The Attackers Eye View™

Using the tools of a cybercriminal to address increasing risk

STORM Guidance

Founded 2014

CEO Neil Hare-Brown

Assess

Cyber risk assessments to enable clients to learn and improve their cyber security and to enable insurers and reinsurers to manage book risk.

Plan

Helping insured clients to create, learn (through training) and exercise/test their plans in dealing with different types of cyber incidents in the context of their business.

Respond

Delivering a fully coordinated and Integrated Cyber Incident Response Team (ReSecure & CyberCare).

Jonny Baker

Technical Lead

- Working with STORM developing services and products for Cyber insurers, brokers and end-user clients for around 5 years.
- Current capacity as Technical lead for the last year and a half
  - Assist with technical operations on various incident response cases that come through in areas such as digital forensics, data retrieval, open source intelligence gathering and big data analysis
  - Oversee technical execution of our software products and services
- Previously in the Fintech sector and co-founded an FCA regulated company integrating with Open banking APIs

Ransomware

What we're seeing

- 2 x increase in active cases vs this time last year
- 60% of those are ransomware
- 80% Linked to known ransomware gangs
- Increased evidence of organised crime
  - Initial access brokers
  - Ransomware as a service
  - Support centres
- Ransom demands from $40,000 - $1.5 million

Ransomware

Future trends that we are expecting

- A continued trajectory in active cases
- A similar share of ransomware cases that we deal with
- Same ransomware gangs but rebranded
- Ransom demands to be on a wider scale to cater for the amount of SMEs that are being attacked

Ransomware

What we’re trying to do about it

- Increasing awareness of Cybersecurity
- Offering support such as trauma counselling
- Developing user friendly services to help end-user clients
- Collaborating with insurers and brokers to reduce the risk on their books

The Rise in Ransomware

↑ ~80%

Building Cyber Resilience

Multi-Factor Authentication, Privileged & Remote Access Controls, Network Segmentation etc.

Addressing the Human Factor

- ❖ Training & Awareness on Social Engineering Risks
- ❖ Regular Simulated Phishing Exercises
- ❖ Incident Reporting

Testing Potential Ransomware Attack Scenarios

Ensuring Effective Third Party Cyber Security

STORM CyberProfiler | Made possible QBE

> *The report is fascinating… I will share it with the IT team*
> ”

- Offering CyberProfiler as a value add service to QBE Cyber Policyholders
- Providing insights into potential vulnerabilities
- Enabling businesses to better understand their online exposures
- Practical knowledge to remediate and improve risk profiles
- Feedback so far…

> *“Excellent Service”*

STORM

CyberProfiler

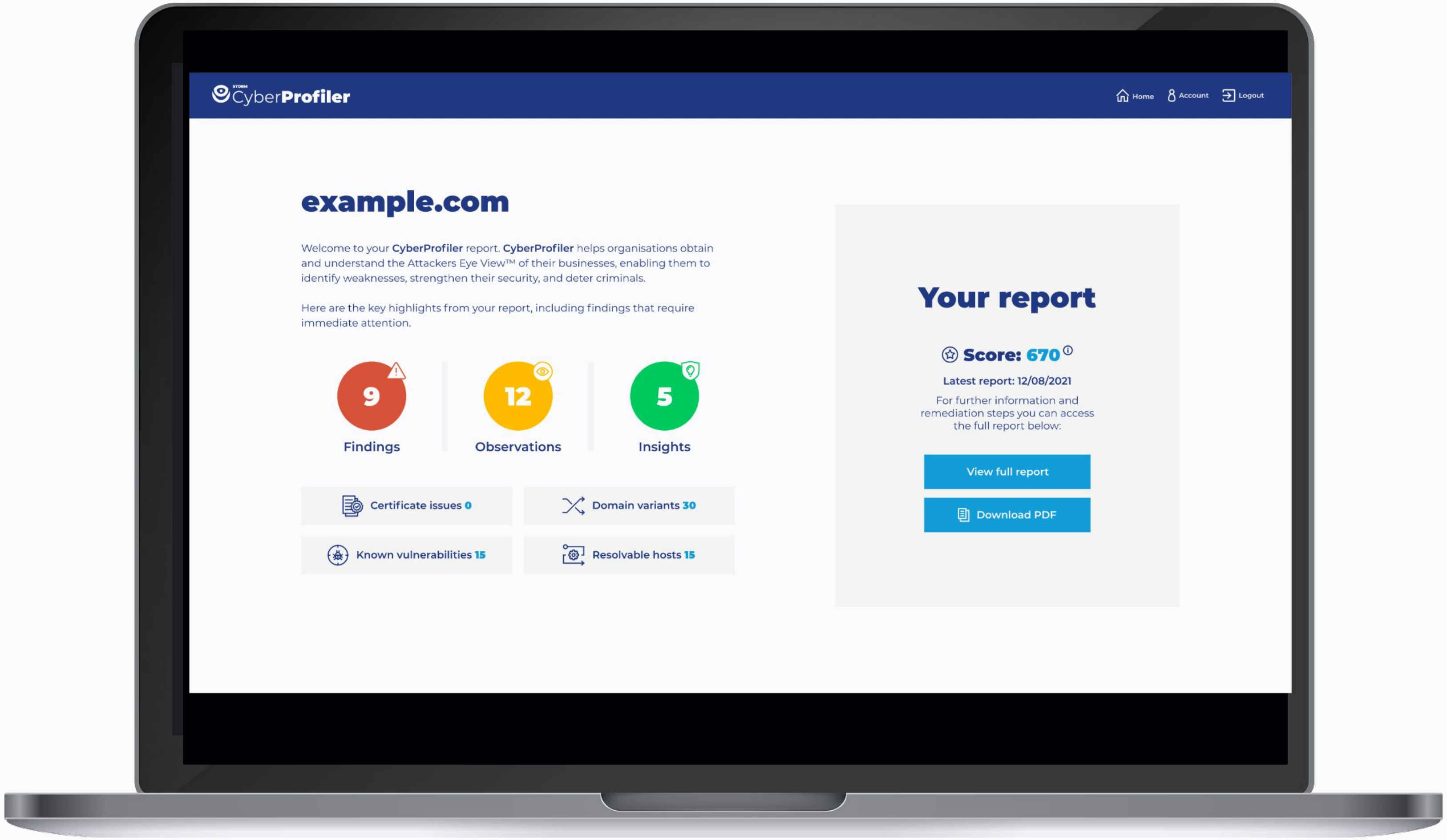
The Attackers Eye View™

Helping organisations to understand their cyber risk from an attackers perspective

Using cyber profiling for good

- STORM have created both tools and have a trained group of OSINT specialists with cyber profiling knowledge
- This gives clients an outside facing in '**Attackers Eye View™**' of their online presence
- Designed with insurers/brokers in mind - enables insureds to reduce their vulnerabilities and significantly restrict the information that cybercriminals need to plan their attacks
- Support clients on the journey to cyber resilience through clear remediation steps in a report deliverable and also an account for our CyberProfiler customer portal
- Additional help also available via our CyberCare support centre for both technical and non-technical clients

STORM: CyberProfiler Portal



example.com

Welcome to your **CyberProfiler** report. **CyberProfiler** helps organisations obtain and understand the Attackers Eye View™ of their businesses, enabling them to identify weaknesses, strengthen their security, and deter criminals.

Here are the key highlights from your report, including findings that require immediate attention.

9 Findings

12 Observations

5 Insights

Certificate issues **0**

Domain variants **30**

Known vulnerabilities **15**

Resolvable hosts **15**

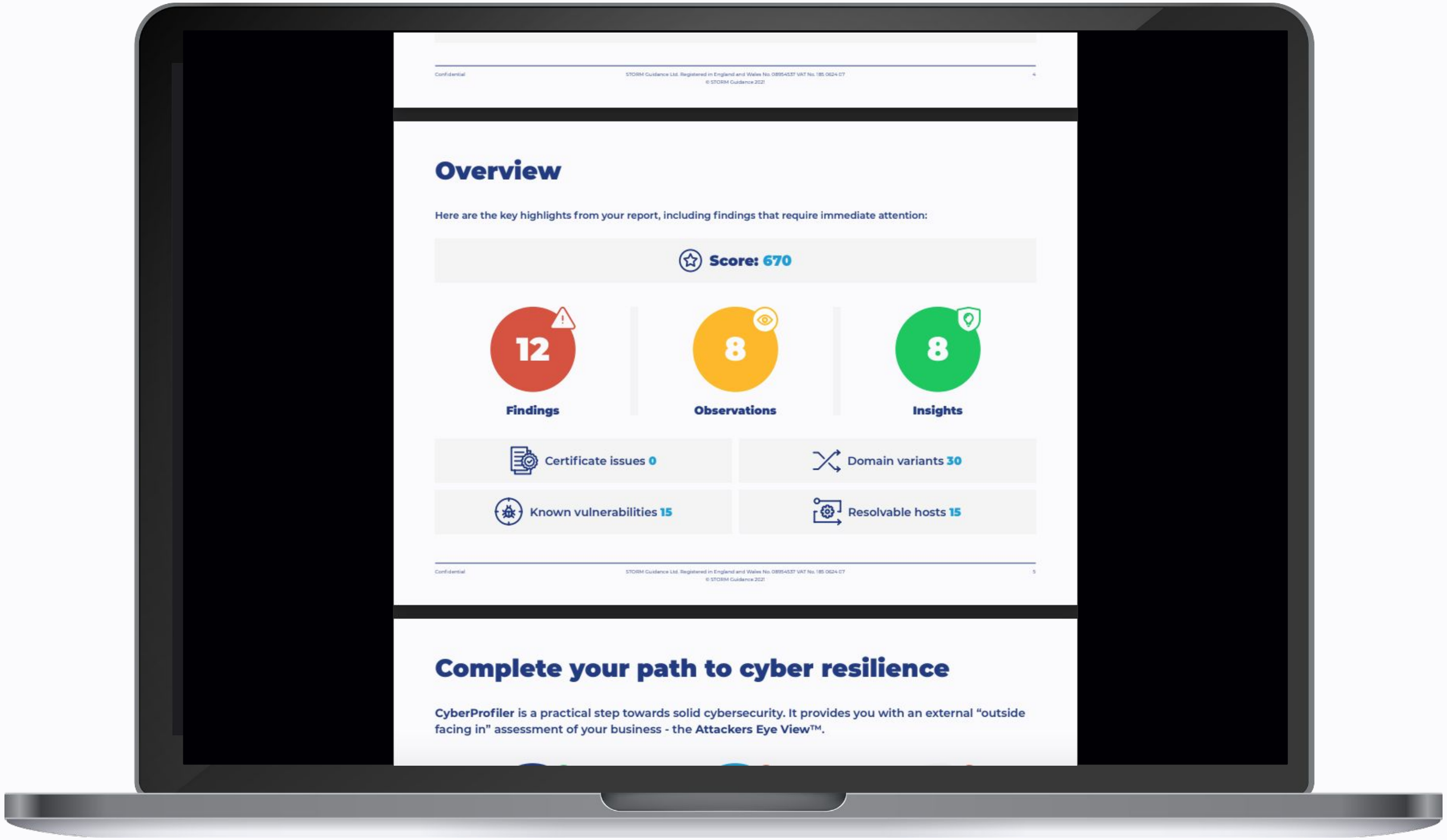
Your report

Score: 670

Latest report: 12/08/2021

For further information and remediation steps you can access the full report below:

STORM: CyberProfiler Portal



Confidential STORM Guidance Ltd. Registered in England and Wales No. 08954537 VAT No. 185 0624 07 4
© STORM Guidance 2021

Overview

Here are the key highlights from your report, including findings that require immediate attention:

Score: 670

12	8	8
Findings	**Observations**	**Insights**

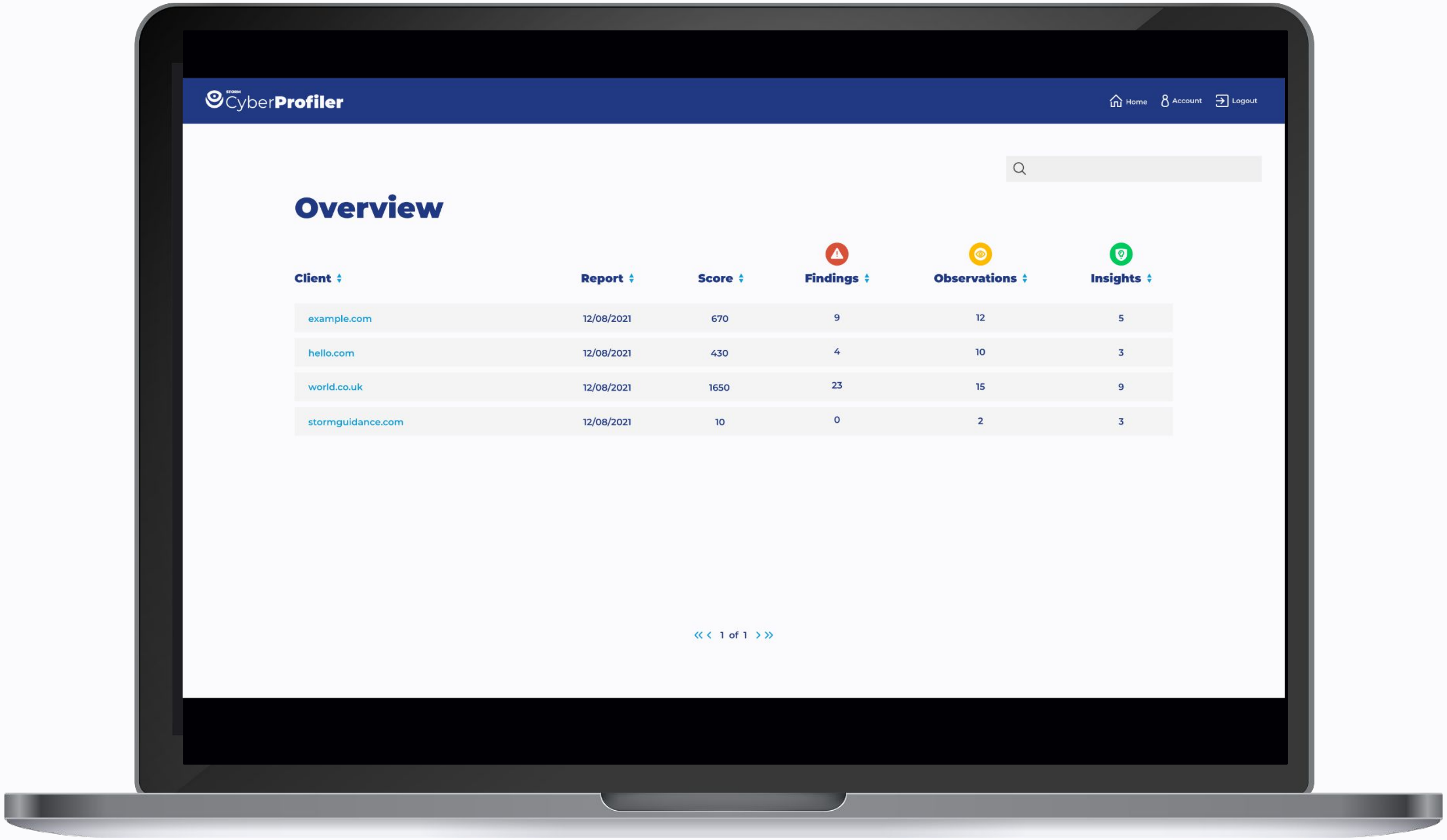
Certificate issues **0**	Domain variants **30**
Known vulnerabilities **15**	Resolvable hosts **15**

Confidential STORM Guidance Ltd. Registered in England and Wales No. 08954537 VAT No. 185 0624 07 5
© STORM Guidance 2021

Complete your path to cyber resilience

CyberProfiler is a practical step towards solid cybersecurity. It provides you with an external "outside facing in" assessment of your business - the **Attackers Eye View™**.

STORM: CyberProfiler Portal



Overview

Client	Report	Score	Findings	Observations	Insights
example.com	12/08/2021	670	9	12	5
hello.com	12/08/2021	430	4	10	3
world.co.uk	12/08/2021	1650	23	15	9
stormguidance.com	12/08/2021	10	0	2	3

Proxyshell Case study

- Exploited 3 known vulnerabilities on Microsoft Exchange servers
- Discovered April 2021
- Similar to Proxylogon and Hafnium attacks
- Can be broken down into three steps:
  - Initial access
  - Elevation of privileges
  - Deployment of malicious payload

Proxyshell Case study

Step 1: Initial access

CVE-2021-34473

Pre-auth Path Confusion leads to ACL Bypass

- Takes advantage of a feature called Explicit login
- By manipulating this URL you are able to gain access to the server

```
https://exchange/autodiscover/autodiscover.json?@foo.com/mapi/nspi/
?&Email=autodiscover/autodiscover.json%3f@foo.com
```

Becomes

```
https://exchange/mapi/nspi/
```

Proxyshell Case study

Step 2: Elevate privileges

CVE-2021-34523

Elevation of Privilege on Exchange PowerShell Backend

- Takes advantage of a feature called Powershell remoting
- With access to the server you can set a default value for what user to authenticate as
- Exchange admin will do nicely… ;)

Proxyshell Case study

Step 3: Deployment of malicious payload

CVE-2021-31207

Post-auth Arbitrary-File-Write leads to RCE

- RCE: Remote code execution
- Takes advantage of a feature called New-MailboxExportRequest
- Send encoded payload to new mailbox
- Server saves and decodes payload

- Gotcha...

Proxyshell Case study

Summary

- All CVE information publicly available
- Easily mitigated with patches
- Dedicated search engines for IPs with these vulnerabilities
- Vulnerabilities on IPs across entire digital estate provided by CyberProfiler

Remote Desktop Protocol (RDP)

Case study

- RDP allows systems administrator to control users machines to fix issues
- Most commonly works by exposing port 3389 on the computer you are trying to connect to

Once target is acquired.. how shall we get in?

- Guess username/password
- Acquire stolen credentials
- Man-in-the-middle (MITM)
- Known vulnerability for RDP software being used

Remote Desktop Protocol (RDP)

Case study

Once access is gained

- Explore the network
- Elevate privileges
- Locate backups
- Start preparing ransomware deployment

How do we stop this?

- Restrict the IPs that can access the RDP port via a VPN connection
- Multifactor authentication enforced
- Limit the login attempts
- Offsite backups

Remote Desktop Protocol (RDP)

Case study

Summary

- Many port scanning tools out there
- Annual penetration testing provides active scanning
- Passive port scanning provided with CyberProfiler

Social engineering Case study

- Still one of the most common ways of deploying ransomware
- Facilitated in a number of different ways
  - Watering hole attacks
  - Call centres
  - Phishing emails

Social engineering Case study

Phishing emails

Who shall I send it to?

- Accounts department?
- HR department?
- A busy individual eg. CEO ?
- Another verified individual

How do I send it to the correct email?

- Basic search of Linkedin
- Guess email of employees

Find data breaches..

Social engineering
Case study

Phishing emails

Data breaches

- Compromised passwords - quick win
- Legitimate email - not likely to change
- Readily available

Got some email addresses.. best way to get in touch?

- Spoof a legitimate contact
- Invent a company relevant to target
- Or..

Why not send an internal email..

Social engineering Case study

Phishing emails

How can you send something from someone else’s domain?

- Send from a similar domain, or 'domain variant'
  - example.com, examp1e.com, e.xample.com
- Set domain in ‘from’ email
  - Protected with DNS records:
  - MX, SPF, DMARC, DKIM
- Send from unprotected subdomain
  - DNS configurations in main domain do not always protect subdomains

Social engineering
Case study

Phishing emails

Summary

- Social engineering is a common way of getting malicious payloads deployed
- Phishing emails can be highly effective
- Breached emails easy to find
- DNS misconfigurations easy to find
- All checked for in CyberProfiler

STORM Cybersecurity principles

- Have good security hygiene
  - Methodical maintenance procedures around updating technologies
  - Clear, sensible security guidelines that everyone is aware of
  - Remove unused services and reduce the risk of forgotten systems
- Be secure by default
  - Enforced MFA as standard
  - Good DNS record management

STORMGuidance

Thank you