How I Found Your Password, and Other Advanced Data Hoarding Techniques

Recon Village, DEF CON 31

Introductions

M4x 5yn74x

unixnerd

Wall of Disclaimers

- The opinions expressed within this presentation do not reflect the opinions of our employers.
- The topics covered in this talk can get you in trouble. So, proceed with caution.
- The tool released during this talk is intended for security professionals and is for research and educational purposes only.
- The presenters of this talk, and their associated organizations relinquish all responsibility for any misuse of this research.
- We do not condone any monetary exchange for acquiring breach data.
- We are not lawyers! Consult your legal council for legal advice. Not us!

Agenda

- Opening Statements
- Breach Data
- Law & Ethics
- Search Engine Discussion
- Tool Release
- Demo
- Conclusion

Opening Statements

Addressing the elephant in the room…

Our aim is to dispel misinformation and normalize breach data research for security professionals.

Questions

- How many of you know what breach data is?
- How many of you use breach data in one form or another?

Breach Data

What is it?

Breach data is any data that was intended to remain private/secret but was leaked through some form of compromise.

What does it contain?

Breach data comes in all shapes and sizes

- Database dumps
- Credentials
- PII/ePHI
- Credit Card Numbers
- Etc…

Breach Data
(continued)

Examples from the news:

- The Office of Personnel Management Leak
- The Ashley Madison Leak
- DOD Fitness Tracker GPS Data Leak
- Shanghai Police Database Leak

The list of breaches isn't getting any shorter…

It keeps going on and on…

and on…

Breach Data
(continued)

Who uses Breach data?

In short, everyone!

- Blackhats
- Whitehats
- Script Kiddies
- Scammers
- Private Investigators
- Law Enforcement
- Military
- Nation States
- Threat Actors
- Etc…

Breach Data
(continued)

Where does breach data end up once its been leaked?

Breach data doesn't just go away as fast as the news cycle does…

It ends up on deep and darkweb markets for sale.

The darkweb is not just some magical void where stolen things end up.

People steal things
These things are kept “safe”
Usually in the hands of the thieves

…sometimes on a PasteBin near you 😉

Breach Data
(continued)

Either way, leaked data ends up in the hands of someone.

And they pursue their own interests with it.

- Financial Gain
- Clout
- Political Motives
- Intelligence Gathering
- Etc…

Breach Data
(continued)

Eventually, much of it makes its way onto the capital "**I**" **Internet**.

Over time breach data eventually finds it's way into the public domain.

Or it's just leaked directly to the public.

What was ***PII***, becomes ***OSINT*** data.

Breach Data
(continued)

Is breach data valuable?

YES!

- Sold on the darkweb
- Carding
- Identity Theft
- Scamming
- Etc…

Breach Data
(continued)

Is there any value to it other than financial gain?

It depends on motive.

- Hacktivism
- Gathering Intelligence
- Marketing Research
- Etc…

Breach Data
(continued)

Why is breach data valuable to security researchers?

- Adversarial Simulation
- Credential Reuse
- Profiling Targets
- Generating realistic password lists
- Illustrating Impact
- “The Pucker Effect”

Breach Data
(continued)

How long is it valuable?

- Leaks are timely.
  - Does anyone know there was a leak?

What's vulnerable today might not be vulnerable tomorrow.

So, is old breach data still valuable?

YES!

Generally speaking,
humans are terrible at security.

Breach Data
(continued)

Breach data can be too valuable...

- Shadow Brokers NSA Leak

Either way, as breach data ages, Eventually, much of it gets handed around freely on the Internet.

Breach Data
(continued)

As security professionals, should we use breach data?

YES!

- Breach data is beyond "Low hanging fruit"

If we don't use breach data, we are doing a gross disservice to our clients.

Law & Ethics

Considering the origins of breach data, is this legal?

Well, it is...

&&

it isn't...

It's illegal with misuse and if you don't have justification.

It's legal based on intention and proper justification.

Law & Ethics
(continued)

But isn’t breach data publicly available?

YES!

But so are a lot of things!

- Default passwords
- Keyed Alike Systems:
  - (1284X, FEOK1, 16120, 222343, Etc…)
- Personal Information
- PoC Exploits for N-day Vulnerabilities
- Etc...

Just because you have the capability to attack something, should you?

This depends on scope and ethics.

Law & Ethics
(continued)

A lot of breach data is for sale too...

We do not condone any monetary exchange for acquiring breach data.

Adhere to your moral convictions

Unless your ethical framework is "Don't get caught”…

-- We're lookin’ at you alphabet boys…

Law & Ethics
(continued)

When should you approach legal?

Determine your needs for using breach data.

Consider the risk and impact to yourself (most importantly), your company, employees, and clients if you do/don't.

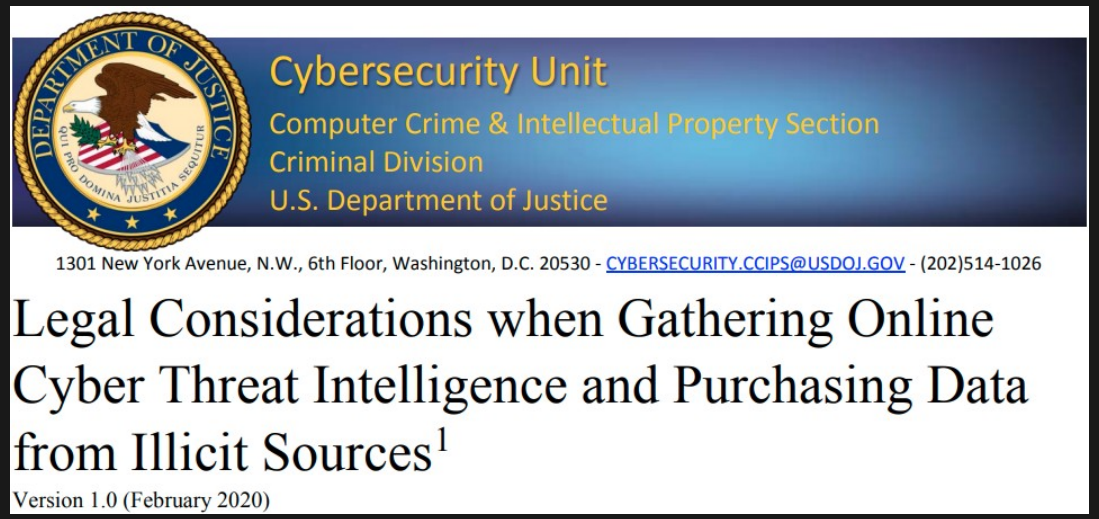
Do your own research.

That's what we did…

And we discovered something important!

Law & Ethics
(continued)

Did you know that the DOJ has public guidance around how to legally handle breach data?



Cybersecurity Unit
Computer Crime & Intellectual Property Section
Criminal Division
U.S. Department of Justice

1301 New York Avenue, N.W., 6th Floor, Washington, D.C. 20530 - CYBERSECURITY.CCIPS@USDOJ.GOV - (202)514-1026

Legal Considerations when Gathering Online Cyber Threat Intelligence and Purchasing Data from Illicit Sources[1]

Version 1.0 (February 2020)

Reference:
https://www.justice.gov/criminal-ccips/page/file/1252341/download

Law & Ethics
(continued)

Quotes from the DOJ:

“If a practitioner does not intend to use information obtained on a forum to commit a federal criminal violation, asking questions or soliciting advise on a forum is unlikely to constitute as a crime.”

“… assumes the practitioners obtain information solely so that it can be used and shared for legitimate cybersecurity purposes (e.g., to help others identify and defend against cybersecurity threats) and with no criminal or malicious intent or motive.”

Reference:
https://www.justice.gov/criminal-ccips/page/file/1252341/download

Law & Ethics
(continued)

Going to Council

- Come up with a plan based on the guidance outlined by the DOJ and your specific needs.
- Consult your executive leaders and legal team.
- Draft an official charter document that outlines the specifics in detail.
- Resolve any feedback based on legal council discussion.
- Finalize the initiative.
- Hurry up and wait...
- PWN'd!

Questions

- How many of you already had legal policy in place for handling breach data before this talk?
- How many of you will now?

Search Engine Discussion

- How many of you use the Internet?
- How many of you use a search engine?
- How many of you ***used to*** use Google?
- How many of you **still** use Google?
- What about other search engines?
- What do you use?

Search Engine Discussion
(continued)

There are far too many search engines out there to mention here…

But we've come to find that we really love ***SearXNG***!

SearXNG

Search Engine Discussion
(continued)

SearXNG is a…

- Privacy Focused
- Self-Hosted
- Hackable...
- Meta-Search Engine
- That supports 138 different search engine services

That's cool right?

SearXNG

Search Engine Discussion
(continued)

But we're hackers…

We *like* control…
But we **LOVE** root…

We *like* privacy…
But we **LOVE** anonymity…

We like to push things to their limits…

Search Engine Discussion
(continued)

But above all…

Information should be Free...
Right?

"**Free**" as in ***Freedom***;
Not "**Free as in *Beer***"

But we'll take the **beer** too!! 🍻

Introducing *DorXNG*

DorXNG is one-part custom tool, one-part modified ***SearXNG*** **Docker** container.

Multi-threaded search queries are routed over the **Tor** network with a ten second circuit refresh rate.

The resulting search results are stored in a SQL database.

We have also disabled ***SearXNG***'s client-side search request error timeout features.

These configuration settings allow for evading search engine restrictions commonly encountered while issuing many repeated requests.

DorXNG
(continued)

In closing before we demo the tool.

Please **DO NOT** use the ***DorXNG*** client application against any public ***SearXNG*** instances.

Our tooling is not meant for traditional ***SearXNG*** instances.

They do not have the customizations we have implemented.

And the last thing we want to do is piss off that amazing community!

```
➜ DorXNG ./DorXNG.py -q 'intitle:news breach data' -c8 -n64
```

```
Next Generation DorX. Built by Dorks, for Dorks. 🤓

Latest data breach news | The Daily Swig - PortSwigger | https://portswigger.net/daily-swig/data-
Data breaches - BBC News | https://www.bbc.co.uk/news/topics/c0ele42740rt
Latest Data Breach news - Bleeping Computer | https://www.bleepingcomputer.com/tag/data-breach/
data breach | Breaking Cybersecurity News - The Hacker News | https://thehackernews.com/search/la
Breaches and Incidents | Cyber Security News Today - Cyware | https://cyware.com/category/breache
Data Breach | News, Videos & Articles | https://globalnews.ca/tag/data-breach/
Data Breaches | Latest News, Photos & Videos | WIRED | https://www.wired.com/tag/data-breaches/
Data Breach - latest news, breaking stories and comment | https://www.independent.co.uk/topic/dat
Latest News & Videos, Photos about data breach | https://economictimes.indiatimes.com/topic/data-
Siemens and UCLA say data compromised in MOVEit data breach | https://www.reuters.com/technology/
Personal data of millions of Americans exposed in global cyber attack ... | https://www.tomsguide
USDA is investigating a 'possible data breach' related to global ... | https://www.cnn.com/2023/0
Biggest Healthcare Data Breaches Reported This Year, So Far | https://www.healthitsecurity.com/fe
MOVEit data breach: 45,000 NYC students among victims | https://ny.chalkbeat.org/2023/6/23/237720
Cyberattack exposes sensitive data on NYC public school students, staff ... | https://abc7ny.com/
Siemens and UCLA Say Data Compromised in MOVEit Data Breach | https://www.insurancejournal.com/ne
Hackers steal data of 45,000 New York City students in MOVEit breach | https://www.bleepingcomput
Progess Software Faces More Lawsuits Over MOVEit Data Breach | https://news.bloomberglaw.com/priv
Data Breaches News and Articles - Infosecurity Magazine | https://www.infosecurity-magazine.com/c
Millions of Americans' personal data exposed in global hack - MSN | https://www.msn.com/en-us/new
MOVEit breach: Harris Health patient, employee information exposed in ... | https://abc13.com/mov
The Nation's Two Biggest Pension Systems Report a Data Breach | https://www.governing.com/securit
Recruitment portal exposes data of US pilot candidates | https://www.theregister.com/2023/06/26/a
Top 10 cybersecurity findings from Verizon's 2023 data breach report | https://venturebeat.com/se
Maryland agency, Johns Hopkins University affected by data breach | https://www.heraldmailmedia.c
Cybercrime thrives during pandemic: Verizon 2021 Data Breach ... | https://www.verizon.com/about/
Cyberattack impacts U.S. federal government, NATO allies. Here's what ... | https://www.cbsnews.c
Early-2023 T-Mobile Data Breach Sparks Class Action | https://www.classaction.org/news/early-2023
Data Breaches 101: How They Happen, What Gets Stolen, and Where It All ... | https://www.trendmic
You Could Be Owed $5,000 After 2020 Data Breach - Yahoo Finance | https://finance.yahoo.com/news/
Latest breaking news articles on data security breach - DataBreachToday | https://www.databreacht
Here's what to do after huge Louisiana OMV data breach | News - NOLA.com | https://www.nola.com/n
News - Garante Privacy | https://www.garanteprivacy.it/news-e-comunicazione/news
MoveIt hack: What action can data-breach victims take? - BBC | https://www.bbc.com/news/technolog
Data breaches - BBC News | https://www.bbc.com/news/topics/c0ele42740rt?page=5
data breach - Singapore - CNA | https://www.channelnewsasia.com/topic/data-breach
Data protection - BBC News | https://www.bbc.co.uk/news/topics/cwz4lvzgq9gt
MoveIt hack: What action can data-breach victims take? - BBC | https://www.bbc.co.uk/news/technol
data breach - Singapore - Today Online | https://www.todayonline.com/topic/data-breach
data breach news - The Indian Express | https://indianexpress.com/about/data-breach/
Cyber security news headlines - 9News | https://www.9news.com.au/cyber-security
Latest News, Photos, Videos on Data Breach - NDTV.COM | https://www.ndtv.com/topic/data-breach
Listening | Data Breach - Breaking News English | https://breakingnewsenglish.com/1803/180327-dat
Data-breach News - CNBCTV18 | https://www.cnbctv18.com/tags/data-breach.htm
```

DorXNG

(demo)

Lessons Learned

Policy sucks…

But somebody's gotta do it…

Your intention matters.

International law is not US law.

Shit can still happen.

This is about having legal safeguards in place.

You could still get a knock on the door and actually have to prove your intent.

Above all, practice good **OPSEC, a**nd stay within the ethical guidelines you put in your policy.

Conclusion

We hope you enjoy our research!

Our research can be found here:

https://github.com/researchanddestroy/BDR

https://github.com/researchanddestroy/DorXNG

If you want to chat about our research, find us at the bar and buy us a beer! 🍻

Maybe we'll show you some stuff. 😉

Shout Outs!

In closing we'd like to shout out the developers of ***SearXNG*** and **Tor** for making this possible!

Please donate to both projects! <3

Shout out to all our mentors!

We love you all!

And finally, shout out to **Illuminati Party**!

You are our home away from home at **DEF CON**.

HACK THE PLANET!

Peace! ✌✌