DIGITAL RISK PROTECTION FOR LEX MUNDI MEMBERS

January 2021

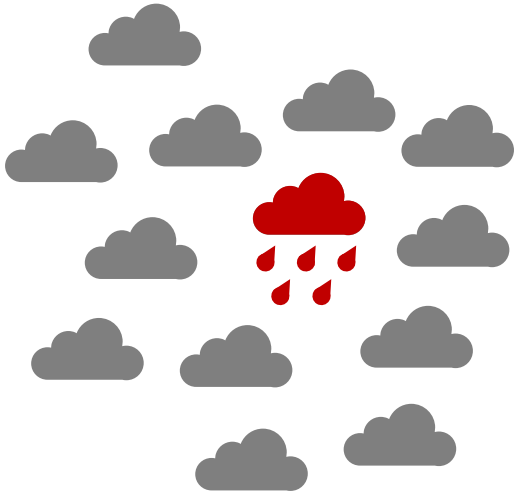
AGENDA

- Overview of Skurio's BreachAlert Digital Risk Protection Platform
- Lex Mundi member offer
- Platform demo
- How to sign up to your free 6 month subscription
- Q&A

YOUR DATA IS ALREADY OUTSIDE THE PERIMETER

Digital Transformation

Cloud Apps



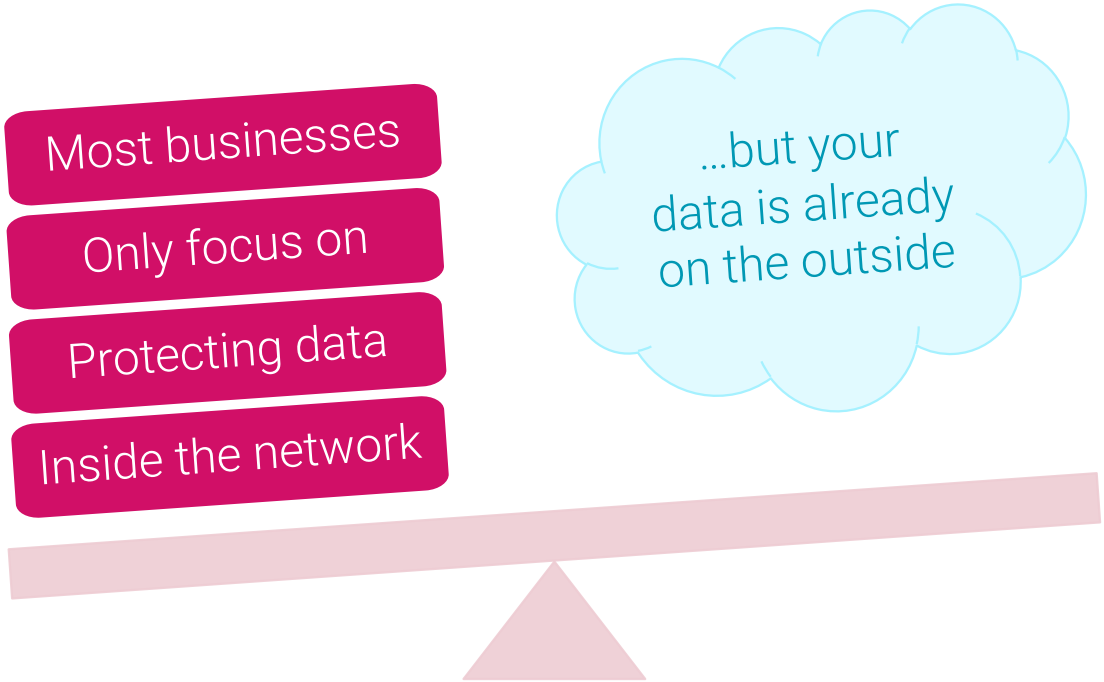
Shadow IT

…AND YOUR PERIMETER JUST GOT A WHOLE LOT BIGGER

- COVID : Widespread remote working
  - Likely to continue into 2021
- Uncontrolled network environment
  - WiFi, IOT, Physical Access
- Harder to verify things with colleagues
  - Increased risk from impersonation
  - Fraud & Business Email Compromise
- Increased malicious insider activity
  - Economic situation, salary / job cuts

TRADITIONAL CYBERSECURITY IS LAGGING BEHIND

- 95% of cybersecurity is still network-centric
  - Protecting your machines and networks
  - “Defending the perimeter”
- Digital Risk Protection looks after your data, wherever it lives
  - Advance warning of threats
  - Real-time detection of data leaks throughout your supply chain



CYBERSECURITY VS DIGITAL RISK PROTECTION

	Traditional Cybersecurity	Digital Risk Protection
Continuously monitoring	Inside the perimeter	Outside the perimeter
Philosophy	Machine-centric	Data-centric
Detection surface	Endpoints, network traffic, firewalls	Surface, Deep & Dark Web
External Threats	Generic : Signatures, Malicious IPs, Blocklists	Tailored : Organization Specific
Responsibility	IT Security	Data Owners, Risk, Compliance, CISO

DIGITAL RISKS ARE INVISIBLE AND DYNAMIC

Continuous monitoring

- Fast changing
- Invisible
- Automated
- Highly targeted

Continuous improvement

- Training
- Security Controls
- Patching
- Automation

Theft or loss is often invisible

- Confidentiality
- Integrity
- Availability

Large scale breach or outage is increasingly an “existential threat”

DIGITAL RISK FOR LEGAL FIRMS

Probability

Threat X Vulnerability → Asset → Impact

Law firms at high risk of being targeted

- Financial
- Ideological
- Political

Law firms (usually) better protected than other industries

- Take security seriously

High value assets

- Client Money
- Sensitive Data

The security flaws at the heart of the Panama Papers

Technology | Science | Culture | Gear | Business | Politics

The front-end computer systems of Mossack Fonseca are outdated and riddled with security flaws, analysis has revealed.

The law firm at the centre of the Panama Papers hack has shown an "astonishing" disregard for security, according to one expert. Amongst other lapses, Mossack Fonseca has failed to update its Outlook Web Access login since 2009 and not updated its client login portal since 2013.

Mossack Fonseca's client portal is also vulnerable to the DROWN attack, a security exploit that targets servers supporting the obsolete and insecure SSL v2 protocol. The portal, which runs on the Drupal open source CMS, was last updated in August 2013, according to the site's changelog.

PROTECT YOUR DATA, WHEREVER IT LIVES.

LexMundi World Ready

Four categories of data

- Login Credentials
- Assets & Infrastructure
- Personal Data
- Business Critical Information

Stored in three places

- Inside your network
- Within your supply chain
- Outside your network

Two types of breach

- Malicious Attack
- Human Error

DRP Platform

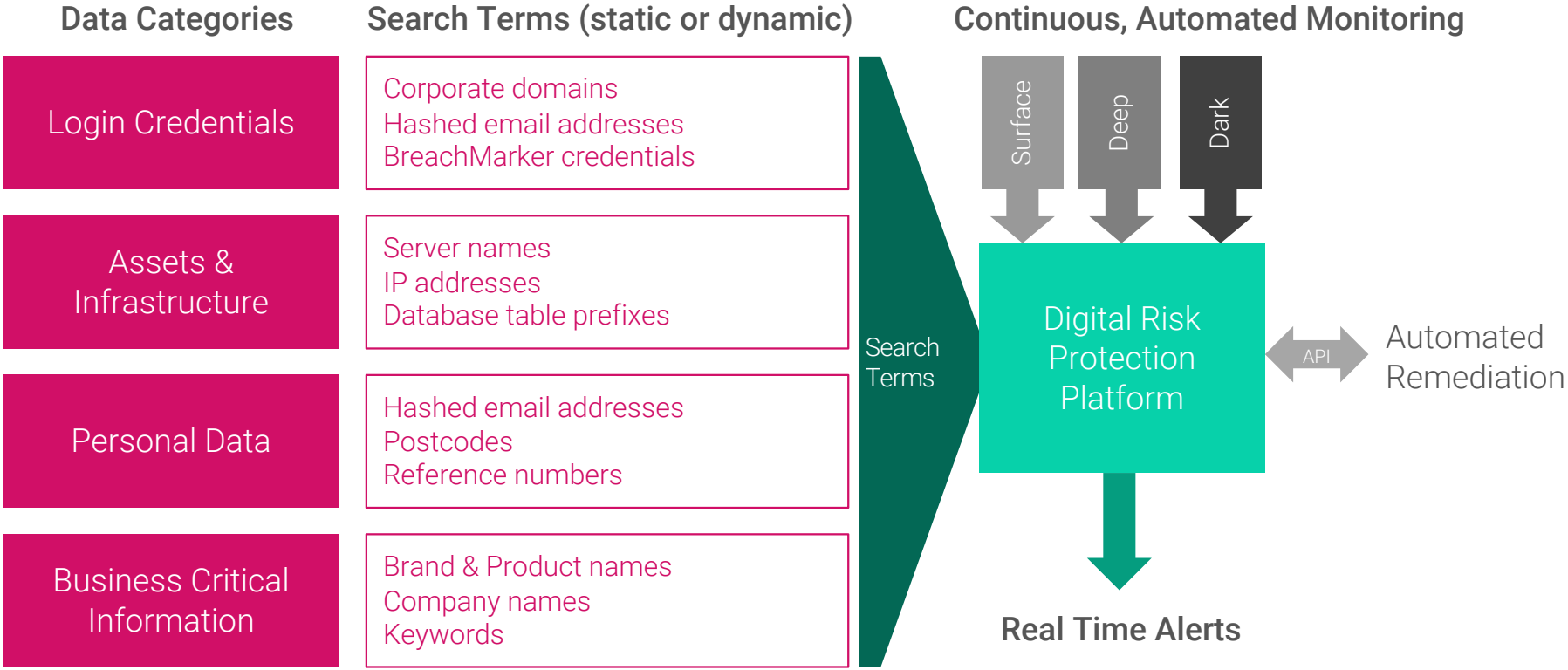
Digital Risk Protection

1. Detect
2. Alert
3. Take Action
4. Analyse & address

SKURIO

SKURIO DIGITAL RISK PROTECTION PLATFORM

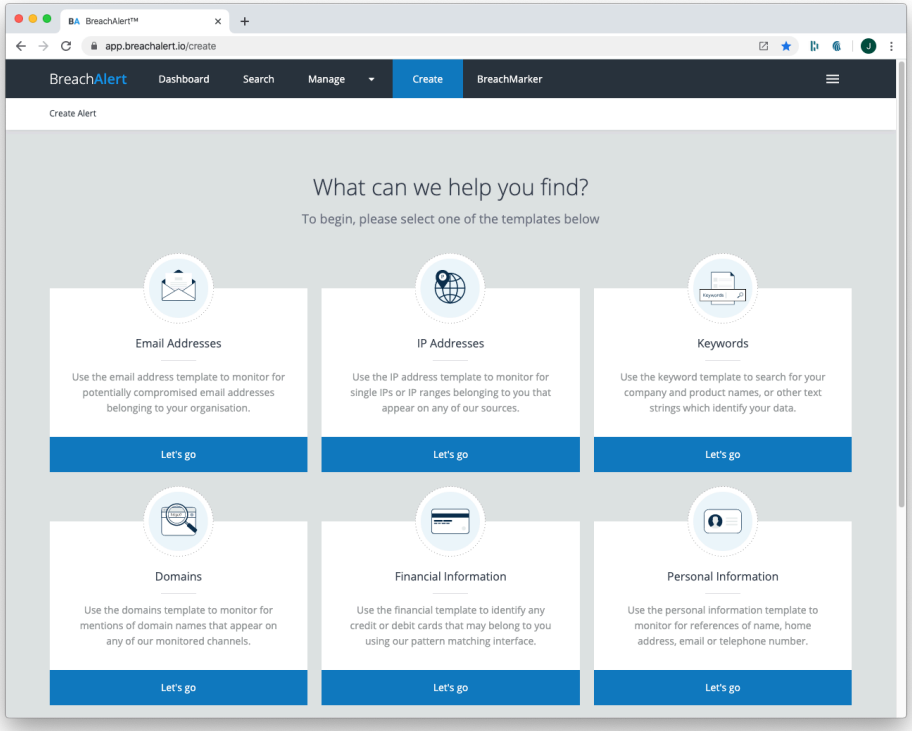
LexMundi World Ready



SKURIO

SKURIO DIGITAL RISK PROTECTION PLATFORM

- Intuitive web application
- Cloud hosted, nothing to install
- Configured in minutes
- Powerful REST APIs
- Annual SaaS subscription model
- Continuous monitoring
- Real-time alerts



PROTECT YOUR DATA, WHEREVER IT LIVES.

LexMundi World Ready

Login Credentials

Assets & Infrastructure

Personal Data

Business Critical Information

- Corporate networks
- Cloud Apps & Shadow IT
- Websites and customer-facing apps

unknown 2019-10-08 21:15:07

rt62@yahoo.co.uk|littledude1
denise@gloriousbridal.co.uk|glentoran
chandnicarpanini@me.com|marcus14a
kitty_hodson@btinternet.com|super2reds
marcus@green-electrics.co.uk|liverpool
dayaflack27@gmail.com|r8091504
conna.rose@btinternet.com|Rainbows97
connadoherty@btconnect.com|maxpodcoff...

Matched items in your search

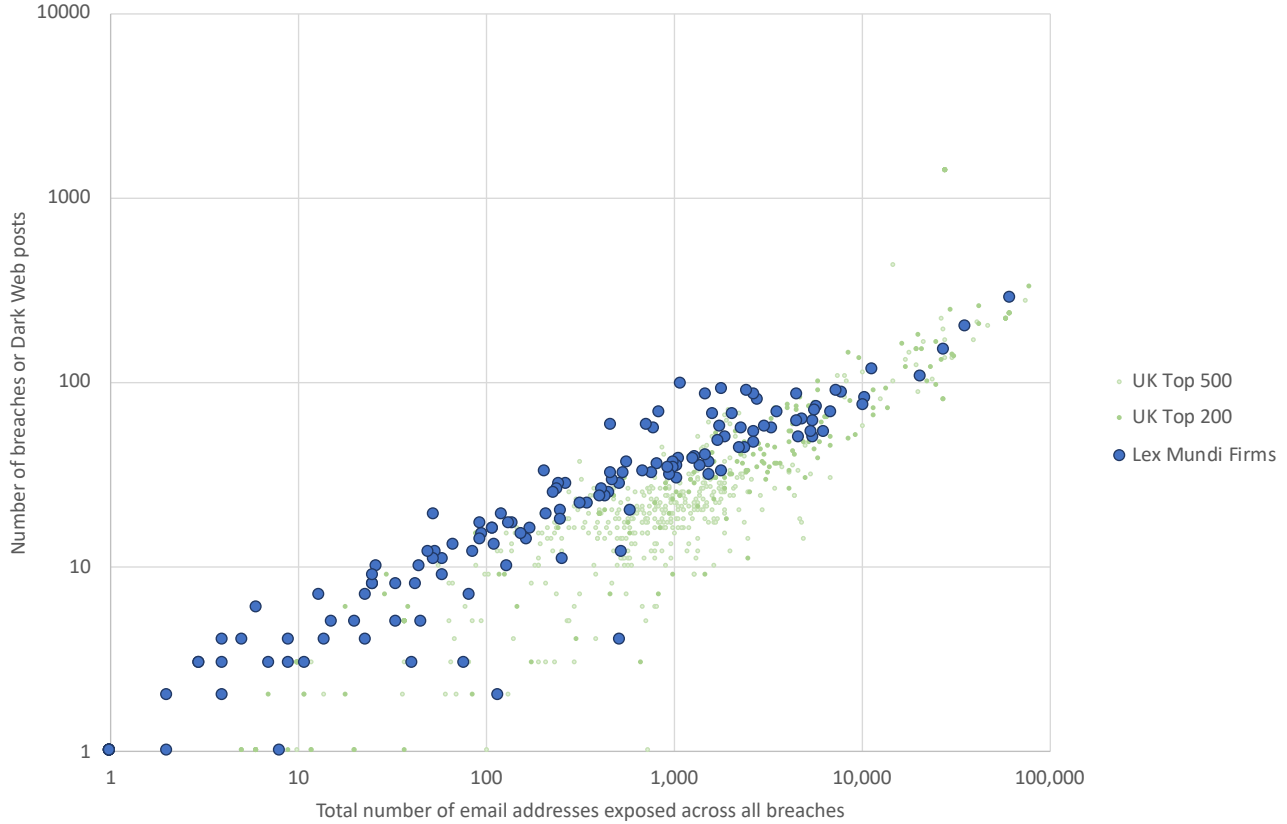
Email Addresses
1

- Typical example : Dump of credentials on a bin site
- Triggered an automated alert on Skurio platform
- Contained an email address from one of our customers
- Exposed corporate email address & plaintext password : “liverpool”

Real case study, with fictional data

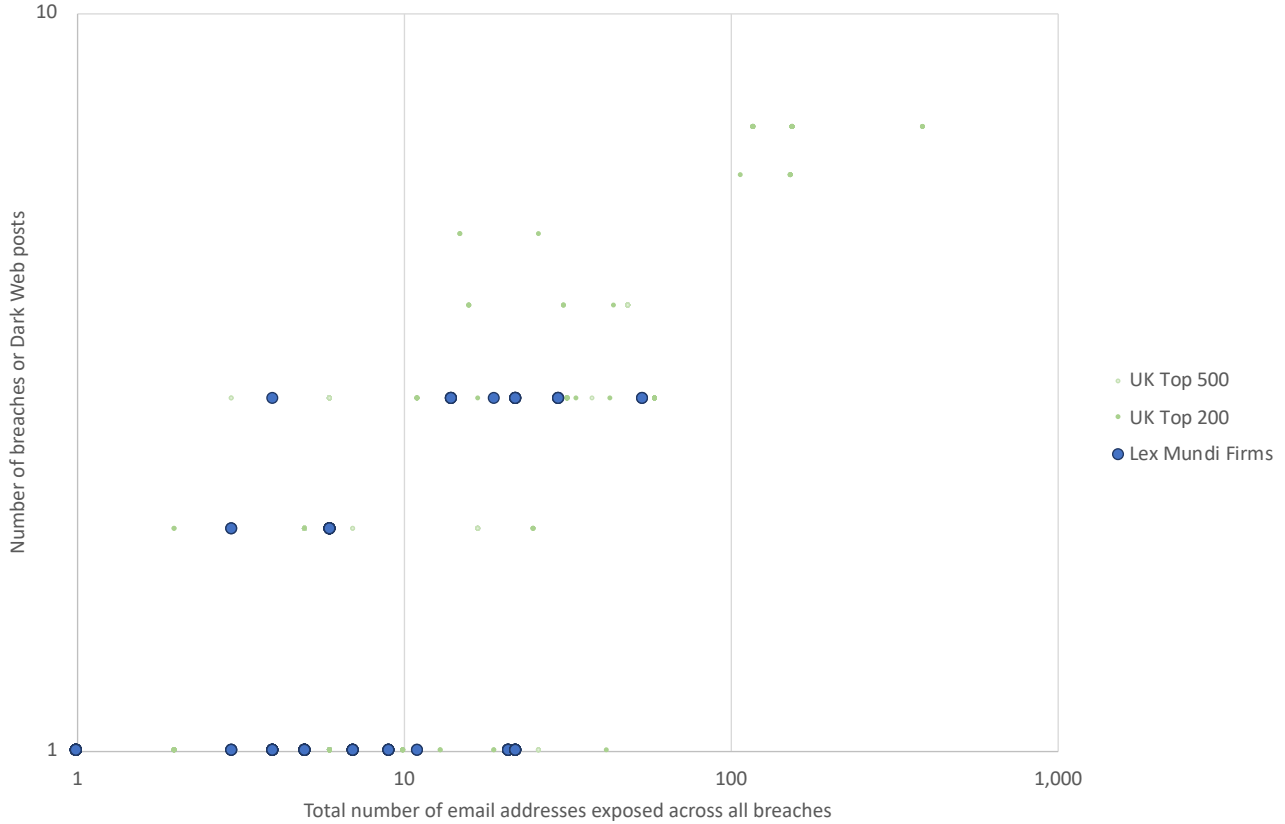
LEX MUNDI MEMBER FIRMS – EXPOSED CREDENTIALS

- Most firms have hundreds or thousands of staff email addresses exposed in data breaches
  - Lex Mundi firms broadly similar to UK top 500
- Many leaks also contain plaintext passwords
  - Staff often reuse the same password or variants
  - Risk of unauthorized access to your networks or third party systems
  - Business Email Compromise
  - Phishing / Spearphishing



CONTINUOUS LEAKS : STATS FROM LAST 30 DAYS

- 22 Lex Mundi member firms have had leaked credential alerts in the last 30 days
- Important to automate the monitoring, alerting and remediation process as far as possible



IMMEDIATE ACTION TO REDUCE IMPACT

Understand risks

- Business Email Compromise
- Network / VPN access
- Spearphishing
- Blackmail

Mitigate impact

- Takedown post
- Force network password rotation

Inform user

- Email staff member
- Include redacted password
- "Suggest" they reset any 3rd party sites

Educate

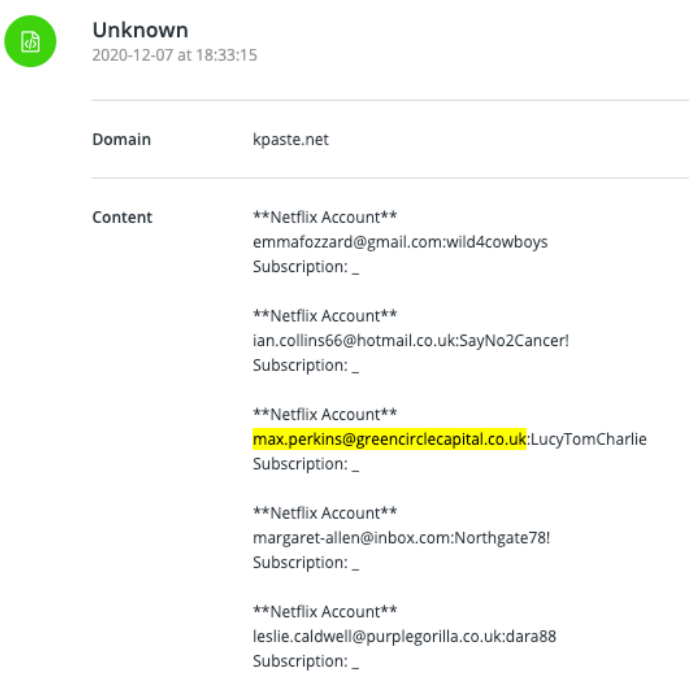
- Phishing awareness
- Password hygiene
- Password manager

marcus@green-electrics.co.uk | liverpool

Real case study, with fictional data

CASE STUDY : INVESTMENT FUND MANAGER

- Max Perkins : uses work email address and the same password on multiple sites
  - Names of his kids
- One of those sites gets hacked
  - Credentials leaked in ‘combo’ dump list
- Second hacker uses automated ‘credential stuffing’ tools
  - Tries automated login to other sites
  - Finds valid Netflix accounts and sells them
  - Delivers data to the buyer on an anonymous paste site



Real case study, with fictional data

PROTECT YOUR DATA, WHEREVER IT LIVES.

LexMundi World Ready

Login Credentials

Assets & Infrastructure

- Servers
- Sites & Apps
- Domains & IP addresses

Personal Data

Business Critical Information

CASE STUDY: HACKTIVIST TARGETING

- Reconnaissance by hacker group
  - Often targeting multiple organizations, ideological motivation
- Bad actors run automated penetration test scripts
  - Identify weaknesses in your infrastructure
- Publish the results on hacker forums or bin sites
  - Encouraging hacking or DDOS attacks by their followers
- Can detect this in near-real-time and block attack
  - Automatically detect mentions of IP addresses, domains, etc
  - Early warning of operation being planned
  - Deploy countermeasures, e.g. increased Web Application Firewall

```
NMAP PORT SCAN
==============================

Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-20 12:56 UTC
Nmap scan report for mail.hospitaldipreca.cl (200.74.161.66)
Host is up (0.15s latency).

PORT STATE SERVICE
21/tcp filtered ftp
22/tcp filtered ssh
23/tcp filtered telnet
80/tcp open http
110/tcp filtered pop3
143/tcp filtered imap
443/tcp filtered https
3389/tcp filtered ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 3.20 seconds
################################################################################
############################################################
[+] Starting At 2019-12-20 07:56:10.113861
[+] Collecting Information On: http://www.hospitaldipreca.cl/home/OpenNet/asp/default.asp?boton=Hom
[#] Status: 200
---------------------------------------------------
[#] Web Server Detected: Microsoft-IIS/7.0
[#] X-Powered-By: ASP.NET
[!] X-Frame-Options Headers not detect! target might be vulnerable Click Jacking
- Cache-Control: private
- Content-Length: 402904
- Content-Type: text/html
- Server: Microsoft-IIS/7.0
- Set-Cookie: ASPSESSIONIDCATACSDT=MKFBCOECKHOCMLLGPOHKJGDI; path=/
- X-Powered-By: ASP.NET
- Date: Fri, 20 Dec 2019 12:54:16 GMT
---------------------------------------------------
[#] Finding Location..!
[#] status: fail
[#] message: invalid query
[#] query: hospitaldipreca.cl
---------------------------------------------------
[x] Didn't Detect WAF Presence on: http://www.hospitaldipreca.cl/home/OpenNet/asp/default.asp?
boton=Hom
---------------------------------------------------
[#] Starting Reverse DNS
[-] Failed ! Fail
```

TYPOSQUATTING : BRAND IMPERSONATON

- wwwskurio.com
- www-skurio.com
- scurio.com
- skur1o.com
- skuriio.com
- skürio.com
- skụrio.com
- sḳurio.com

https://skurio.com

https://skurio.com

Can you spot the fake?

PROTECT YOUR DATA, WHEREVER IT LIVES.

LexMundi World Ready

Login Credentials

Assets & Infrastructure

Personal Data

- Customers
- Staff
- VIPs

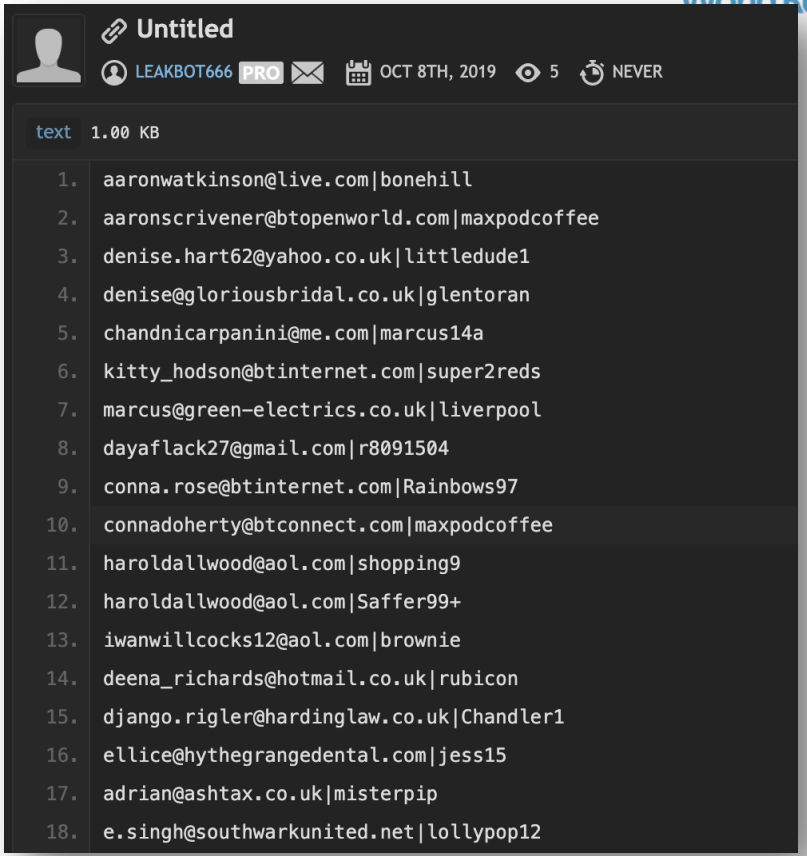
Business Critical Information

LexMundi World Ready

Where did it come from?

How did it leak out?

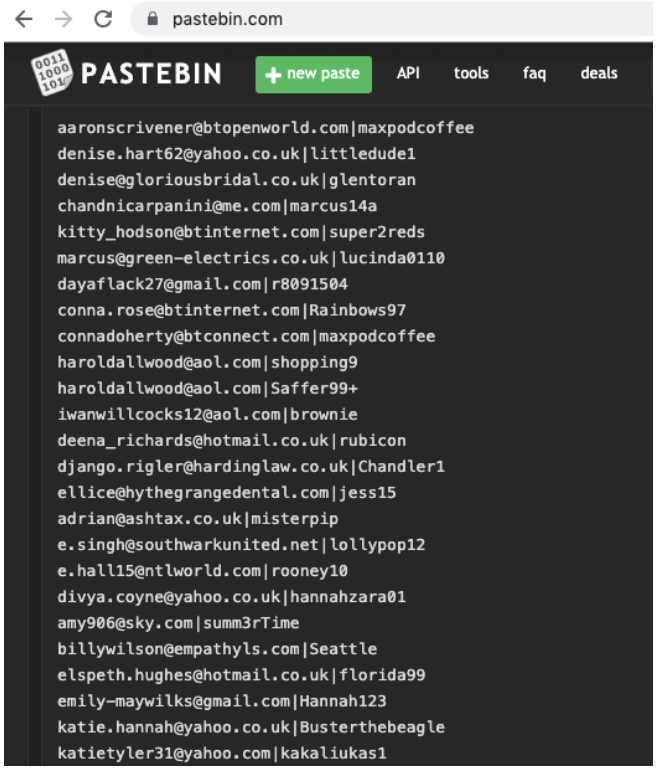
How would you know if this is your customer data?

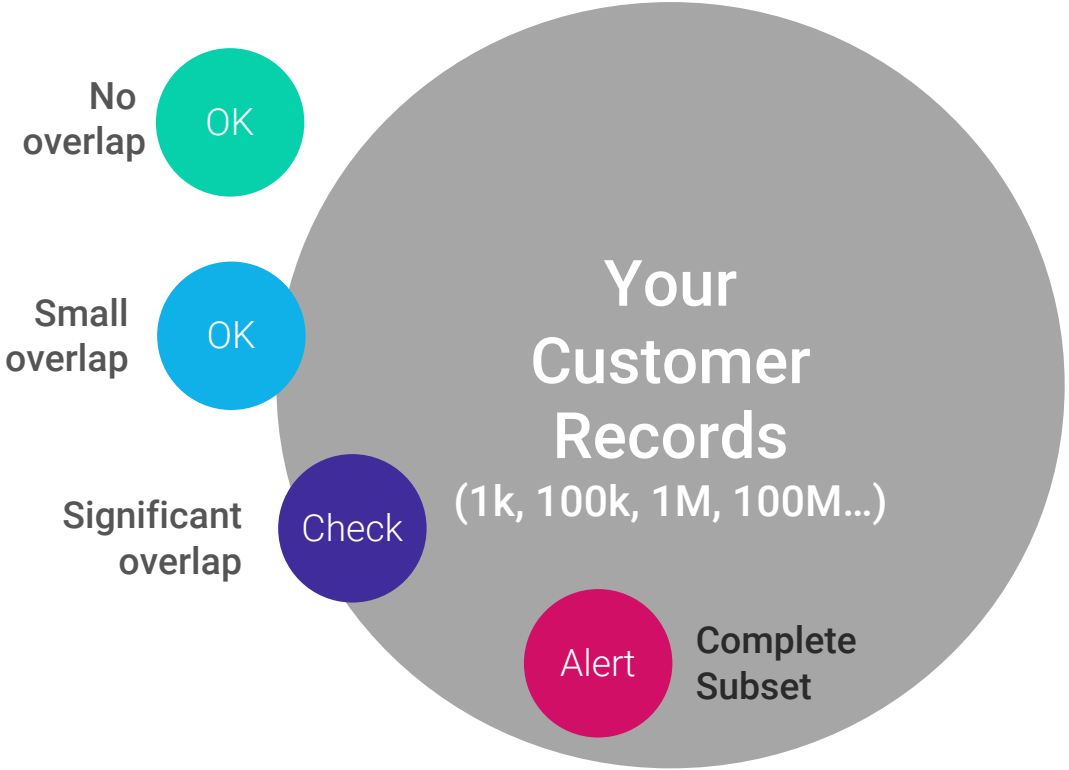


Real case study, with fictional data

SKURIO

CUSTOMER DATA MONITORING : THE DETECTION CHALLENGE





CUSTOMER DATA FINGERPRINTING

Secure Fingerprint

- Unique, 1:1 mapping
- Difficult / impossible to reverse engineer
- If you have the original data, you can compare the fingerprint

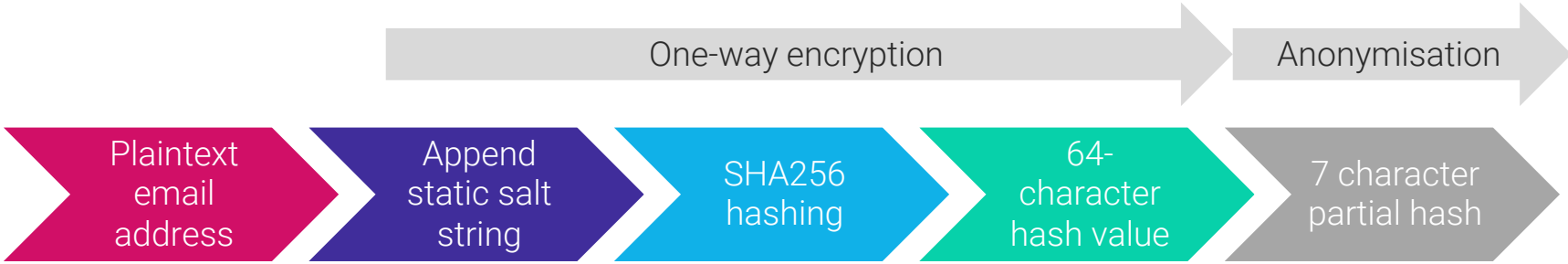
Scrambled Fingerprint

- Unique, 1:1 mapping
- Also incorporates a shared secret
- Comparison requires both the original data and the secret

Scrambled Fingerprint Fragment

- Non-unique, 1-to-many mapping
- Stored in the Skurio platform as an initial search term
- Will also return some false positive results
- Final comparison match is performed in your platform

SECURITY MODEL



Customer Email Address	Hashed Email (Salted SHA256)	Anonymous Fingerprint (K=6)
georgie.coldwell@greenhorsebank.co.uk	2c5a5a6bb0e5f476966d0ac726d1fd4c574ed462b09b3321b54acd15d1748bb2	2c5a5a6*
alan.wright9@talktalk.net	c89436c7d7df0c499ece5531716d226dd6e8dac67c224d4dbbb1b2620cbf1f89	c89436c*
gemma.butcher@gmail.com	119ecb71d5caded6c0e7489bd7c9f323112ac00841cef8663bda3478ea625a03	119ecb7*
Stays in your systems, never uploaded to ours	Uploaded to Skurio system, 1-way encrypted No way to identify the customer	Fully anonymised option

PROTECT YOUR DATA, WHEREVER IT LIVES.

LexMundi World Ready

Login Credentials

Assets & Infrastructure

Personal Data

Business Critical Information

- Counterfeit Goods
- Intellectual Property
- Trade Secrets

SKURIO

LEAK OF EMAIL THREAD FROM LAW FIRM

- Email thread between partner of Canadian law firm and client / third party
- Posted to anonymous dump site
- Discloses PII and potentially sensitive information
  - Did the leak originate from the law firm or the client?
- Automated real-time detection mitigates damage
  - Request takedown of post to minimise propagation
  - Investigate network logs to see if post was made from inside the corporate network
  - Make legal request for log data to dump site

Real case study, with fictional data

from: Adam Solta [mailto:aSolta@gmail.com]
Sent: February-04-19 2:48 PM
to: Osman, Hamid <hamid.osman@aardvark.com>
cc: Brendan, Florence <Florence.Brendan@aardvark.com>; Klepp, Nicholas <Nicholas.Klepp@aardvark.com>; Peachtree, Clive <Clive.Peachtree@aardvark.com>
subject: Re: Acme Case Payment Verification

Thanks Hamid,

I'll send my payment to Jack now. I signed the engagement letter and sent it to him already but I don't think he sent me anything for KYC yet. I'll ask him about that.
Adam

On Mon, Feb 4, 2019 at 11:42 AM Osman, Hamid <hamid.osman@aardvark.com> wrote:

Hi Adam –
I can. (Just to clarify, it is for the CCAA proceeding, vs a class action). You should have received an engagement letter and KYC document. If you did not, our insolvency team (which is cc'd) can assist.

Regards,
Hamid Osman
Partner
T +1 416 324 3627
hamid.osman@aardvark.com

http://www.aardvark.com/images/signature/logo.png

from: Adam Solta [mailto:aSolta@gmail.com]
Sent: February-04-19 2:00 PM
to: Osman, Hamid <hamid.osman@aardvark.com>
subject: Acme Case Payment Verification

Hello Hamid,

Jack Jiang has informed me that he is collecting payments from the class action plaintiffs and will be sending you a lump sum payment tonight. Just wondering if you can independently confirm this for me before I send him my payment of $500.

Thank you,

Adam Solta
604-294-6745

LEXMUNDI MEMBER PACKAGES

LexMundi World Ready

Functionality	BreachAlert SP (Free 6 month)	BreachAlert Pro	CTI Pro
Discounted member pricing (Year 1 subscription)	~~$1,250~~ $500	~~$15,600~~ $6,250	~~$23,400~~ $9,250
User logins (Maximum)	1	2	2
Number of included Email Domains	3	20	20
Max search terms	30	500	500
Number of Alert Monitors	3	10	10
Search terms per Alert Monitor	10	50	50
Number of BreachMarkers	3	10	10
Historical search	-	Yes	Yes
Dark Web, Data Dumps, Bins, etc	Yes	Yes	Yes
News, Social Media & Blogs (Reddit, News)	-	-	Yes
Result Analytics (Multi-message analysis)	-	-	Yes

BreachAlert™ | Skurio Digital Risk Protection fr

info.skurio.com/lexmundi-member-offer

SKURIO Products Solutions Resources Company Partners Login Contact

LexMundi World Ready

Skurio Digital Risk Protection for LexMundi Member Firms

Skurio is pleased to announce our exclusive partnership with LexMundi, to bring Dark Web monitoring & data breach detection to your firm with our innovative Digital Risk Protection platform. LexMundi is covering costs for members to receive a six-month subscription to the platform, so you can start protecting your important data and monitor for potential threats to your firm right away.

How Skurio works

The Skurio DRP system monitors surface, deep and Dark Web sources around the clock for instances of your data appearing where they shouldn't. When our automated monitoring detects leaked data you are instantly notified so that you can take timely steps to avoid attacks and mitigate risk.

This type of monitoring for data specific to your firm provides the following benefits:

- Eliminates false positives and reduce noise by searching for specific content relevant to your firm
- Creates simple targeted alerts to search for your organisation using keywords, email domains, login credentials, IP Addresses, email addresses or account numbers

Subscribe for free Skurio DRP Account

First Name*

Last Name*

Job Title*

Company Name*

Please enter the full name of your firm

Work Email*

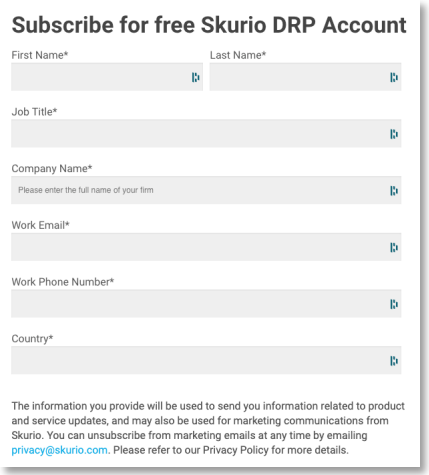
Work Phone Number*

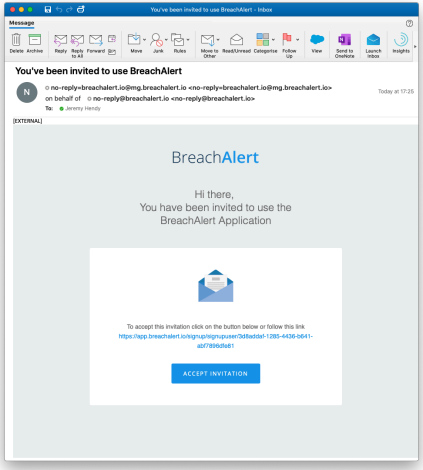
Country*

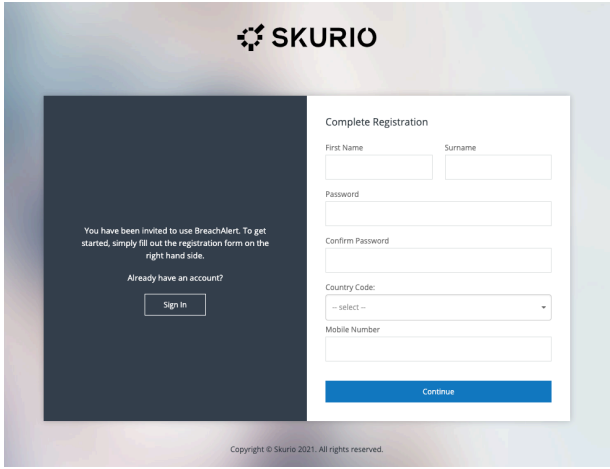
The information you provide will be used to send you information related to product and service updates, and may also be used for marketing communications from Skurio. You can unsubscribe from marketing emails at any time by emailing privacy@skurio.com. Please refer to our Privacy Policy for more details.

SIGNING UP

1. Website form → 1 working day → 2. Email Invitation → 3. Set password & get started!







LEX MUNDI MEMBER FIRM OFFER

- Free 6-month trial of Skurio BreachAlert SP – basics covered
  - Signup before end of May 2021, will run for 6 months
  - Can then be extended for just $500 / year
- **70% discount** on year 1 upgrade subscriptions signed by **15th February**
  - CTI Pro subscription : $23,400 discounted to **$7,000**
- **60% discount** on year 1 upgrade subscriptions during your free 6 month period
  - CTI Pro subscription : $23,400 discounted to $9,400
- **40% discount** on year 1 subscriptions at the end of your free 6 month period
  - CTI Pro subscription : $23,400 discounted to $14,000

HOW TO SIGN UP

- Via the Lex Mundi portal
- https://info.skurio.com/lexmundi-member-offer
- lexmundi@skurio.com

PROTECT YOUR DATA, WHEREVER IT LIVES.

LexMundi World Ready

Four categories of data

- Login Credentials
- Assets & Infrastructure
- Personal Data
- Business Critical Information

Stored in three places

- Inside your network
- Within your supply chain
- Outside your network

Two types of breach

- Malicious Attack
- Human Error

DRP Platform

Digital Risk Protection

1. Detect
2. Alert
3. Take Action
4. Analyse & address

SKURIO

THANK YOU

https://info.skurio.com/lexmundi-member-offer