



GLACY+

Global Action on Cybercrime Extended
Action Globale sur la Cybercriminalité Élargie

Funded
by the European Union
and the Council of Europe



Implemented
by the Council of Europe

Regional Conference on Policies and Strategies on cybercrime for the Caribbean Community

The role of the private sector

Santo Domingo – 13 June 2019

Sources of evidence

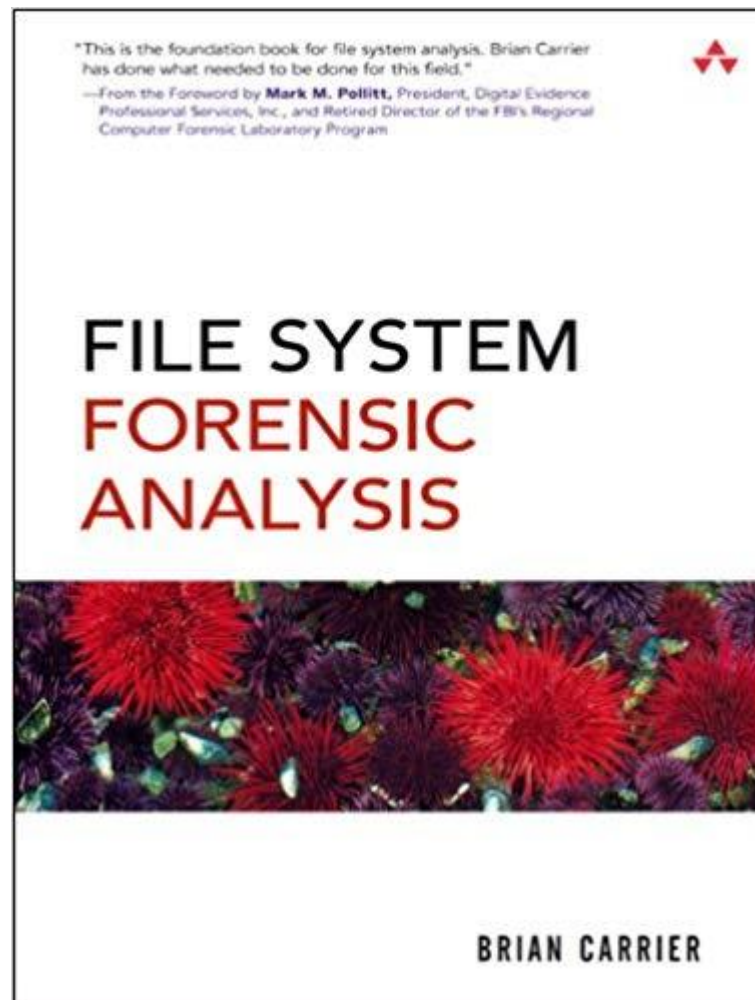
- Internet Service Providers are holders of potential evidence such as:
 - Subscriber information
 - Traffic data
 - Content data
- Data preservation
- Online services are numerous today, way beyond email and social networks. As good as all online service maintain transaction logs. Request made to Uber is increasingly common.



Forensics knowledge

Technology companies can explain the innards of their products such as:

- The file system
- Log files kept by the operating system or applications
- IMEI numbers and what they say about device models
- Authentication reliability information
- Memory/RAM forensics



Victims of cybercrime

- Companies have frequently been reluctant to report cybercrime incidents.
- Various legislation have introduced mandatory breach notifications such as:
 - HIPAA
 - Network and Information Security Directive
 - GDPR

The screenshot shows the 'Have I Been Pwned?' website interface. At the top, there's a navigation bar with links for Home, Notify me, Domain search, Who's been pwned, Passwords, API, About, and Donate. Below this is a search bar with the email 'uwe@rasmussen.eu' entered and a 'pwned?' button. The main content area has a dark blue header with the text 'Oh no — pwned!' and 'Pwned on 18 breached sites and found no passes (subscribe to search sensitive breaches)'. Below this is a section titled '3 Steps to better security' with three icons: 'Protect yourself using 1Password', 'Enable 2 factor authentication', and 'Subscribe to notifications'. The main body of the page lists several breaches with their respective logos and details:

- 2,844 Separate Data Breaches**: In February 2023, a massive collection of almost 3,000 alleged data breaches was found online. While some of the data had previously been seen in Have I Been Pwned, 2,844 of the files consisting of more than 80 million unique email addresses had not previously been seen. Each file contained both an email address and plain text password and were consequently indexed as a single "unverified" data breach. **Compromised data:** Email addresses, Passwords
- 500PX**: In mid-2018, the entire photography community 500px suffered a data breach. The incident exposed almost 15 million unique email addresses alongside names, usernames, genders, dates of birth and either an MD5 or bcrypt password hash. In 2023, the data appeared listed for sale on a dark web marketplace (along with several other high-profile and subsequently higher-credibility ones already). The data was reported to HIBP by a source who requested it to be attributed to "benjamin@supl0it.in". **Compromised data:** Dates of birth, Email address, Gender, Geographic locations, Names, Passwords, Usernames
- Adobe**: In October 2013, 153 million Adobe accounts were breached with each containing an internal ID, username, email, encrypted password and a password hint in plain text. The password cryptography was poorly done and many were quickly cracked back to plain text. The unencrypted text was also disclosed much about the passwords adding further to the risk that hundreds of millions of Adobe customers already faced. **Compromised data:** Email addresses, Password hints, Passwords, Usernames
- APOLLO**: In July 2018, the sales engagement startup Apollo left a database containing billions of data points publicly exposed without a password. The data was discovered by security researcher 'Vinyt Toia' who subsequently sent a subset of the data containing 126 million unique email addresses to Have I Been Pwned. The data left exposed by Apollo was used in their "revenue acceleration platform" and included personal information such as names and email addresses as well as professional information including dates of employment, the roles people hold and where they're located. Apollo stressed that the exposed data did not include sensitive information such as passwords, social security numbers or financial data. The Apollo website has a contact form for those looking to get in touch with the organization. **Compromised data:** Email addresses, Employers, Geographic locations, Job titles, Names, Phone numbers, Salutations, Social media profiles
- Collective #1**: In January 2013, a large collection of credential stuffing lists (combinations of email addresses and passwords used to hijack accounts on other services) was discovered being distributed on a popular hosting forum. The data contained almost 2.7 billion records including 773 million unique email addresses alongside passwords those addresses had used on other breached services. Full details on the incident and how to search the breached passwords are provided in the blog post 'The 773 Million Record "Collective #1" Data Breach'. **Compromised data:** Email addresses, Passwords
- dailymotion**: In October 2016, the video sharing platform Dailymotion suffered a data breach. The attack led to the exposure of more than 85 million user accounts and included email addresses, usernames and bcrypt hashes of passwords. **Compromised data:** Email addresses, Passwords, Usernames
- DISQUE**: In October 2017, the blog commenting service Disqus announced they'd suffered a data breach. The breach dated back to July 2012 but wasn't identified until years later when the data finally surfaced. The breach contained over 17.5 million unique email addresses and usernames. Users who created logins on Disqus had suffered SHA1 hashes of passwords while users who logged in via social providers only had references to those accounts. **Compromised data:** Email addresses, Passwords, Usernames

At the bottom, there's a note: 'DataBreach - In mid-2019, DataBreach suffered a data breach which exposed the stored credentials of tens of millions'.

Witnesses to crime

- The private sector may have collected information on cybercrime for different reasons:
 - Microsoft Tech Support Scams
 - TeliaSonera database of communications to unallocated IP addresses
- Similarly CERTs, such as financial sector CERTs could provide information about unlawful activity they see; including recurring phishing or hacking attempts.

 Microsoft [Office](#) [Windows](#) [Surface](#) [Xbox](#) [Deals](#) [Support](#)

Report a technical support scam

Microsoft takes its commitments seriously to protect and maintain the privacy of our customers who use our services in a protected manner. Unfortunately, technical support scams are a global problem worldwide. Customers, family, friends, and Microsoft employees are all reporting being contacted by someone claiming to be from a reputable company or a Microsoft partner.

If you have been contacted by someone claiming to be from Microsoft or a Microsoft partner, please contact us to report all the information regarding your interaction with them.

The information you provide will assist Microsoft in ongoing investigation targeting our customers, and will NOT be used to contact you for general marketing purposes.

Microsoft is committed to helping our customers and to protecting your privacy. We will use the information you provide to help us protect customer information.

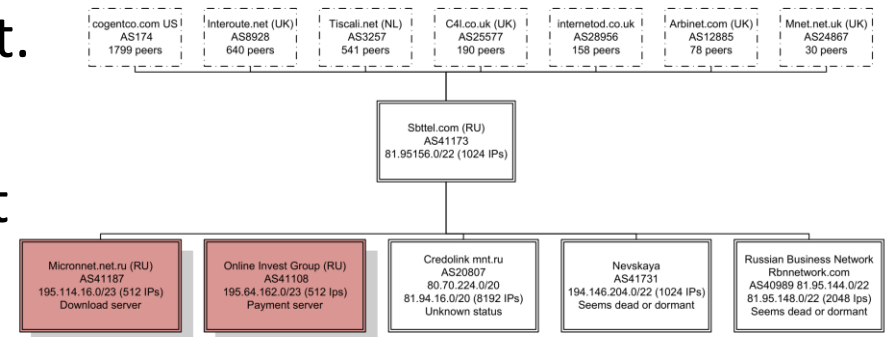
This customer complaint form is not for requesting Microsoft technical support.

* Required

Fraudulent Company Detail Information

Improving policies and practices

- Conversations with the private sector about detected cybercrime can help them adopt policies or codes of conduct that would eliminate it.
- ICANN had a policy for the fair distribution of IP addresses but needed to adopt a policy for revoking IP addresses.
- Providing free domain names lead to an increase of Advance Fee Fraud from the provider. Having a policy requiring some identification through payment systems reduced this.



Forums with the private sector

- Often the private sector is happy to participate in forums to discuss cybercrime in all its facets: whether it is as a victim, witness, or general discussions on cybercrime.
- The Council of Europe has published guidelines on cooperation between LE and ISPs on cybercrime which could be used to improve cooperation.





Questions