SKURIO

The essential guide to

Digital Risk Protection

Protecting your infrastructure

skurio.com

Protect your infrastructure

Bad actors and criminals could be targeting your organisation already.

By collaborating and using techniques like port scans and reverse DNS lookups, they can get hold of valuable information about your network infrastructure, vulnerabilities, and the software you use.

It could be worse still if one of your team leaks sensitive information.

Stop the next attack on your infrastructure before it happens

3 things bad actors look for

- Domains, subdomains, and IP addresses
- Vulnerabilities in operating systems, hardware and software used
- Temporary storage and databases used for system testing

3 ways they can use them against you

- Denial of Service, either at a critical point (DoS) or distributed (DDoS)
- Vulnerability exploitation to deploy ransomware or malware
- Exfiltration of unprotected databases or digital assets

3 ways this increases digital risk

- **Reputational:** inability to provide service or capture new customers
- **Operational:** availability, confidentiality and integrity impacts on your systems
- **Revenue:** payment diversion, extortion or ransom could impact your bottom line

It's not all bad news

To plan attacks on your business, bad actors and criminals need information. To get this, they may access the Dark Web to buy, sell or share details about your infrastructure. They may discuss or collaborate on attack planning using hacktivist forums. And, when they do, they will often keyword terms specific to your business. Monitoring for these keywords can give an early warning of an imminent attack.

Automated early warning

- Automated Dark Web monitoring can check if your information is being discussed or circulated, and it works 24x7
- Instant alerts give you crucial hours, days or even months to implement mitigating steps

3 easy ways to reduce risk

- Close ports that are open unnecessarily
- Prioritise patch application and other measures to protect against exploitation of vulnerabilities discussed
- Deploy web application firewalls

Our customers agree...

"If we didn't have this type of threat intelligence capability, we would be under attack before we even knew that we were under attack."

CISO, travel and tourism sector

Close up

Network information breach

How your data is exposed

- **Port scans:** Tools designed to help your security teams conduct penetration testing also provide hackers intelligence on exposed or poorly configured equipment and vulnerabilities. There is no specific law to prevent hackers from performing an ‘aggressive port scan’ on your network.
- **Domain whois:** Information about your domain registration, including expiration dates and similar available domains, can be discovered using a simple whois search.
- **Reverse lookup:** a reverse IP or name server (NS) lookup scan can provide hackers with details of all domains hosted on an IP address or name server. It could uncover unprotected contact details and allow hackers to monitor activity.
- **Insider threat:** A member of staff leaks important details about your infrastructure when asking for help with a technical issue on a support forum.

Details you can use to monitor for attack planning

- Individual IP address
- IP Address (range) search (“185.90.35.150”)
- Domain and subdomain names
- Email addresses that have privileged system access

Monitoring results you might expect

- Published port scans or reconnaissance (recon) results
- Forum conversations that mention your company or staff
- Mentions of your company name in conjunction with known bad actors

Close up

Network information breach

How criminals can use this data to target your business

- **DoS/DDoS attacks:** denial or distributed denial of service attacks using recruitment of multiple parties.
- **Direct network attack**: attempted network penetration by exploiting a vulnerability.
- **Spearphishing:** phishing that targets an individual who has administration access to network infrastructure or network management tools.
- **Extortion:** fake ethical hackers target your company. These fraudsters will seek payment in exchange for giving you details of vulnerabilities you could have found yourself.
- **Typosquatting:** hackers use readily available details to register a typosquatting domain and impersonate your business.
- **Domain takeover:** without additional protection services, your domains are registered by activists if they lapse.

Steps you can take that reduce risk

- Address any vulnerabilities listed for software and equipment you use
- Deploy a web application firewall to reduce the impact of a DoS attack
- Inform staff of potential extortion attacks
- Request a takedown of posts containing sensitive details where possible
- Monitor for typosquatting domain registrations

Close up

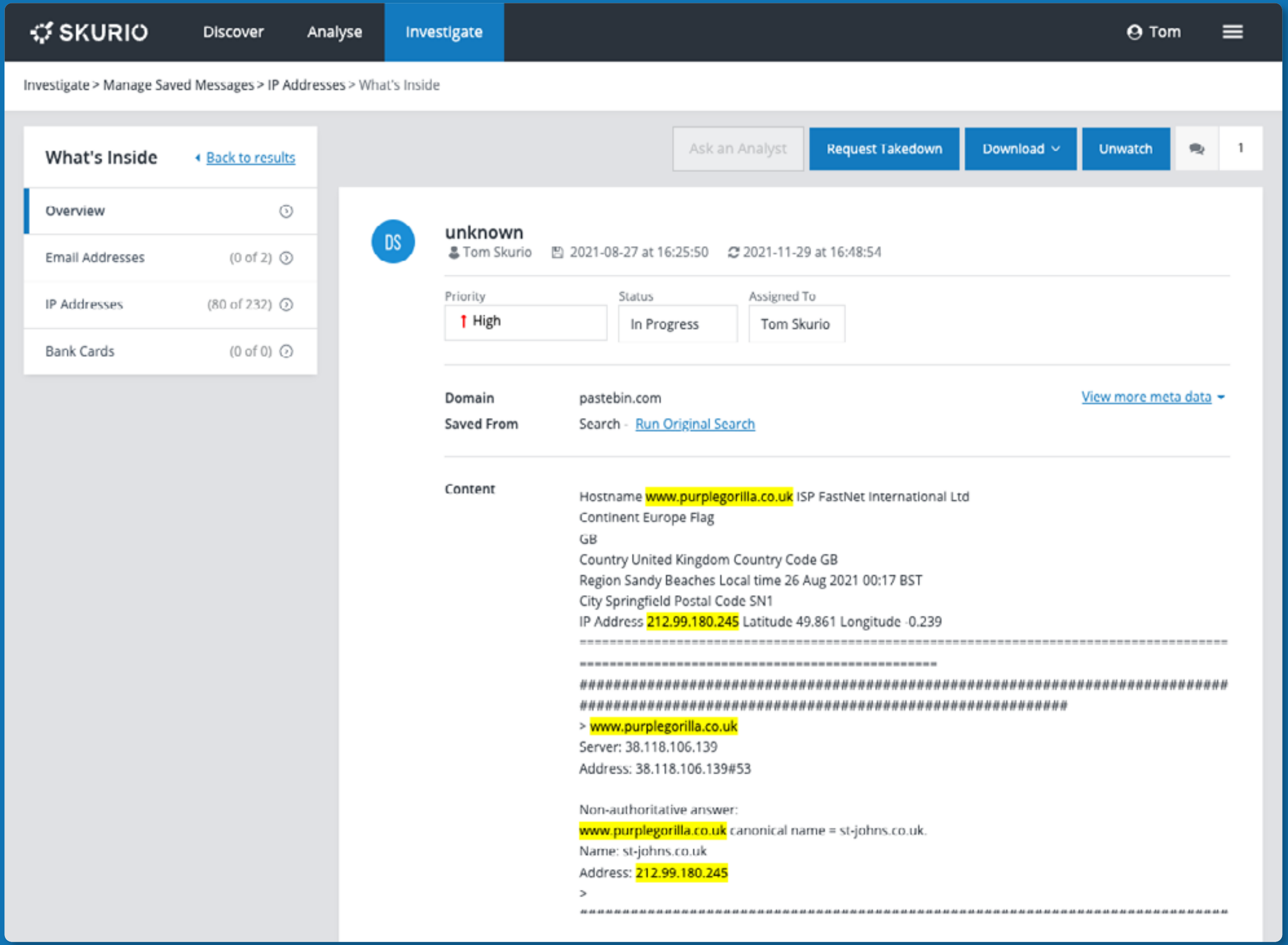
Network information breach

IP address and domain search

Widely available recon tools can capture infrastructure details. These tools can highlight vulnerabilities, including open ports or unpatched servers.

If they are shared on dumpsites, as this example shows, or discussed in forums, your organisation could become a target of hackers.

Without monitoring or conducting manual searches every day, this exposure can go unnoticed. A simple takedown request can get the content taken down and the risk reduced.



Investigate > Manage Saved Messages > IP Addresses > What's Inside

What's Inside Back to results

Overview	
Email Addresses	(0 of 2)
IP Addresses	(80 of 232)
Bank Cards	(0 of 0)

unknown

Tom Skurio 2021-08-27 at 16:25:50 2021-11-29 at 16:48:54

Priority	Status	Assigned To
High	In Progress	Tom Skurio

Domain pastebin.com

Saved From Search - Run Original Search

View more meta data

Content

```
Hostname www.purplegorilla.co.uk ISP FastNet International Ltd
Continent Europe Flag
GB
Country United Kingdom Country Code GB
Region Sandy Beaches Local time 26 Aug 2021 00:17 BST
City Springfield Postal Code SN1
IP Address 212.99.180.245 Latitude 49.861 Longitude -0.239
==========================================================================================
==================================================
##################################################################################
#############################################################
> www.purplegorilla.co.uk
Server: 38.118.106.139
Address: 38.118.106.139#53

Non-authoritative answer:
www.purplegorilla.co.uk canonical name = st-johns.co.uk.
Name: st-johns.co.uk
Address: 212.99.180.245
>
##################################################################################
```

Use case samples represent real life examples. Data has been changed to protect the privacy organisations where appropriate.

Extended use cases

	Indicator of attack planning	Ransomware	Supply chain compromise
	Known threat actors discuss your company on forums in conjunction with attack methods, indicating that a cyber-attack is imminent or likely.	If a new vulnerability affects your infrastructure, your business could become a target for ransomware gangs. So, scanning for mentions of your business in discussions about vulnerabilities is vital. Posting exfiltrated data regardless of ransomware payment is a recent trend with ransomware gangs. Any company experiencing a ransomware attack should monitor for leaked data.	Swift detection of data breaches or vulnerabilities in your supply chain is key to preventing follow-on incidents like ransomware attacks and reducing financial exposure. Monitoring for supplier information can provide an early indicator of supply chain vulnerabilities, attack planning or attacks in progress.
Details bad actors look for	• Brand or company name mentions alongside potential threat actors or attack methods	• Newly discovered vulnerabilities • Published recon details • Credential breaches from your supply chain partners	• Newly discovered vulnerabilities • Published recon details • Credential breaches from your supply chain partners
How they can be used	• To recruit additional individuals to assist with the attack • Claiming responsibility for an attack • Discussing the best way to target your business	• Direct cyber-attacks on your partners that result in leaks of your data or intelligence on your operations • Exploiting access to your infrastructure that you have granted to your partners	• Direct cyber-attacks on your partners that result in leaks of your data or intelligence on your operations • Exploiting access to your infrastructure that you have granted to your partners
How this increases digital risk	• Loss of operational systems • Loss of customer and partner trust • Loss of business/income	• Exfiltration of customer data • Extortion • Supply chain compromise	• Exfiltration of customer data • Extortion • Supply chain compromise
Steps you can take	• Address outstanding vulnerabilities • Add additional protection to critical assets	• Add BreachMarker IDs to identify customer data leaks from partners • Notify partners of potential threats so they can act • Monitor for exfiltrated data dumps from supply-chain partners that include your content	• Add BreachMarker IDs to identify customer data leaks from partners • Notify partners of potential threats so they can act • Monitor for exfiltrated data dumps from supply-chain partners that include your content

SKURIO

Skurio Digital Risk Protection

Skurio Digital Risk Protection provides you with the foundation necessary to adopt a data-centric approach to cybersecurity for your business.

Skurio continuously monitors the surface, deep and Dark Web for your data and instantly alerts you whenever it is found.

Skurio Cyber Threat Intelligence looks for cyber threats specific to your business, giving you a single view of all data protection incidents and threats outside your network. BreachMarker and BreachResponse features protect your data across your supply chain and integrate valuable alerts into your response management systems.

Dark Web Monitoring

- Monitor for staff, customer, infrastructure, and critical business data 24x7
- Tailored searches on social, surface, Deep and Dark Web sources
- Search years of historical data to know your digital footprint

Data Breach Detection

- Get instant alerts if your Skurio detects data outside your network
- Automate your breach response playbooks with readymade integrations to SIEM and ITSM systems
- Instantly identify the source of a breach with data-watermarking

Cyber Threat Intelligence

- Combine curated content relevant to your business to speed up investigations
- Use intuitive analytics to get usable insights faster
- Organise intelligence insights with simplicity and collaborate to improve resolution

To understand how Skurio can help protect what's important to your business and reduce your digital risk, please visit: **skurio.com.**

SKURIO

SKURIO LTD | ARTHUR HOUSE | 41 ARTHUR STREET | BELFAST | BT1 4GB

+44 28 9082 6226   info@skurio.com   skurio.com