Driving Cyber Security Excellence in e-Government

Protecting Delaware's Citizens and Critical Systems

RedShield

DELAWARE
DTI
DELIVERING TECHNOLOGY THAT INNOVATES
DEPARTMENT OF TECHNOLOGY AND INFORMATION

GREAT SEAL OF THE STATE OF DELAWARE
LIBERTY AND INDEPENDENCE
1704 • 1776 • 1787

Agenda

Driving Cybersecurity Excellence in e -Government

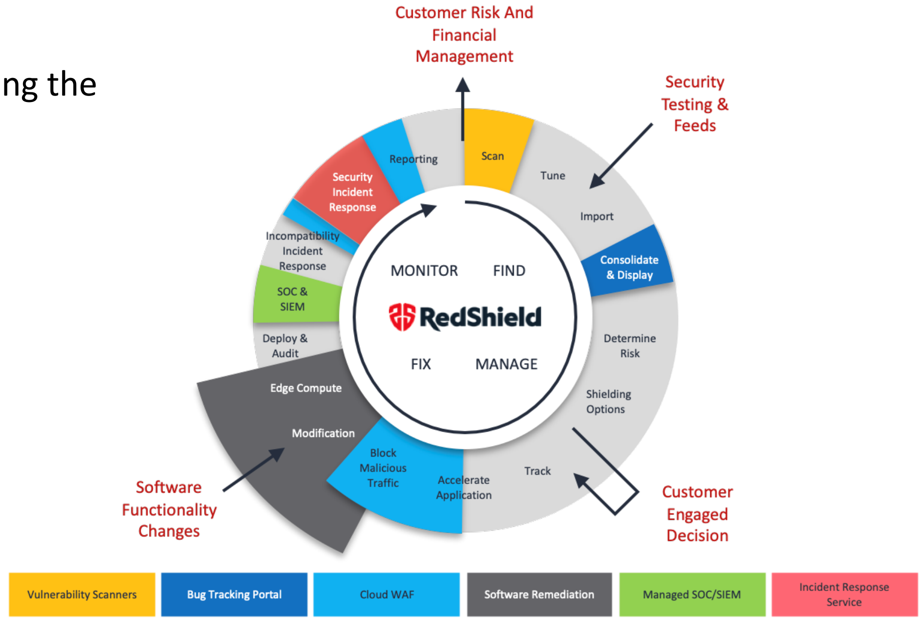
Intro and background	5 mins
Risk Landscape into 2024	20 mins
Changing the game with effective mitigation	15 mins
Q&A	5 mins

Intro and background

RedShield is a security service, which finds, fixes and manages web application vulnerabilities

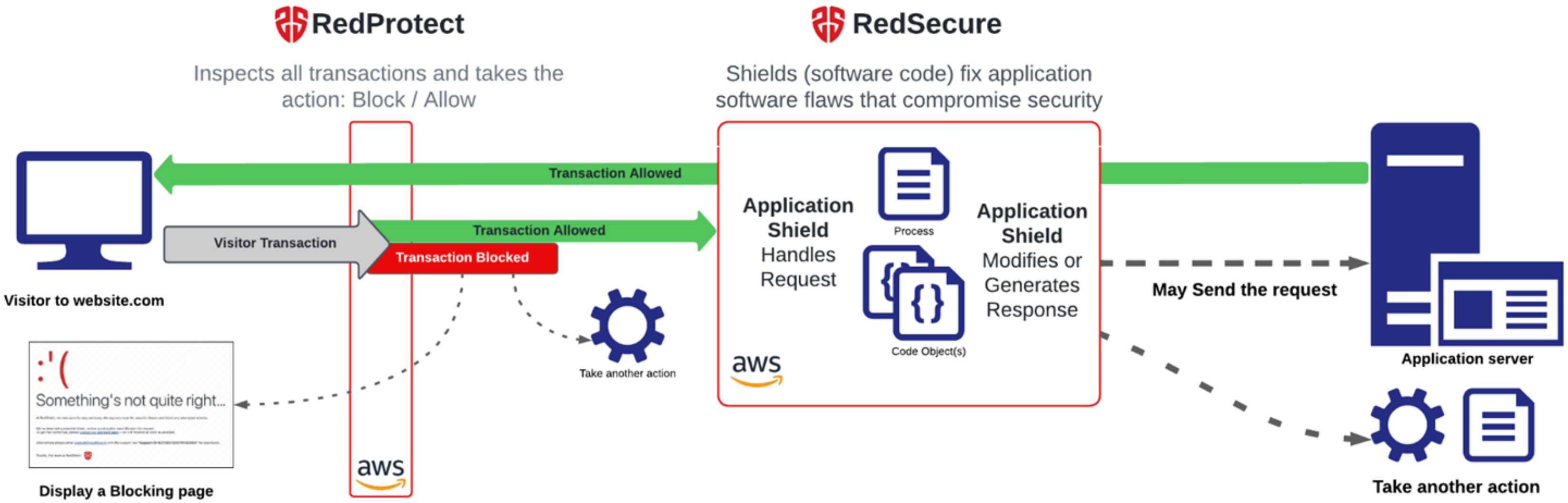
- Fully outsourced web security operations and platform/tooling
- Shields are code objects in a reverse proxy, removing the need to redevelop applications

12.6 billion	Legitimate website transactions secured by RedShield per month
100 trillion	Security inspection point checks performed on website transactions per month - checking for good vs bad
40 million	Malicious hacking attempts blocked in August
>80,000	Website vulnerabilities under management



RedShield includes a cloud platform based on a full proxy architecture in AWS* to guarantee speed and availability

RedShield's proprietary processes (playbooks) and software protects and secures customers' most critical applications



RedProtect

Inspects all transactions and takes the action: Block / Allow

RedSecure

Shields (software code) fix application software flaws that compromise security

*AWS migration completed in Q1 2024

RedShield's approach continues to gain traction with both new enterprise customers and partners.

Selection of US Customers

Groundworks®

SENTARA®

NATIXIS
INVESTMENT MANAGERS

GREAT SEAL OF THE STATE OF DELAWARE
•1704•1776•1787•

Ben The Beneficient Company Group, LP

CAMCapital®
CAXTON ALTERNATIVE MANAGEMENT

IKO®

NIBCO®
AHEAD OF THE FLOW®

TechnipFMC

LOOMIS | SAYLES

Partners

AT&T

aws

Deloitte.

G.

Rimini Street®

Compliance

Information Security Management
ISO 27001
Certified

PCI DSS CERTIFIED

SOC 2
AUDITED
TYPE I

GDPR

CCPA
COMPLIANT

HIPAA
COMPLIANT

Shareholders

PENCARROW
PRIVATE EQUITY

Deloitte.

SAGE
INVEST WITH WISDOM

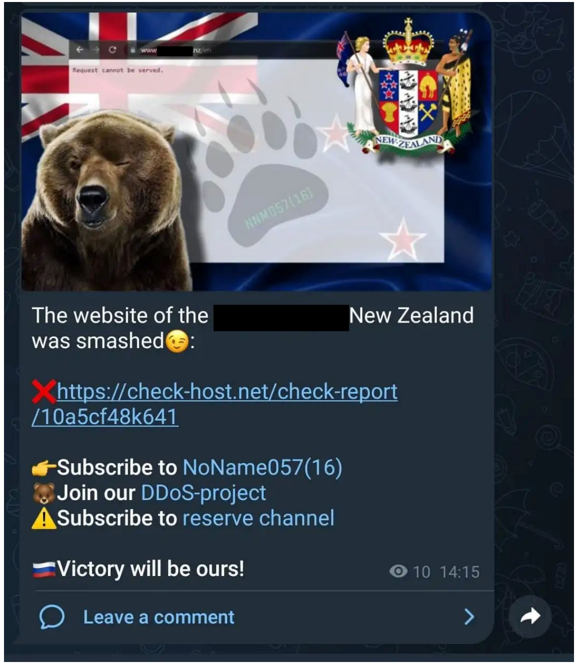
Risk Landscape into 2024

2024's enemies are gearing up with focus and persistence

2023 has seen Pro Russian hacking groups threatening Ukraine allied nations

“NoName057” joined Killnet and Anonymous Sudan in attacking government and enterprise websites

- Specifically calling out government organisations publicly supporting Ukraine with sanctions and militiary assistance
- A series of cyber attacks ensued, targeting high profile government and enterprise websites across western nations.
- NoName057 claimed that they had caused disruption to several unprotected websites.



The website of the [redacted] New Zealand was smashed😉:

❌https://check-host.net/check-report/10a5cf48k641

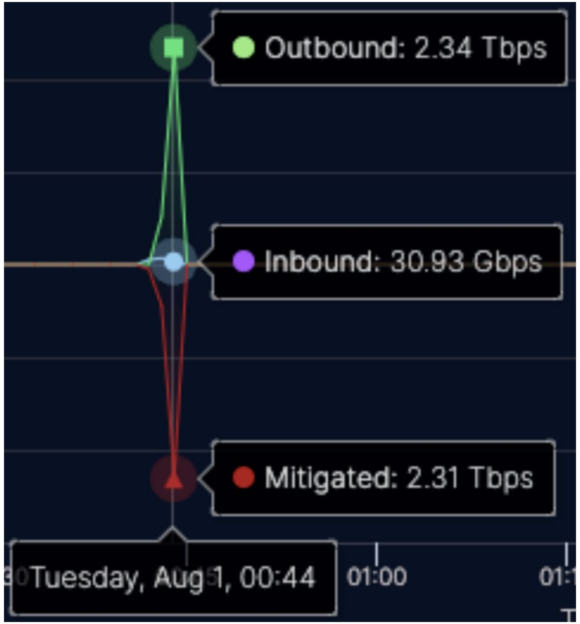
👉Subscribe to NoName057(16)
🐻Join our DDoS-project
⚠️Subscribe to reserve channel

🇷🇺Victory will be ours!

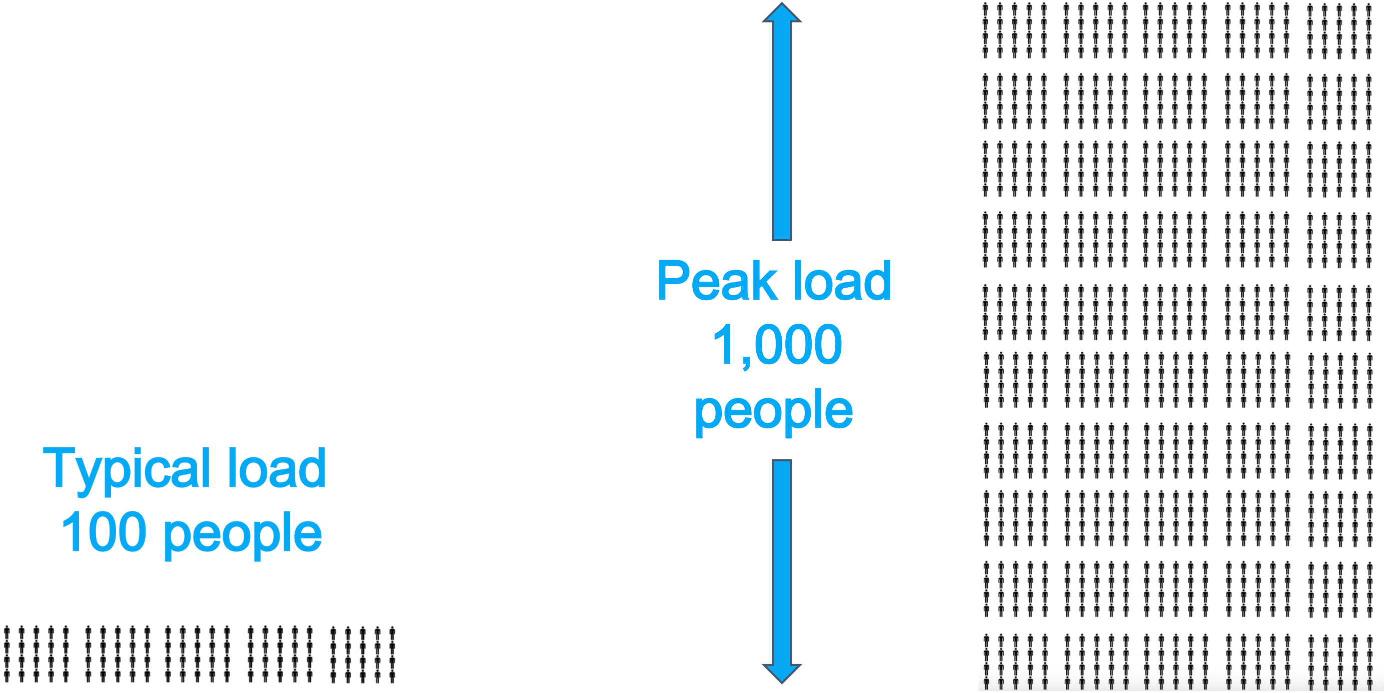
A series of attacks began targeting websites protected by RedShield

Large scale attacks peaked every ~24 hours

- Large scale attacks occurred throughout the day and night
- Following a repeated pattern targeting particular sites
- Culminating in a 2.34Tbps monster attack, one of the largest DDoS attacks of 2023 reported globally
- Expect to see attack sizes into 2024 take another jump in size



Normal user load of 100 - 1,000 people using the site

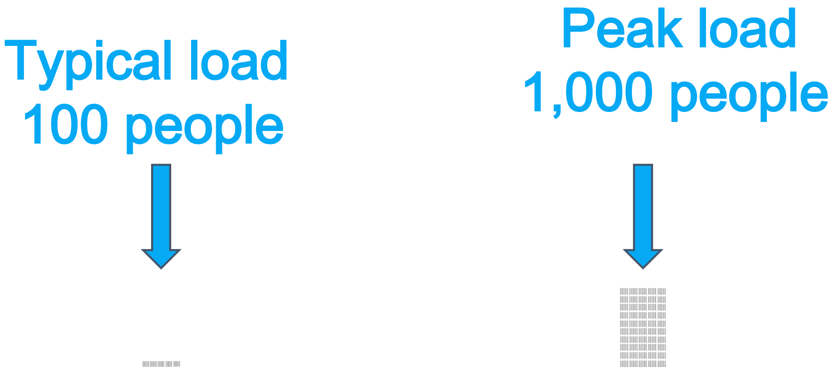


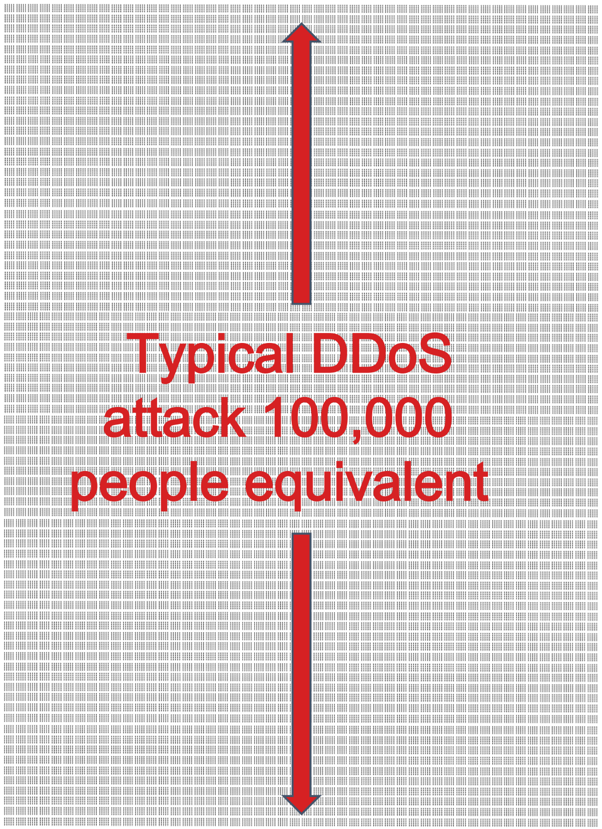
Typical load
100 people

Peak load
1,000
people

A typical large “DDoS” attack

- A common DDoS attack would see >100x normal load, equivalent to 100,000 normal users.
- Philadelphia Stadium holds 67,000



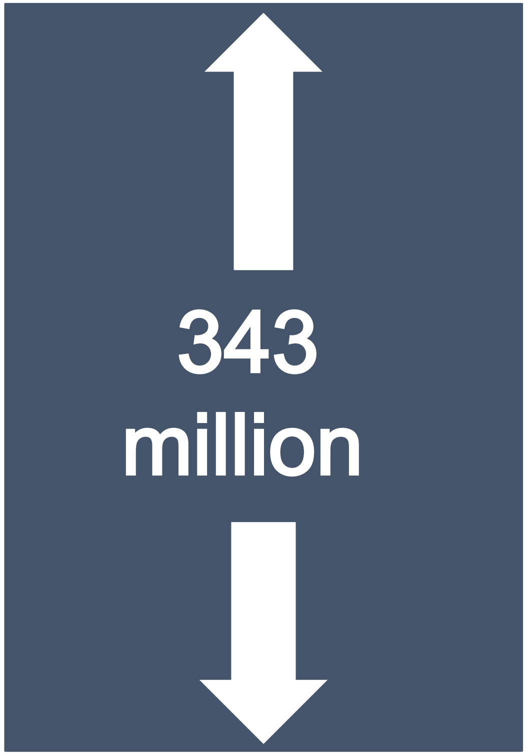


Colossal attack, equivalent to 343 million simultaneous web visitors

- This attack consumed network bandwidth equivalent to the entire population of the United States all visiting the website at once.
- Identifying and blocking the bad traffic throughout an attack at this scale, whilst providing uninterrupted service to good users, requires a massive globally distributed infrastructure, with autonomous machine-driven defensive controls

1000

100,000



343 million

Web Applications were the biggest avenue for data breaches in 2022

62%

Of all actual breaches now involve web applications

246 days

In 2021, the average time taken by developer teams to fix high severity vulnerabilities

12 months

It typically takes enterprise organizations 12 months to remediate **half** of their **new** vulnerabilities

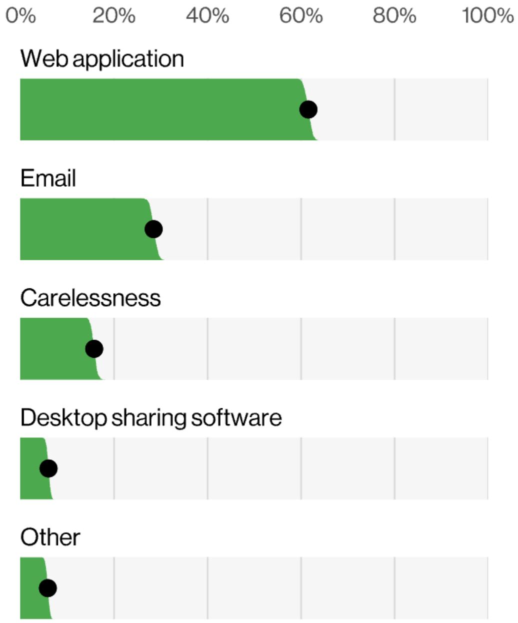
1.8B vs **27M**

With 1.8B websites globally and only 27M developers, **it is impractical to apply sufficient resources to resolve all exploitable problems for all applications.**

Web application breaches reinforce the need for MFA and vulnerability mitigation

- Threat actors rely on **exploitable flaws** within your applications - they can attack from the shadows and do not require social engineering or tricking of your staff.

- They leverage the **technical debt** that is common in all organizations with the competing resource requirements of innovation, and continuous maintenance of legacy systems

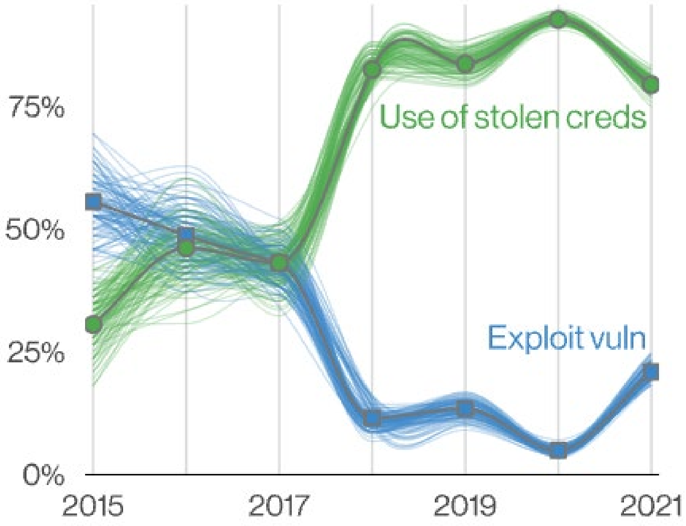


Verizon Breach Report 2023

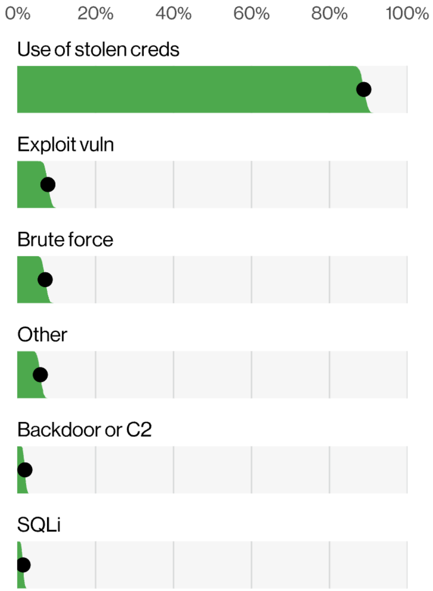
Stats taken from 3,194 breaches. Motivations are mostly financial (97%), and espionage (3%). Approx 70% organized crime, 7% nation state actors.

Use of stolen credentials is by far the biggest attack vector for bad actors, offering cost/time efficiency for breaching applications

Main sources of web app breaches



2022 main sources of web app breaches



Requires MFA

Requires strong perimeter hygiene

Requires MFA

Requires strong baseline controls

Requires strong baseline controls

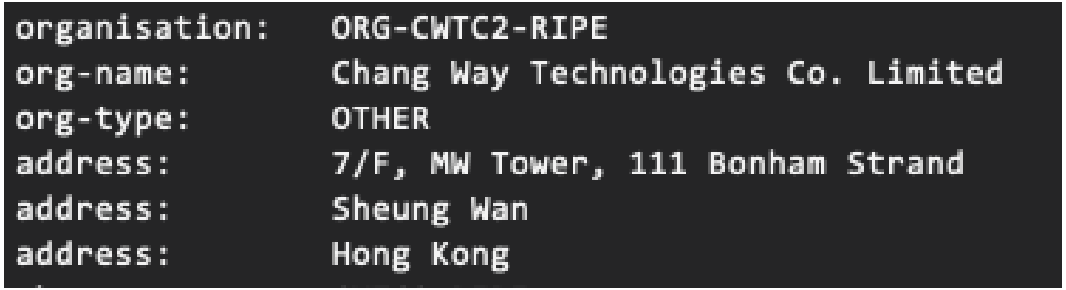
Login forms are soft targets for stolen credentials and brute force so should be a priority for security teams to protect

What are the problems with login pages?

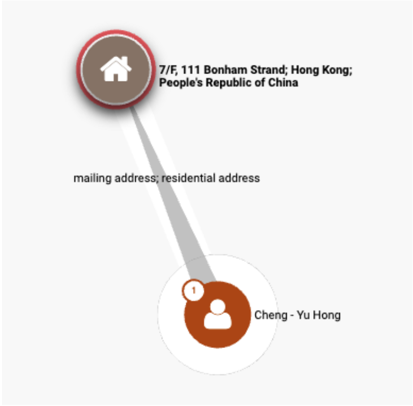
- Applications using login forms are often vulnerable:
  - Some apps allow weak or dictionary guessable passwords
  - Most apps allow reuse of creds which already appear in stolen password databases
  - MFA is not yet ubiquitous, especially for legacy apps
- Many apps do not prevent excessive / automated login attempts so brute force remains an effective attack vector
- Widespread availability of stolen credentials lists on the internet make exploitation easy and cost effective
- RedShield has observed growing numbers of bots crawling the enterprise perimeter, guessing large numbers of passwords; persisting for months

Russian hosted networks continuously probing for weaknesses

- The operating model is consistent with organised criminal groups
- Example: 193.x.y.z/24 network hosted in central Moscow has a poor reputation
- Continuous vulnerability scanning combined with brute force attempts
- Owned by Hong Kong shell company, registered to an address linked to many others via “Paradise Papers” leak
- Appears to be a Command and Control hosting network. A large number of fake websites, which often move hosting companies, and hostnames changing constantly

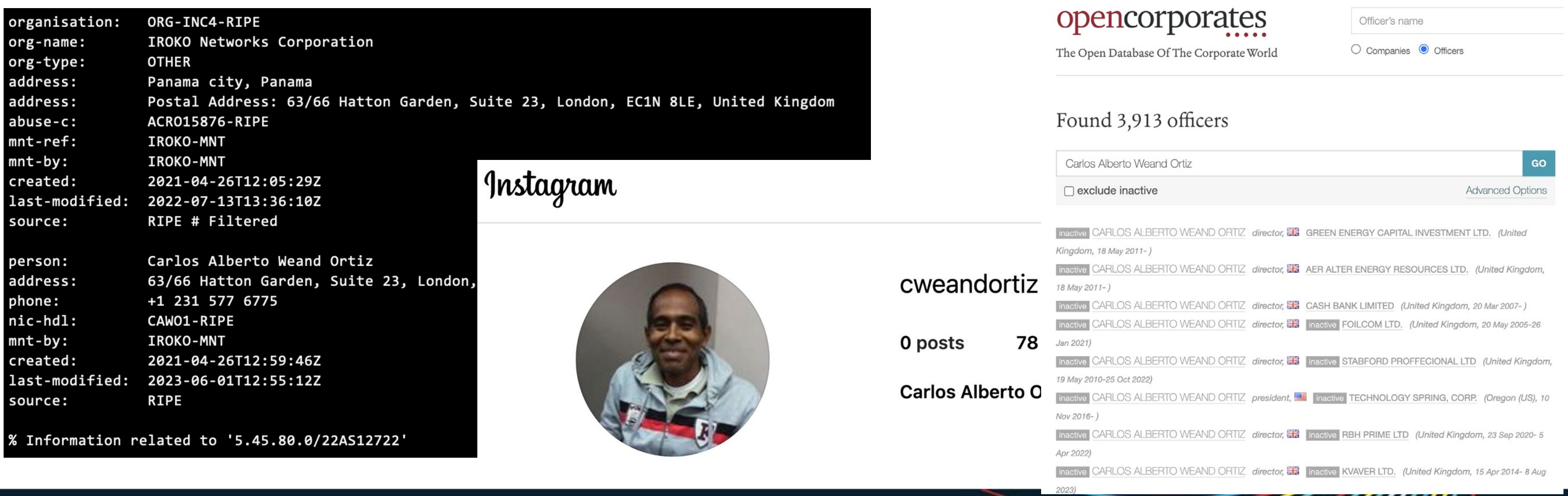


```
organisation:   ORG-CWTC2-RIPE
org-name:       Chang Way Technologies Co. Limited
org-type:       OTHER
address:        7/F, MW Tower, 111 Bonham Strand
address:        Sheung Wan
address:        Hong Kong
```


7/F, 111 Bonham Strand; Hong Kong; People's Republic of China
mailing address; residential address
1
Cheng - Yu Hong

Russian hosted networks continuously probing for weaknesses

- Iroko is a hosting and colocation company with abundant links to criminal activities
- 5.45.80.0/24 network hosted in Moscow has a poor reputation - spam, web blacklists, anonymizer proxies
- Continuous vulnerability scanning combined with brute force attempts
- Owned by Panama colo company, registered in UK, touting Panama’s “strong commitment to privacy”



```
organisation:   ORG-INC4-RIPE
org-name:       IROKO Networks Corporation
org-type:       OTHER
address:        Panama city, Panama
address:        Postal Address: 63/66 Hatton Garden, Suite 23, London, EC1N 8LE, United Kingdom
abuse-c:        ACRO15876-RIPE
mnt-ref:        IROKO-MNT
mnt-by:         IROKO-MNT
created:        2021-04-26T12:05:29Z
last-modified:  2022-07-13T13:36:10Z
source:         RIPE # Filtered

person:         Carlos Alberto Weand Ortiz
address:        63/66 Hatton Garden, Suite 23, London,
phone:          +1 231 577 6775
nic-hdl:        CAWO1-RIPE
mnt-by:         IROKO-MNT
created:        2021-04-26T12:59:46Z
last-modified:  2023-06-01T12:55:12Z
source:         RIPE

% Information related to '5.45.80.0/22AS12722'
```

Found 3,913 officers

Carlos Alberto Weand Ortiz GO

☐ exclude inactive Advanced Options

inactive CARLOS ALBERTO WEAND ORTIZ *director,* 🇬🇧 GREEN ENERGY CAPITAL INVESTMENT LTD. *(United Kingdom, 18 May 2011-)*

inactive CARLOS ALBERTO WEAND ORTIZ *director,* 🇬🇧 AER ALTER ENERGY RESOURCES LTD. *(United Kingdom, 18 May 2011-)*

inactive CARLOS ALBERTO WEAND ORTIZ *director,* 🇬🇧 CASH BANK LIMITED *(United Kingdom, 20 Mar 2007-)*

inactive CARLOS ALBERTO WEAND ORTIZ *director,* 🇬🇧 inactive FOILCOM LTD. *(United Kingdom, 20 May 2005-26 Jan 2021)*

inactive CARLOS ALBERTO WEAND ORTIZ *director,* 🇬🇧 inactive STABFORD PROFFECIONAL LTD *(United Kingdom, 19 May 2010-25 Oct 2022)*

inactive CARLOS ALBERTO WEAND ORTIZ *president,* 🇺🇸 inactive TECHNOLOGY SPRING, CORP. *(Oregon (US), 10 Nov 2016-)*

inactive CARLOS ALBERTO WEAND ORTIZ *director,* 🇬🇧 inactive RBH PRIME LTD *(United Kingdom, 23 Sep 2020- 5 Apr 2022)*

inactive CARLOS ALBERTO WEAND ORTIZ *director,* 🇬🇧 inactive KVAVER LTD. *(United Kingdom, 15 Apr 2014- 8 Aug 2023)*

Further underlying pressures from other APT groups are implicated in attacks blocked by RedShield

In addition to public claims by NoName057 hacker group, other Advanced Persistent Threat groups are implicated by the characteristics of attacks mitigated by RedShield against government applications:

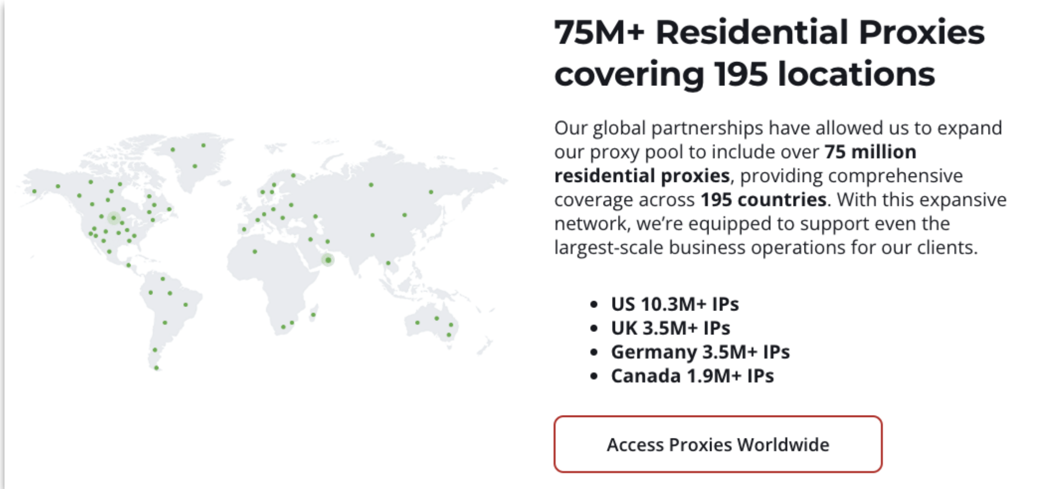
APT Group	Description	Attribution matching factors
APT41 Wicked Panda	APT41 is a threat group that researchers have assessed as a Chinese state -sponsored espionage group that also conducts financially -motivated operations. Active since at least 2012, APT41 has been observed targeting healthcare, telecom, technology, and video game industries in 14 countries.	● Attempts to exploit CVE-2019-3396 ● Attacks originating from extensive purpose-built infrastructure based in China
CARBANAK	CARBANAK is a cybercriminal group that specializes in financial crimes. They have conducted numerous high-profile attacks on banks and financial institutions, resulting in substantial financial losses.	● Attempts to exploit CVE-2017-5638 ● This attribution is lower confidence, due to this group historically targeting banks more than government organisations.
MUDDYWATER	MuddyWater is a cyber espionage group assessed to be a subordinate element within Iran's Ministry of Intelligence and Security (MOIS).[1] Since at least 2017, MuddyWater has targeted a range of government and private organizations across sectors, including telecommunications, local government, defense, and oil and natural gas organizations, in the Middle East, Asia, Africa, Europe, and North America.[2][3][4][5][6][7][8]	● Attempts to exploit CVE-2019-2725 ● Known to target government organizations.

Anonymising proxy networks

Massive parallel IPs - residential proxy services

Attackers can rotate through virtually unlimited proxies hosted on unlisted IPs, making traditional defenses much less effective:

- IP based session tracking and rate limiting
- IP reputation and geo blocking
- IP threshold banning



75M+ Residential Proxies covering 195 locations

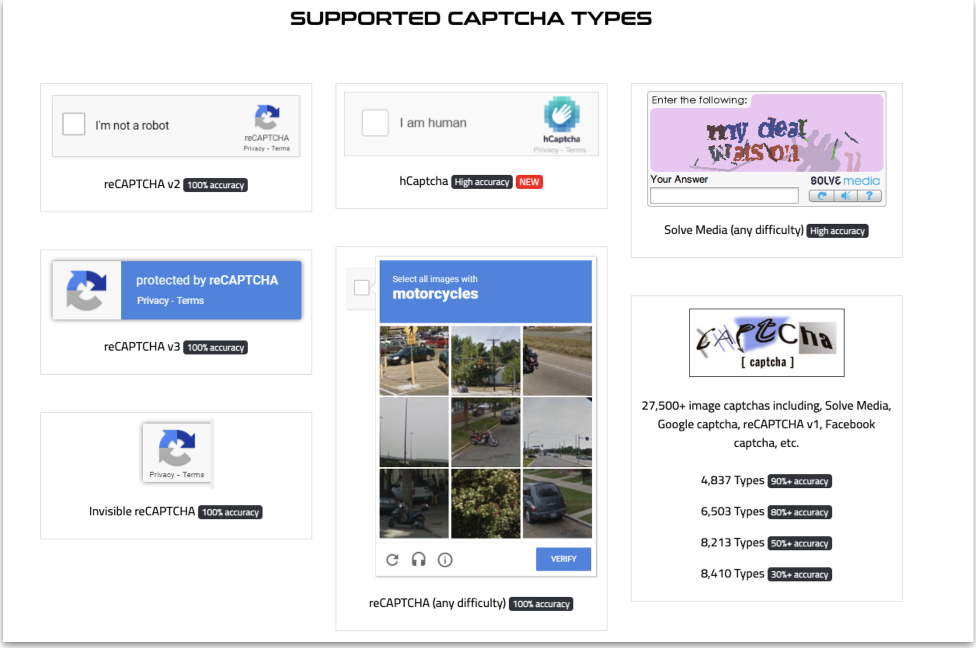
Our global partnerships have allowed us to expand our proxy pool to include over **75 million residential proxies**, providing comprehensive coverage across **195 countries**. With this expansive network, we're equipped to support even the largest-scale business operations for our clients.

- **US 10.3M+ IPs**
- **UK 3.5M+ IPs**
- **Germany 3.5M+ IPs**
- **Canada 1.9M+ IPs**

AI Powered CAPTCHA Services are Rapidly Evolving

AI has reduced the cost of CAPTCHA solving for bot herders, improving economies of scale for attackers

- AI-powered CAPTCHA services have automated solutions for most common CAPTCHA services
- Easy and cheap, via API
- Human-powered services fill the gaps with complex/premium CAPTCHA schemes



SUPPORTED CAPTCHA TYPES

reCAPTCHA v2 100% accuracy

hCaptcha High accuracy NEW

Solve Media (any difficulty) High accuracy

reCAPTCHA v3 100% accuracy

reCAPTCHA (any difficulty) 100% accuracy

Invisible reCAPTCHA 100% accuracy

27,500+ image captchas including, Solve Media, Google captcha, reCAPTCHA v1, Facebook captcha, etc.

4,837 Types 90%+ accuracy

6,503 Types 80%+ accuracy

8,213 Types 50%+ accuracy

8,410 Types 30%+ accuracy

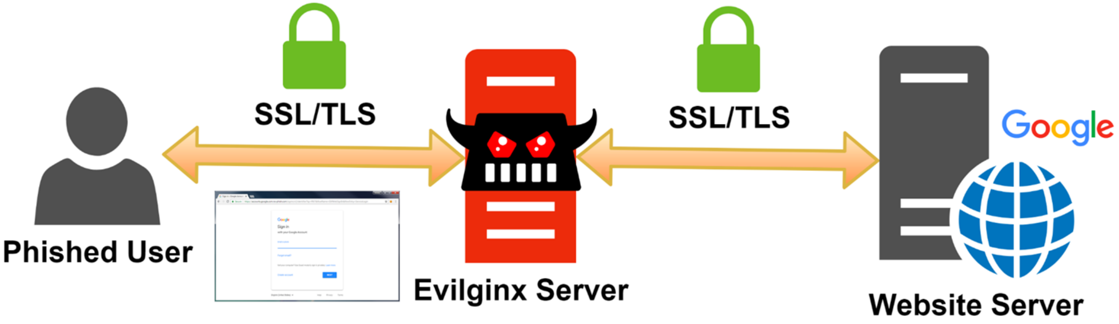
Phishing kits offer an easy way to bypass some MFA

Non-phishing -resistant MFA is easily bypassed

- Time-based One Time Password apps
- Apps which allow login approval in-app
- SMS and email one-time-passwords

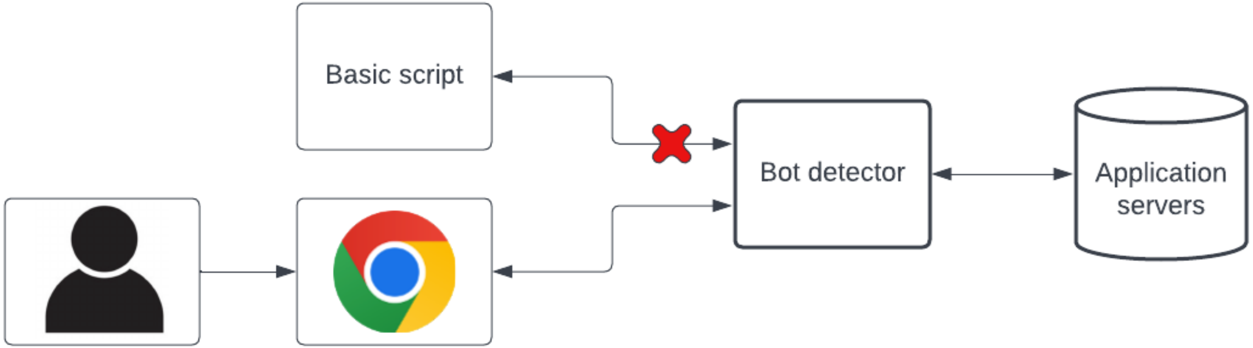
Trivially set up a proxy which is transparent/identical to the victim website except for hostname

https://yourdomain.com.KE6wlBDdSV.co/dxIFrvcK9JslqC



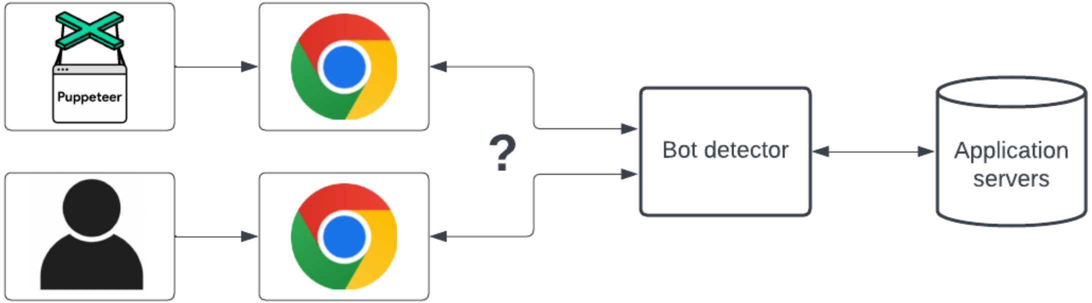
Bot mitigation used to be so simple

- Early bots were standalone scripts that did not process Javascript sent from the server.
- Client side Javascript tests worked to detect a bot vs a real browser.



Bots used to be so simple

- Newer bots are more often scripts that drive a headless browser to evade detection.
- The headless browser has Javascript execution capability and can behave just like any real browser - it IS a real browser



Anti -bot defense systems

Anti-bot defenses try to detect bots vs humans:

- Client fingerprinting, human/bot indicators
  - IP reputation, geolocation
  - Client side javascript sensors (indicators of automation frameworks, window size, plugins, mouse movements)
- Behaviour analysis over time
  - Non-human session characteristics - URI patterns, tripwires
  - Timing of requests (ML-based)
  - Trending and thresholding (eg failed logins per minute, per IP, per geo, etc)

Anti -bot defense systems have serious challenges

All of the ’sensor’ information is under the control of the adversary and should not be trusted.

- Indicators of real human activity can be spoofed
- Indicators of automation frameworks can be hidden

CAPTCHAs are facing serious challenges from AI and human-driven solving services

False positives are typically not tolerated by the business. AI approaches to mitigation must be extremely accurate.

The effort of defining, implementing, configuring, tuning and maintaining countermeasures should not be underestimated.

https://owasp.org/www-pdf-archive/Automated-threat-handbook.pdf

Anti -bot defense systems have serious challenges

RedShield engineers performed testing of automated login processes against login pages

- Three target websites - mix of production (online banking) and test sites
- Three leading* cloud WAF and anti-automation vendors
- Anti-bot feature sets enabled and tuned according to vendor recommendations

Goals:

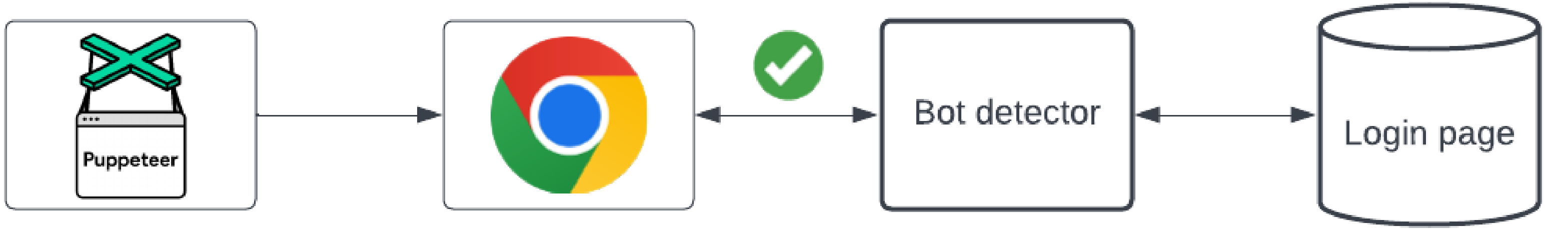
- Test automated logins using a dictionary of credentials
- Observe any differences in detection techniques, and their effectiveness

Anti -bot defense systems have serious challenges

Configuration of some bot mitigation strategies caused excessive false positives, and in all cases had limited tuning options and visibility

- eg, Advanced behavioural detection

For successful automated logins, randomised mouse move calls and randomised wait times were all that was required (minimal expertise).



Bots are increasingly human -identical

- Detecting the difference between an unknown human user, and a bot impersonating a human, is becoming impossible
- For this reason, security policy makers and insurance providers are increasingly mandating the use of MFA for all applications which handle personal information.
- In practise, this includes many existing and legacy applications
- Integrating MFA into the login flow for web applications can be a major burden on over-busy developer teams

Changing the game with effective mitigation

Exploring the challenges and emerging solutions for mitigating risk

CISA cannot put it more strongly: MFA is a critical priority

> As the Nation’s Cyber Defense Agency, CISA sees how our nation’s adversaries operate and what tools they use.
>
> While some of these adversaries use advanced tools and techniques, most take advantage of **unpatched vulnerabilities**, poor cyber hygiene or the **failure of organizations to implement critical technologies like MFA**.
>
> Sadly, too few organizations learn how valuable MFA is until they experience a breach.
>
> ***Jen Easterly, Director, US Cyber Security and Infrastructure Security Agency (CISA)***

FIDO2 is ideal for critical accounts, but has some limitations

- **Hardware tokens** are strong and very difficult to clone, but have drawbacks:
    - Logistics
    - User/key lifecycle management can weaken security, reliant on email and helpdesk
    - Cost

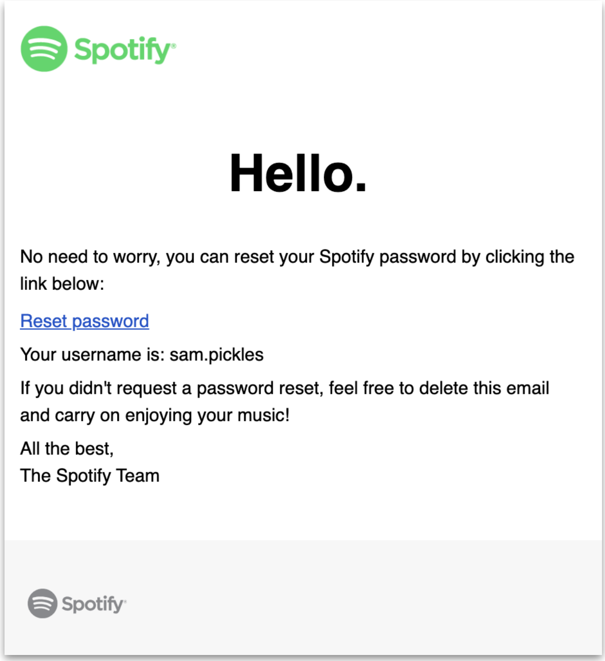
- **Passkeys** are very promising for devices that the user exclusively controls
    - Not suitable for public library or shared computers
    - Can present challenges for marginalized communities and the general public

https://stablediffusionweb.com

Email “Magic Link” Solves Many of these Issues

“Magic link” provides a non-guessable link via email, to open a new session

- Works well as additional factor, to augment existing password authentication in legacy apps
- Password delete takes additional setup
- Security of email is foundational to this scheme
  - Note: in practical use, email security is foundational to most authentication, even FIDO2 - *because of enrollment processes and password/MFA reset via email and/or support tickets.*



Hello.

No need to worry, you can reset your Spotify password by clicking the link below:

Reset password

Your username is: sam.pickles

If you didn't request a password reset, feel free to delete this email and carry on enjoying your music!

All the best,
The Spotify Team

RedShield’s No Touch MFA reduces the risk of a breach due to compromised accounts without relying on constrained resources

Let RedShield implement and manage MFA and SSO for legacy web applications; leaving your developers free to focus

RedShield’s No Touch MFA service includes options for:

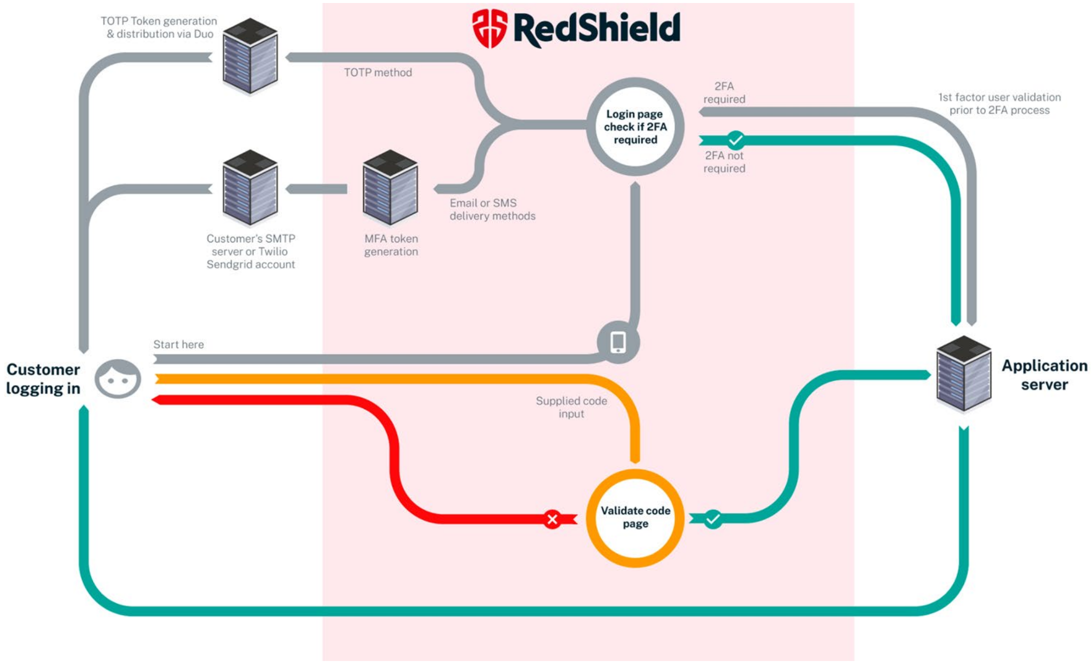
- TOTP, SMS and email, Phishing Resistant Magic Link
- Integration with Sendgrid, Twilio, Duo
- Logging integration with common SIEM platforms
- Standard and customised email and login form templates
- SSO integration with Okta and Entra ID (Azure AD)
- Hardening application session tokens and authorization vulnerabilities
- IP reputation, geolocation and email domain restrictions

Without changing your application code, secure your login pages to reduce the risk of these account takeovers.

With RedShield we were able to implement MFA in days. This was for both new and legacy applications and all without having to divert valuable development team resource.

Tier 1 Australian Telecommunications provider

RedShield's No Touch MFA operates on full proxy architecture in global data centres to mitigate DDoS, ensure speed & availability


RedShield
TOTP Token generation & distribution via Duo
TOTP method
Login page check if 2FA required
2FA required
2FA not required
1st factor user validation prior to 2FA process
Customer's SMTP server or Twilio Sendgrid account
MFA token generation
Email or SMS delivery methods
Start here
Customer logging in
Supplied code input
Validate code page
Application server

RedShield's No Touch MFA can flexibly use a range of methods to:

- determine the username & generate authorisation tokens
- engage directly with standard company resources to send the message via email, SMS or TOTP
- validate the authorization token
- handle exceptions
- generate appropriate assurance logs

All that is required is a simple DNS change

Also mitigates CVEs and penetration test findings

No Code. No Resources. No Touch

MFA rollout for the resource -strapped CISO

MFA and SSO for legacy apps addresses the practical challenges

- Excluded content and IPs
- Unusual authn schemes
- Javascript and redirects
- Multi stage form posts
- Password reset schemes
- Single page apps and server-server APIs with token auth schemes
- Device trust workflows, step up authentication and risk-based policies

Whilst avoiding:

- Requirement for code changes and software re-engineering
- Cost of hardware and software tokens, and third party smart device apps
- Logistics of enrollment - helpdesk and excessive customer communications overheads during rollout

Link to Slides and FREE Attack Surface Risk Report

Sam Pickles
sam@redshield.co