Leak The Planet: Veritatem cognoscere non pereat mundus

Or How You Learned To Stop Worrying And Love The Leak

Emma Best, Distributed Denial of Secrets, She/Her
Xan North, Distributed Denial of Secrets, They/Them

Who We Are

Edalyn

Finito

Maurice

Moose

Little Snowden

Zoey

Humans that don’t matter

Bring back the pets

- Emma Best (she/they) - @NatSecGeek
- Brassy (they/them)
- Paul Galante (he/him) - @galanp02
- Lorax B. Horne (they/them) - @bbhorne
- Xan “Grace” North (they/them) - @brazendyke
- Oliver Shuey (he/him) - @olivershuey
- Milo Trujillo (he/him) – @illegaldaydream
- Beka Valentine (she/her)

Types of Leaks and Leakers

Leaking is as value neutral as pharmacology - it comes down to intent and application

- Insiders
- Hacktivists
- Spillage
- State-Affiliated Actors
- Ransomware

Insiders

Cognitive dissonance addresses itself through leaks

- Daniel Ellsberg
- Chelsea Manning
- Edward Snowden
- Reality Winner
- Natalie May Edwards
- Jóhannes Stefánsson

Hacktivists

Not all whistleblowers are insiders

(Shouldn’t we have put a stock photo of a backlit keyboard here?)

- RedHack
- Anonymous
- Jeremy Hammond
- Phineas Fisher
- ACABGang
- Cyber Partisans
- donk_enby

Spillage

When data falls off a truck on the information superhighway

- Accidental release of data
  - Typically result of user error
- Examples:
  - Heritage Foundation
  - Police aerial surveillance footage
  - GiveSendGo
- Services like Grayhat Warfare make misconfigured S3 buckets easy to find and search
- Many leaks are avoided by disclosure protocols

State-Affiliated Actors

You probably love them when they’re yours

- Sabu
- Maksym Popov
- CyberBerkut
- Guccifer 2.0
- DC Leaks
- IT ARMY
- Conti

Ransomware

The “double extortion” scheme has led to government exposés and real police reform

- Very little data of the data merits journalist or academic review, but there are gems:
  - Jones Day / Chicago City Hall
  - Metropolitan Police Department D.C.
  - Illinois Attorney General
  - Perceptics
- Some declared political stances following Russian invasion of Ukraine
- Financial motive means they can be hired by state-actors, e.g. Conti

Publication Models

CRYPTOME

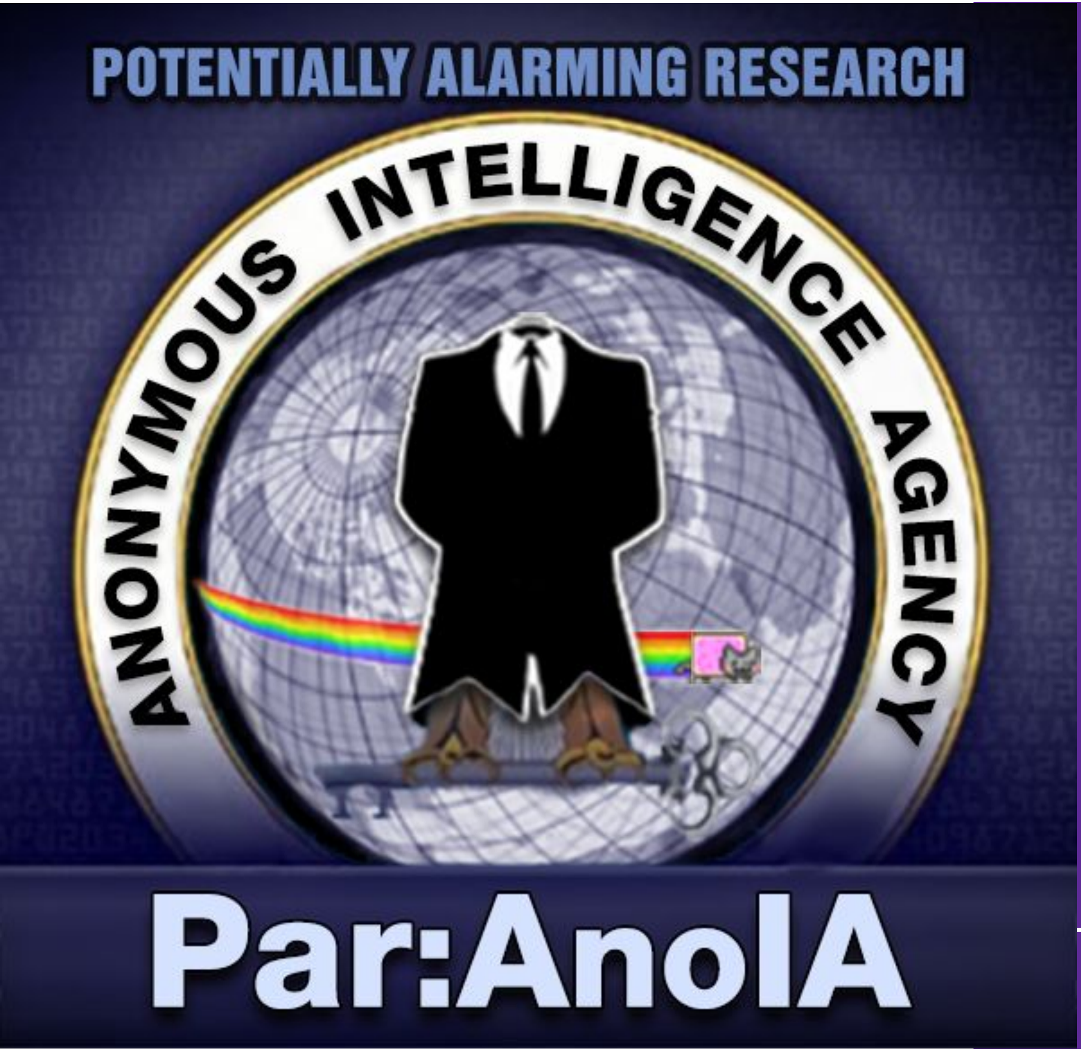
The Cypherpunks' Library

- Has published censored and leaked material online since 1996
- Basic HTTP listings, simple format
  - Previously used FTP
- Helped found WikiLeaks
- Criticizes everyone freely, was an early critic of WikiLeaks and leaked internal emails
  - Opposes extradition and prosecution of Assange
- Continues to be active

WikiLeaks

Wearing every hat;
until it wore none

- Revolutionary at times
- Sparked widespread debate and reform
- Used by Russian intel
  - Exchanged messages with and received DNC emails from Guccifer 2.0 persona
  - Appears to have received Podesta emails from DC Leaks persona
  - OPCW leak ties to Russia explored by Daily Beast, New Lines Magazine, and Bellingcat
- Seemingly inoperable for months at a time



- Anonymous’ answer to WikiLeaks, launched during a feud
    - Anonymous was frustrated by WikiLeaks’ slow releases
    - WikiLeaks accused Anonymous of insecure methods
    - WikiLeaks’ submission system offline
- “A simple, quick leak platform”
- Some release notes were highly inaccurate
- Used by Popov to launder data
- Active 2012-2013

The Intercept

Building journalism around leaks

- Launched to deal with and specializes in reporting on leaked data
- Made the Snowden archive (now closed) available to researchers
- Publishes reporting, not leaks
- Continues to be active and report on large leaks
  - Partners with regional outlets in some instances e.g. during the Russian invasion of Ukraine

The Consortium Model

ARIJ, EIC, Forbidden Stories, ICIJ, OCCRP

- #29 Leaks, FinCEN Files, Mining Secrets, Panama, Paradise & Pandora Papers, Pegasus Project, Tax Evader Radar
- Multiple news outlets collaborating on large projects, often with international reach
- Rarely publishes raw data, sometimes publishes relational data

DDoSecrets

Learning from the successes and mistakes of the past

- 4 years, 50+ countries, 200+ releases
- Balancing source protection with source transparency
- Separating editorial from source handling and data review & publication
- Entrusting local reporters, investigators, activists and experts with local data
- Different solutions for different datasets

DC Leaks

Persona and Access Management

- Some data was public, some was password restricted
- Vague American hacktivist persona, impossible to fact check
- Later linked to fake journalist personas
- Unclear and inconsistent ties to Guccifer 2.0 established publicly
- Links to Podesta emails

Guccifer 2.0

Selling The Narrative

- Persona launched to counter the revelation of Russian hacking of DNC et al
- Combination of blog and social media posts, individual documents and larger dumps
    - Some documents slightly altered
- ~15,000 messages with 1,200+ accounts, both press and public
- Managed by multiple people, often active nearly 24 hours a day

What Does State-Affiliated Look Like?

Popov

The Russian contractor who infiltrated Anonymous and the FBI

- Former FBI asset
- Russian contractor
- Involved in 2004/2005 FBI email hack
  - Paid $10,000 by FBI for it
- Numerous false personas
- Hack and leak of Ukrainian Prosecutor-General overlaps with CyberBerkut’s
- Financially motivated

Sabu

Anonymous member turned FBI asset

- FBI closely monitored and controlled him after his arrest
  - Sabu's activities were either allowed or directed, including:
    - Directing cyber attacks on foreign government and commercial systems
    - Orchestrating Stratfor hack and leak
    - Unwitting collaboration with Popov
- Foreign and domestic intelligence gathering for FBI
  - Not just a criminal informant

Popov and Sabu

When the lines blurred, they enabled each other

- Sabu and Par:AnoIA laundered Popov’s leaks
- Sabu offered Popov early access to Syria emails
- Popov and Sabu discussed using cyber attacks on government systems and false flag cyber attacks to “create real cyberwar”
- Popov gave Sabu targets, credentials and vulnerabilities

GUCCIFER 2.0

“These look very much like they’re from the Russians… [they] almost look too much like the Russians.” - Julian Assange

- Persona managed by Russian intelligence services
- Source of DNC emails
- Transcript shows communications with and submissions to WikiLeaks
- Used for dissemination and propaganda
- Guccifer 2.0 truthers persist despite overwhelming evidence

Free Civilian

The data merchant was a terrorist

- Claimed to sell data, but posted it freely
  - Ukrainian medical data, ~1 million government emails
- Used Cloudflare protected Swiss servers for distribution
  - Swiss servers (Private Layer Inc.) went offline
  - Cloudflare service continued
- Assessment:
  - Hack and leak psyop to create fear
  - Russian state-affiliated actors

Misidentifications

Case studies in failure and bad assumptions

- Sabu
  - But Agent Brutus says he was a hero,
    And Agent Brutus is an honourable man;
    He hath brought many captives home to Rome
- Popov
  - A con artist with too many fake IDs
- Phineas Fisher
  - For some, a vague coincidence transformed into an assumption
- donk_enby
  - The “only a state actor could do this” excuse

The Big Question

Are they, y'know..? 💅 (Spies?)

- Question is surprisingly broad
  - Source can be exploited
  - Material can be exploited
- Is it the right question?
  - A red flag, not an emergency shutdown
  - Soviet propaganda used to point out racism in the U.S. - **correctly**
- The first clue is usually the source
  - Are they trying to micromanage?
  - Can the source answer questions coherently and consistently?
  - Are they trying to sell a narrative?

The Big Question

Are they, y’know..? 💅 (Spies?)

- Timeline questions:
    - Does the situation/timing force your hand?
    - Relevant external events, e.g. elections, armed conflicts, etc.?
        - Is the goal to shed light or to intervene.
            - On behalf of who?
        - Is there time for counterbalances to take effect?
    - Why now?

The Next Big Question

How were they identified?

- Sabu
  - Chat logs
    - Sabu is caught attempting to entrap people
      - A bad idea to keep, but useful to have
  - Hacktivists communicating with each other
    - Patterns are noticed and shared with the community
  - Leaked files
    - Confirm allegations and what the FBI knew

The Next Big Question

How were they identified?

- Popov
  - Chat logs
    - Reviewed in hindsight
  - Extorting simultaneous targets
    - Stonewalled by Agent Hilbert’s refusal to cooperate
  - Footnotes of DOJ filings
  - Boasting to Carr
  - Russian operating environment

The Next Big Question

How were they identified?

- Guccifer 2.0 & DC Leaks
  - Chat logs
  - Money (BTC) trail
  - Linguistic analysis
  - Forensic analysis
    - Guccifer 2.0 once mistakenly logged in without a VPN
  - Analysis of files
    - Overlap between Guccifer 2.0 & DC Leaks
    - Russian metadata

The Next Big Question

How were they identified?

- Free Civilian
  - Inconsistent behavior
    - More interested in "proof" than in selling data
    - Posted 'already sold' data for "reputation"
  - Timing:
    - Data exfiltrated prior to wiper attacks
    - Timed to Russian invasion of Ukraine

What You Should & Shouldn’t Do Next

Newsrooms

Get ready for the next big leak now

- Invest in your ability to work with leaks - if you build it, they will leak
  - Staff
  - Technology
  - Training
- Take the long view
- A collaboration that makes the cut is worth two exclusives that get shelved
- There are no small stories, only small leaks

American newsrooms have trended toward the wrong column in the last year

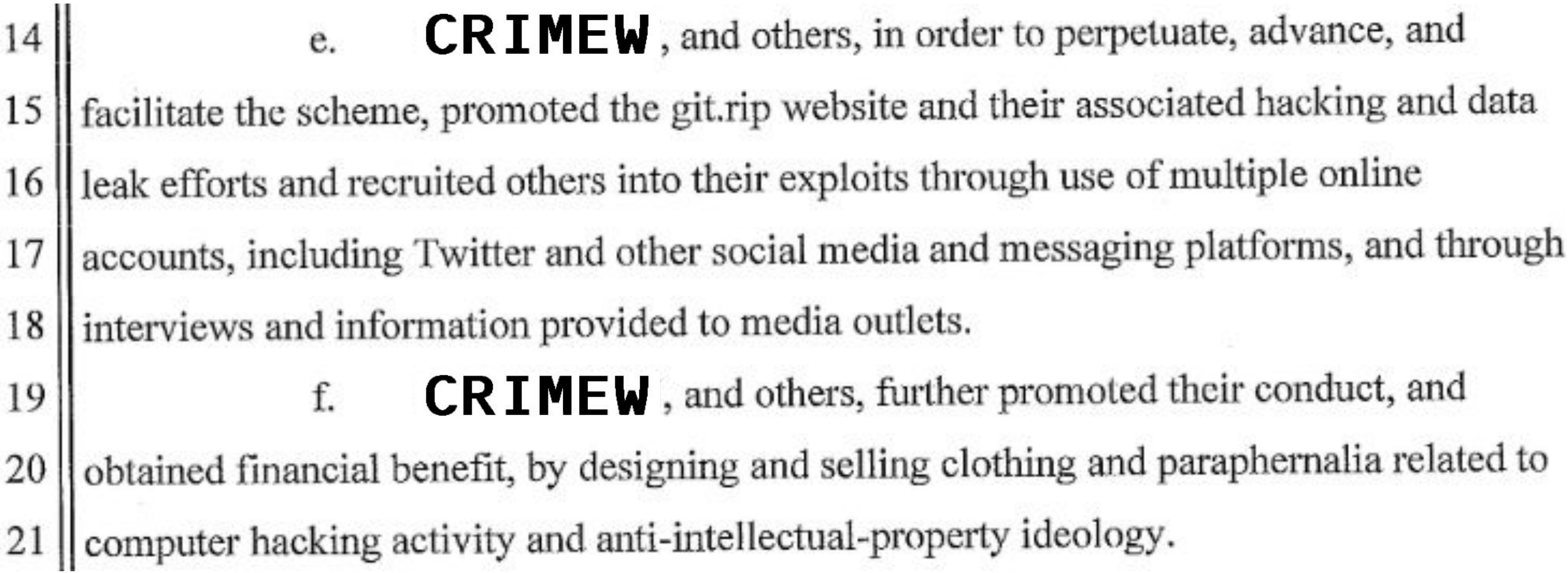
1) Reporting on fake hacks with no proof
2) Reporting on/promoting worthless NFTs
3) Making emotional headlines out of the opinions of inherently biased people
4) Focusing on recent **events** (recency bias)
5) Confusing **news** with **stories**
6) Investing in production

1) Reporting on the trial of the largest CIA leak in history
2) Following the money of NFTs
3) Informing people about what they need to know before they need to know it
4) Focusing on recent **information**
5) Reporting on non-breaking news that may not have closure, because it’s crucial data and **context**
6) Investing in the newsroom

Government

Come see the cognitive dissonance inherent in the system

- Don't just look to security - address the incongruences that cause & amplify leaks
- Communicate with the public better
- Everyone is very impressed with the size of your, um, legal case against Assange - now drop the publication charges
- Pardon all whistleblowers
    - Punitive action is counterproductive



e. CRIMEW, and others, in order to perpetuate, advance, and facilitate the scheme, promoted the git.rip website and their associated hacking and data leak efforts and recruited others into their exploits through use of multiple online accounts, including Twitter and other social media and messaging platforms, and through interviews and information provided to media outlets.

f. CRIMEW, and others, further promoted their conduct, and obtained financial benefit, by designing and selling clothing and paraphernalia related to computer hacking activity and anti-intellectual-property ideology.

Never let anyone hear you say talking to journalists and selling t-shirts is part of a CFAA violation again. Ever. ***Ever***.

Industry

Own your shit

- Stop blaming everything on state sponsored hackers
- Take shit more seriously than security theater
- The buck stops with everyone
- Be someone who isn’t worth leaking
- Never pay the ransom

Leakers and Leak Publishers

Leak The Planet,
Save The World

- Study mosaic theory
- Stay focused on results, not splash or ego
- Learn what the law does and doesn’t let journalists do
- Understand that state-actors can and will look to exploit you and your leaks - whether you want them to or not
- Talk to a lawyer, listen to your conscience

~~Rambling~~ Conclusion

References

- https://ddosecrets.com/wiki/About#The_Team
- https://www.databreaches.net/heritage-foundation-confirms-that-breach-was-a-leak-not-hack/
- https://www.wired.com/story/ddosecrets-police-helicopter-data-leak/
- https://www.dailydot.com/debug/givesendgo-sensitive-data/
- https://www.bleepingcomputer.com/news/security/ransomware-gangs-hackers-pick-sides-over-russia-invading-ukraine/
- https://www.wired.com/story/conti-ransomware-russia/
- https://cryptome.org/
- https://en.wikipedia.org/wiki/Cryptome

References

- https://www.thedailybeast.com/syria-chemical-attack-deniers-admit-links-to-wikileaks-and-russia
- https://newlinesmag.com/reportage/how-an-email-sting-operation-unearthed-a-pro-assad-conspiracy-and-russias-role-in-it/
- https://www.bellingcat.com/news/mena/2020/01/15/the-opcw-douma-leaks-part-1-we-need-to-talk-about-alex/
- https://www.bellingcat.com/news/mena/2020/01/17/the-opcw-douma-leaks-part-2-we-need-to-talk-about-henderson/
- https://www.bellingcat.com/news/mena/2020/01/23/the-opcw-douma-leaks-part-3-we-need-to-talk-about-a-false-flag-attack/
- https://www.bellingcat.com/news/mena/2020/02/11/the-opcw-douma-leaks-part-4-the-opcw-investigation/
- https://www.bellingcat.com/news/mena/2020/10/26/unpublished-opcw-douma-correspondence-raises-doubts-about-transparency-of-opcw-leaks-promoters/
- https://www.bellingcat.com/news/2021/05/14/berlin-group-21-ivans-emails-and-chemical-weapons-conspiracy-theories/
- https://www.dailydot.com/debug/wikileaks-new-submission-portal-broken/

References

- https://www.wired.com/2012/07/paranoia-anonymous/
- https://ddosecrets.com/wiki/About
- https://www.cjr.org/tow_center/emma-best-ddosecrets.php
- https://www.wired.com/story/ddosecrets-blueleaks-wikileaks/
- https://newrepublic.com/article/163106/ddossecrets-new-wikileaks-julian-assange
- https://www.mic.com/impact/distributed-denial-of-secrets-is-picking-up-where-wikileaks-left-off
- https://emma.best/2019/03/20/the-russian-contractor-who-infiltrated-anonymous/
- https://www.wired.com/2016/05/maksym-igor-popov-fbi/
- https://archive.org/details/MaksymIgorPopov

References

- https://www.dailydot.com/debug/hammond-sabu-fbi-stratfor-hack/
- https://www.nytimes.com/2014/04/24/world/fbi-informant-is-tied-to-cyberattacks-abroad.html
- http://www.sabufiles.com/
- https://enlacehacktivista.org/index.php?title=File:Thus_Spoke_Guccifer_2.0.pdf
- https://www.documentcloud.org/documents/7039357-200818-SSCI-Russia-Report
- https://www.buzzfeednews.com/article/kevincollier/assange-seth-rich-lies-guccifer-wikileaks-hannity
- https://thehill.com/policy/cybersecurity/310654-assange-some-leaks-may-have-been-russian/