criminal Activity Occurs on the Dark Web?

- Famous for narcotics
  - While many of the most famous dark web marketplaces were primarily drug marketplaces, these sites are not particularly relevant for our purposes
  - The exception may be pharmaceutical sales, which can be addressed in a later presentation
- Huge ecosystem for payment card fraud and identity theft
  - Sites that exist only to sell payment cards often have thousands to millions of cards in stock
  - Many of these sites also sell “fullz” or full identity packs for identity theft purposes
- Cybercrime and “Cybercrime-as-a-Service”
  - Economy of tools/raw supplies to commit cybercrime
  - Spinoff services of experts act as “hackers for hire” for less experienced actors

https://www.bbc.com/news/technology-22381046, https://acwi.org/2018/12/06/credit-card-fraud-sees-resurgence/, https://affant.com/cybercrime-as-a-service-goes-mainstream/

What Sites Exist on the Cybercriminal Dark Web?

- Focus on forums and marketplaces
- Both sites may have different barriers to entry
  - Invite only
  - Particular nationality/political alignment (Commonwealth of Independent States -aligned)
  - Entry price
  - Must be vouched for
  - Provide proof of crimes committed
- May focus on drugs/contraband or stolen data/cybercrime/fraud, but generally not both

Forums vs Markets

Forums

- May be used to coordinate sales, no ecommerce function
  - Difficult to track sales
- Discussion focused
- Share wisdom, tactics, techniques, and procedures, etc
- Community-led discussion

Marketplaces

- Ecommerce site similar to those you might find on the surface web
  - Buyers can rate sellers
  - Site generally has escrow system
  - More susceptible to shutdown due to exit-scamming or law enforcement action
- May have a partner forum for discussion or internal message function

Dark Web Cybercrime Culture

- Scams – between users, between users and site administrators, between buyers and sellers – abound
- Credible accusations of scamming or “ripping” can result in bans and ostracization
- Site admission policies and reputation points are used to keep bad actors out of sites and evaluate the behavior of users on specific sites
- Actor establish personas across long periods of time and multiple sites to show their credibility
- Networks of actors across sites can distribute stolen data widely

The Life Cycle of Stolen Data

- Stolen data tends to filter down through communities, eventually landing in open forums or large marketplaces
- Data is sold and resold, traded and retraded, repackaged, many times
- One potential life cycle
  - Traded between close associates or sold to known buyers
  - Posted for sale in closed forums with high barriers to entry
  - Posted for sale in closed forums with lower barriers to entry
  - Posted for sale on multi-good marketplaces
  - Posted for free on forums
  - Posted for free on paste sites

https://www.lokad.com/supply-chain-management-definition

Section Takeaway

Security researchers use context about sites, actors, and markets to evaluate and respond to content on these sites.

Incident Overview

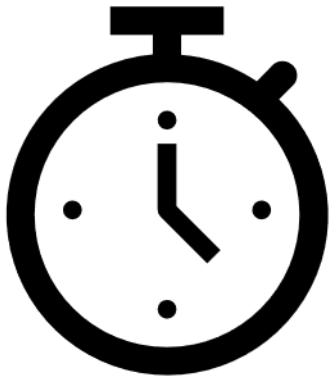
What Happened:

On May 6, 2020, Raid Forums user greenmoon2019 posted in the site's sample section an unlockable link to 100,000 medical records with dates of birth (DOBs) and a specific medical identifier number linked to a healthcare entity. On May 11, 2020, the entity confirmed that this dataset did not contain valid data. On May 13, the actor removed the post.

Why Does It Matter:

This incident illustrates several key principles that can be applied in future incidents (and when live data does appear)

1. **Cyber criminals may not accurately identify data**
2. **Understanding the site, actors, and context matters**
3. **Quick incident response – and teamwork – make a difference**



Site Overview

Raid Forums (RAID)

- Surface web underground hacking forum
- Founded in 2015
- Hosts discussion of hacking topics, advertisements and solicitations of leaked or cracked databases, and provides a master list of all data shared on the site
- No ecommerce functionality, although vendors use the site's private message features to coordinate sales
  - Not clear what has been sold or who buys it
- Semi-public
  - Some parts of the site can be accessed without creating a free account
  - Registering with the site unlocks some content
  - Site credits unlock stolen datasets and can be purchased from the site directly or earned through posting and commenting
- Low barrier to entry
- Reputation points:
  - interactions with other users
  - Positive reputation: hundreds to thousands of points
  - Negative reputation may result in a ban

Above: Raid Forums Logo

Actor Overview

Threat Actor greenmoon2019

- Joined RAID on January 5, 2019
- Internal and external analysts assess this actor's reliability as a "B" – usually reliable.
- On May 6, 2020 had 254 reputation points
  - Posts generally well received
  - No forum members had accused this actor of scamming or "ripping."
  - No identified profiles or aliases of this actor on other surface or dark web sites.
- History of posting free samples of databases
  - Mostly not healthcare/HPH related
  - Two that were HPH related (addressed on next slide)
- Previously sought or sold phone, mortgage, and other consumer records for residents of U.S., Canada, New Zealand

Actor Overview (continued)

Threat Actor greenmoon2019

- History of posting free samples of databases, including two HPH databases in September 2019
- Actor posted 100,000 records from a “Premium Health Insurance Long form database… Total 4 Million Data available.”
    - This actor advertised the dataset as containing the following fields: "IP_Address","INCOMENUMBER","Number_Of_Applicants","First_Name","Last_Name","Address","City","State","Zip","Email","Day_Phone","Household_Income","Household_People","Gender","DOB","Height_Feet","Height_Inches","Weight","Age","Pregnant","Health_Conditions","Tobacco","Currently_Covered","Coverage_Denied","Currently_Employed","Insurance_Company","Conditions","Diabetic","Hospitalized_Last_5_Years","Prescription_Medication","Employment_Status","Spouse_Gender","Spouse_Height_Feet","Spouse_Height_Inches","Spouse_Weight","Spouse_DOB","Spouse_Health_Conditions","Spouse_Conditions","Child_1_Gender","Child_1_Height_Feet","Child_1_Height_Inches","Child_1_Weight","Child_1_DOB","Child_1_Health_Conditions","Child_1_Conditions","Child_2_Gender","Child_2_Height_Feet","Child_2_Height_Inches","Child_2_Weight","Child_2_DOB","Child_2_Health_Conditions","Child_2_Conditions","Child_3_Gender","Child_3_Height_Feet","Child_3_Height_Inches","Child_3_Weight","Child_3_DOB","Child_3_Health_Conditions","Child_3_Conditions","Child_4_Gender","Child_4_Height_Feet","Child_4_Height_Inches","Child_4_Weight","Child_4_DOB","Child_4_Health_Conditions","Child_4_Conditions","Child_5_Gender","Child_5_Height_Feet","Child_5_Height_Inches","Child_5_Weight","Child_5_DOB","Child_5_Health_Conditions","Child_5_Conditions","Spouse_Tobacco","Child_1_Tobacco","Child_2_Tobacco","Child_3_Tobacco","Child_4_Tobacco","Child_5_Tobacco","Dental_Term_Length","Health_Policy_ID","Vision_Policy_ID","Dental_Policy_ID","Agent_Disposition","State2","Income2","Ehealth_Income","Email_OptIn","household_income_revalue","Qualifying_Life_Event_Type"

Actor Overview (continued)

Threat Actor greenmoon2019

- Actor also posted a 100,000 record sample of “US Ailment data.”
  - Ailment databases allow threat actors to target individuals with certain medical conditions
  - The data lists consumer PII alongside any aliments or medical conditions the individual suffers from.
  - This data was allegedly of the format: (Header: FirstName,LastName,Address,City,State,Zip,Gender,Age,Phone,Ailment).
- Other users praised the quality of both datasets
- On May 14, 2020, actor posted an advertisement for 21 U.S. and Canadian consumer databases, including datasets above
  - Claims that the databases are “exclusive and cleaned.”
  - This could indicate that, while users downloaded the 100,000 samples provided on previous posts, the actor has not successfully sold the complete databases to any buyers.

Incident Timeline

May 6
- Actor posts advertisement for medical data on RAID

May 7
- Analysts discover RAID post
- Begin internal investigation by alerting affected entity

May 8
- Sample of 100,000 records downloaded and sent to affected entity for analysis

May 11
- Affected entity confirms that the data is not valid

May 13
- Actor removes advertisement and sample data from RAID following criticism from multiple users about data quality

May 14
- Actor posts advertisement for 21 databases, including Health Insurance Long Form database and Ailment list

Sample Data Overview

- Original post provided five sample records for free, with 100,000 sample records available to download in exchange for eight site credits
- Format: phone1 firstname lastname address1 city state zip email dob gender primarypolicy primarypolicynumber
- Analysis of the 100,000 downloaded records revealed:
  - Data included entity-specific identifier numbers
    - The affected entity identified 4,078 valid identifiers, but only six identifiers accurately matched to the correct last name.
    - The six records with matching identifiers and surnames include relatively common surnames: Adams, Allan, Harrison, Murphy, Smith, and Williams.
    - No other demographic data associated with the record matched. These matches were false positives rather than indicators of valid records.
    - Analysts did not identify valid identifiers for 95,933 records.
  - Several identifier numbers contained characters that the affected entity confirmed do not appear in valid identifiers.
- Comparison of records against open sources identified actual individuals that fit the demographics of the alleged data
  - These records did not contain valid identifiers

Incident Takeaways #1

Cyber criminals may not accurately identify data

- This actor claimed that they acquired the fake data from a third party reseller
  - Stolen data is a commodity market
  - Reselling is common and follows a “trickle down” pattern
- While it appeared to be data from this healthcare entity – and may have been actual data of American citizens – it didn’t stand up to scrutiny
- Do not assume that an actor knows the origin of stolen data

Incident Takeaways #2

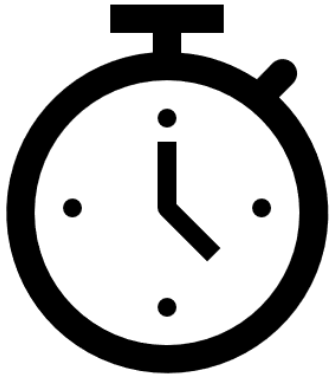
Understanding the site, actors, and context matters

- Familiarity with the standards and etiquette of a site provides context to posts
  - The higher the barrier to entry of a site, the more likely information is to be legitimate (or that the actor *believes* it is legitimate)
  - Heavily moderated sites are less likely to host scammers
- Identify other aliases and past behavior of the actor
  - Is the actor active on other related sites?
  - What is the actor's reputation?
  - How long has the actor been a member of this site?
  - Has the actor previously posted similar content?
- Other context can be helpful when evaluating an incident or threat actor
  - Repeat interactions with other users
  - Credible accusations of scamming or "ripping"
  - Repeat interactions with moderators or other authority figures

Incident Takeaways #3

Quick incident response – and teamwork – make a difference

- Ability to verify is important
  - Because analysts were able to work with the affected entity and provide data quickly, the affected entity was able to identify the data as fake
  - While evaluating context is important, all data should be treated as genuine until proven otherwise
- Post was removed without incurring media attention or panic
- Threat actor can be monitored going forward



Reference Materials

References

- The Untold Story of Silk Road, Wired
  - https://www.wired.com/2015/04/silk-road-1/
- Stolen credit card info on the dark web tripled in 6 months, Yahoo
  - https://www.yahoo.com/now/stolen-credit-card-info-on-the-dark-web-tripled-in-6-months-171720889.html
- The Tor Project
  - https://2019.www.torproject.org/index.html.en
- Cybercrime-as-a-Service Economy: Stronger Than Ever, BankInfoSecurity
  - https://www.bankinfosecurity.com/cybercrime-as-a-service-economy-stronger-than-ever-a-9396

Questions

Questions

Upcoming Briefs

- Securing 5G (20AUG20)

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to **HC3@HHS.GOV** or call us Monday-Friday, between 9am-5pm (EST), at **(202) 691-2110.**

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback. If you wish to provide feedback please complete the HC3 Customer Feedback Survey.

HC3 Customer Feedback

Disclaimer

These recommendations are advisory and are not to be considered as Federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. HHS does not endorse any specific person, entity, product, service, or enterprise.

About Us

HC3 works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector

Products

Sector & Victim Notifications

Directed communications to victims or potential victims of compromises, vulnerable equipment or PII/PHI theft and general notifications to the HPH about currently impacting threats via the HHS OIG

White Papers

Document that provides in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience.

Threat Briefings & Webinar

Briefing document and presentation that provides actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics.

Need information on a specific cybersecurity topic or want to join our listserv? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at (202) 691-2110.
Visit us at: www.HHS.Gov/HC3

Contact

www.HHS.GOV/HC3

(202) 691-2110

HC3@HHS.GOV