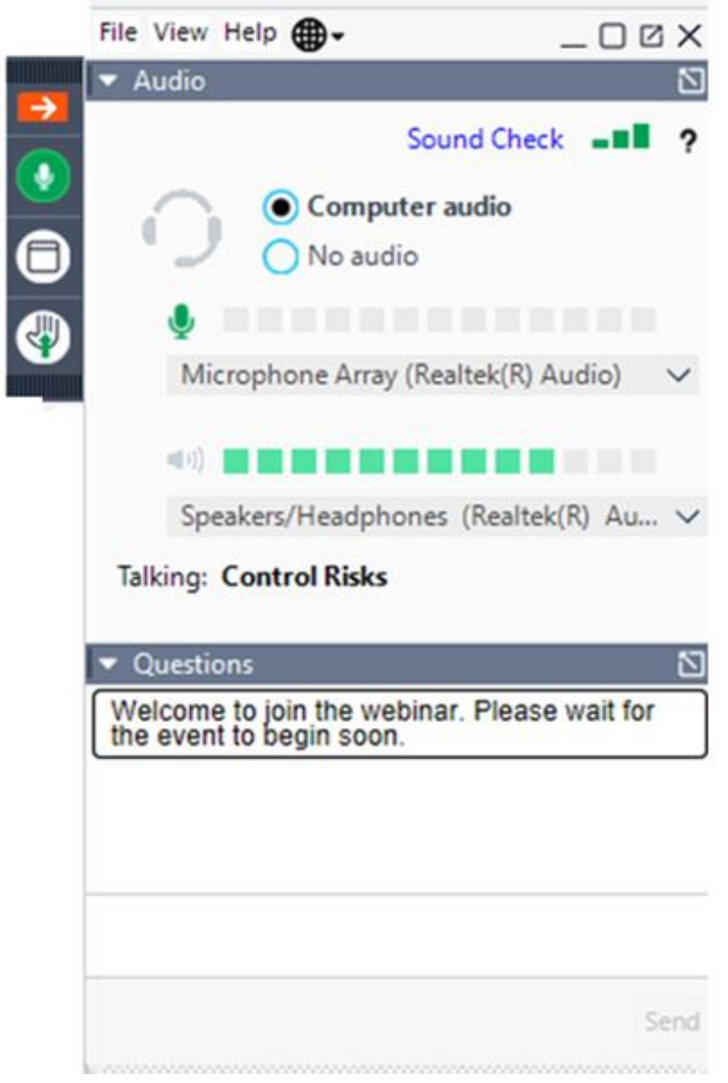
Please type your questions here throughout the webinar



Today's Speakers

From Control Risks

Shaun Flint

Consultant

Cyber Protect

Luke Fardell

Associate Director

Digital Forensics

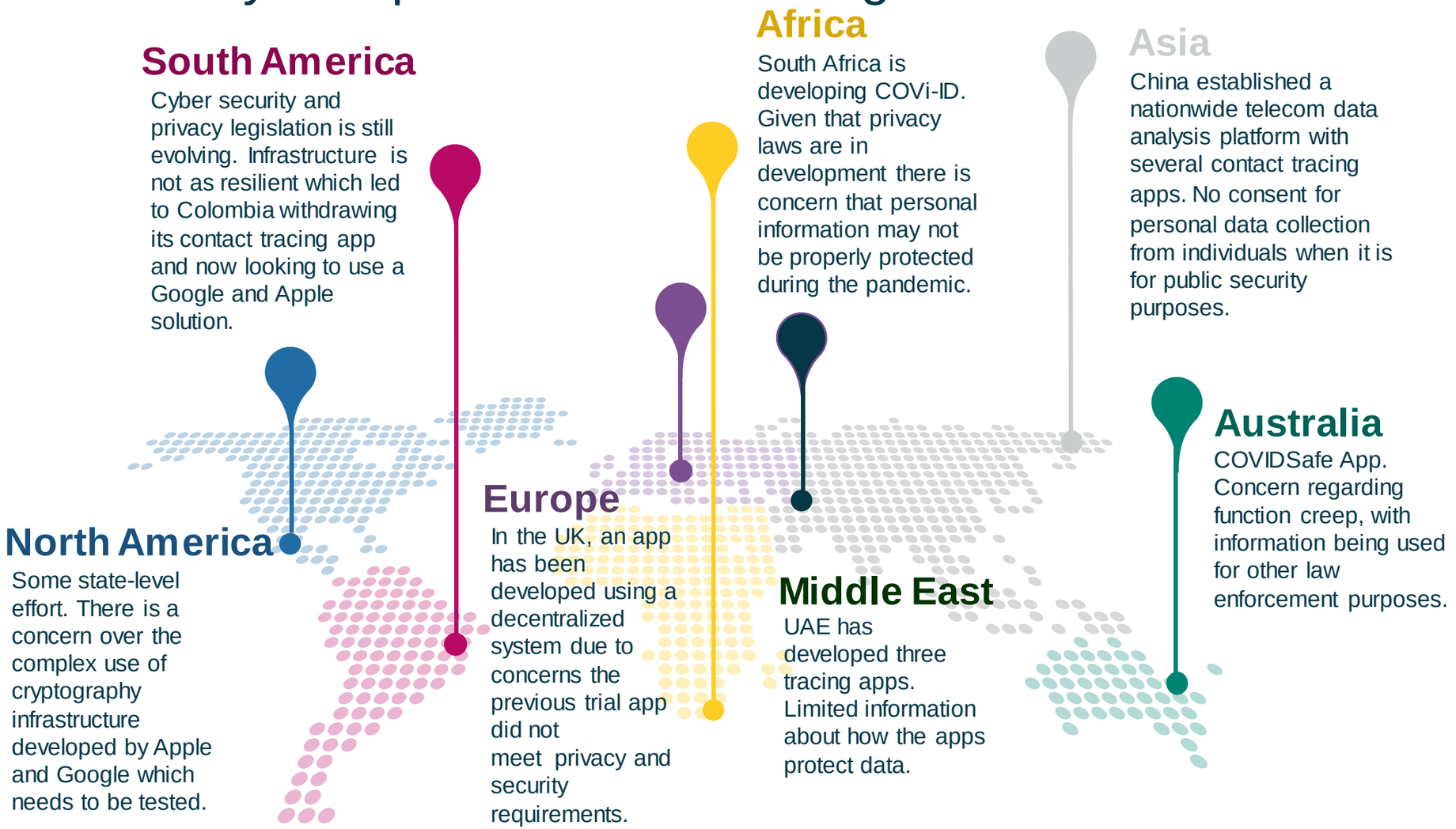
James Lythe

Associate Director

Crisis Management

Global Cyber Security trends

Global cyber security compliance trends during COVID-19



South America

Cyber security and privacy legislation is still evolving. Infrastructure is not as resilient which led to Colombia withdrawing its contact tracing app and now looking to use a Google and Apple solution.

North America

Some state-level effort. There is a concern over the complex use of cryptography infrastructure developed by Apple and Google which needs to be tested.

Europe

In the UK, an app has been developed using a decentralized system due to concerns the previous trial app did not meet privacy and security requirements.

Africa

South Africa is developing COVi-ID. Given that privacy laws are in development there is concern that personal information may not be properly protected during the pandemic.

Middle East

UAE has developed three tracing apps. Limited information about how the apps protect data.

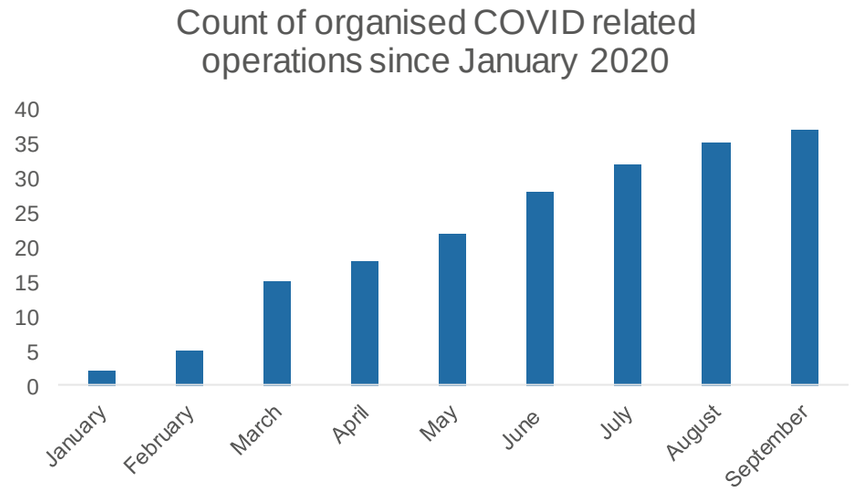
Asia

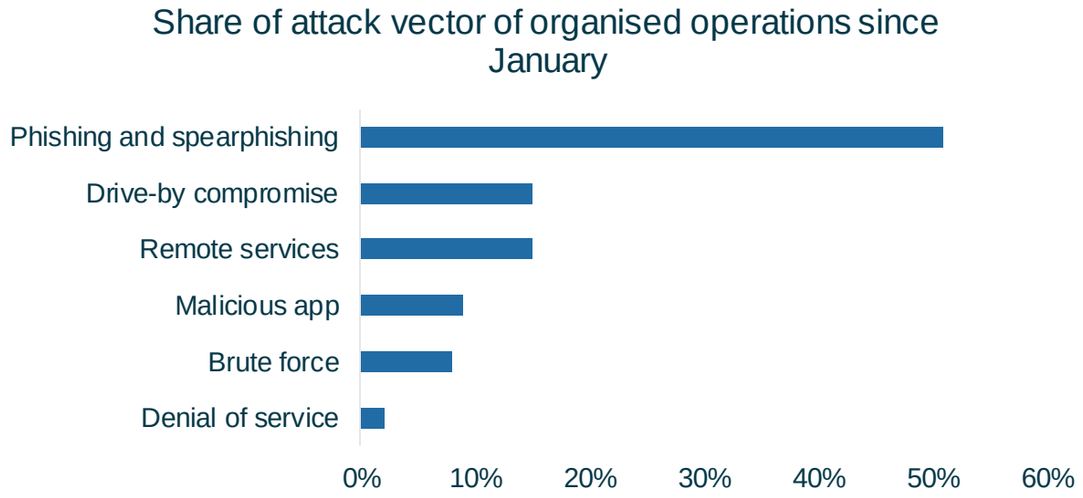
China established a nationwide telecom data analysis platform with several contact tracing apps. No consent for personal data collection from individuals when it is for public security purposes.

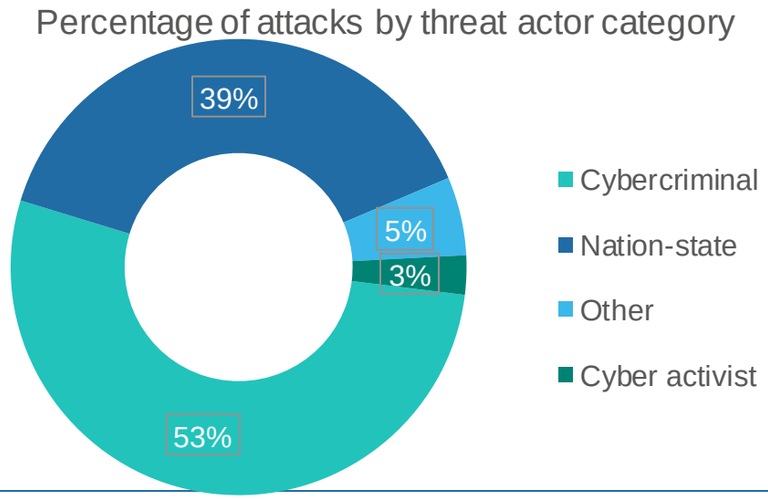
Australia

COVIDSafe App. Concern regarding function creep, with information being used for other law enforcement purposes.

Update on cyber attacks exploiting the pandemic





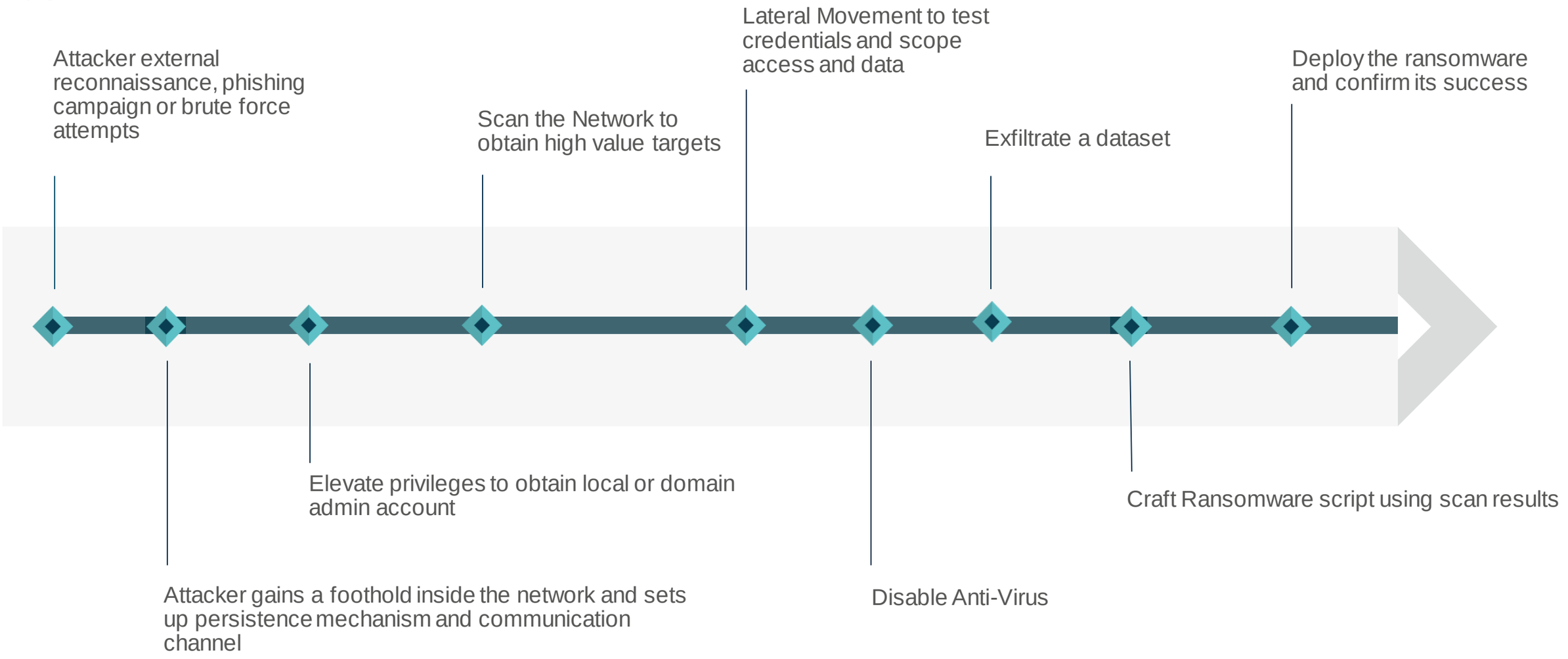


Recent Attack Vectors

Since March 2020 the following attack vectors have been observed during Control Risks Cyber Response Cases

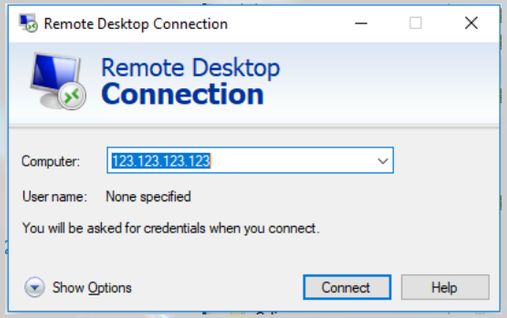
- Enterprise equipment in home environment misconfiguration
- False sense of security phishing
- Perimeter misconfiguration
- Huge email chain campaign – Qakbot/Dopplepaymer
- Remote Desktop Protocol (RDP) access
- Webserver compromise through vulnerable 3rd party application
- Website defacement through Server Side Template Injection

Typical Attack Timeline



Most Common Attack Vectors

VS



Scenario

Pandos Chicken are not getting enough customers

They want to steal the secret recipe from their rivals Nan's Chicken

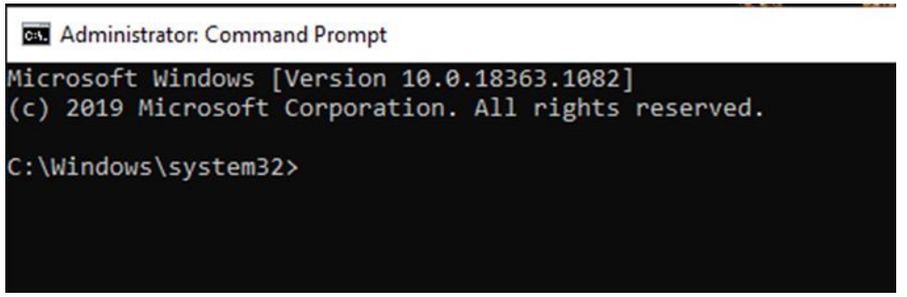
Nan's Chicken have a very secure network, previous attempts have failed.

Pandos identify that Nan's Chicken get their chickens from 'Dave the chicken farmer'

Objective

Obtain a Shell in the Nan's Chicken network

There is no greater objective….



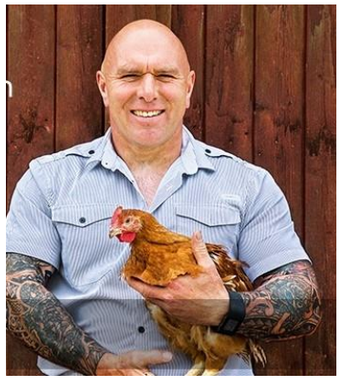
Attack Path

Pandos

01

Dave the Farmer

02



Nan's Chicken

03

Secret_Recipe.txt

Nan's Chicken

Hack Dave's email

Reconnaissance

- Website
- Companies House
- Google
- Facebook
- Twitter
- Instagram

DAVE LIMITED

Company number

Follow this company | File for this company

Overview | Filing history | People | More

Registered office address

Company status

Active

Company type

Private limited Company

Incorporated on

7 July 2004

Accounts

Next accounts made up to **30 April 2020**
due by **30 April 2021**

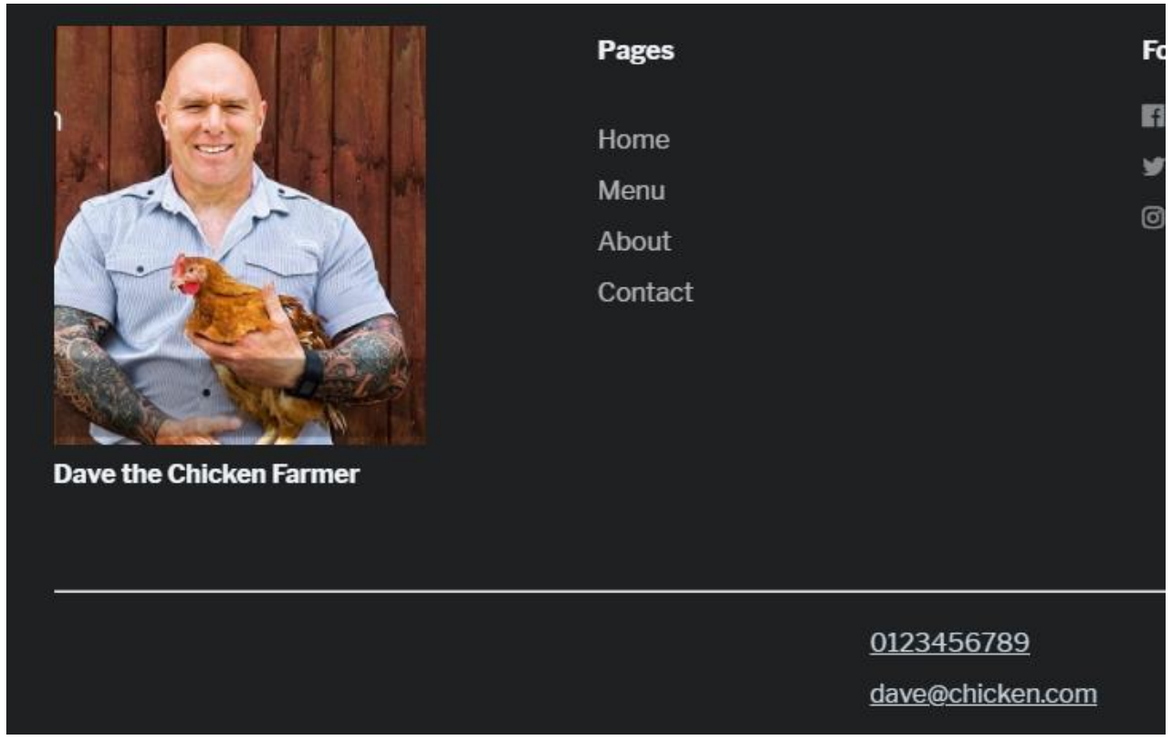
Last accounts made up to **30 April 2019**

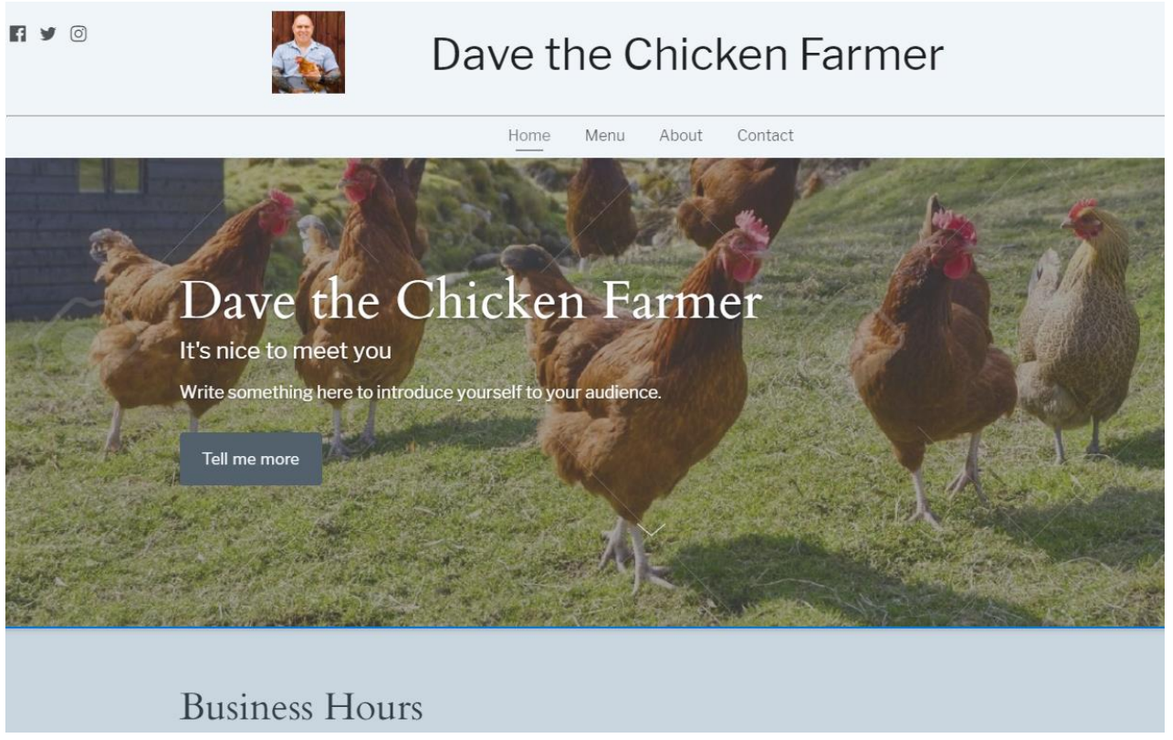
Confirmation statement overdue

Next statement date **14 August 2020**
due by **25 September 2020**

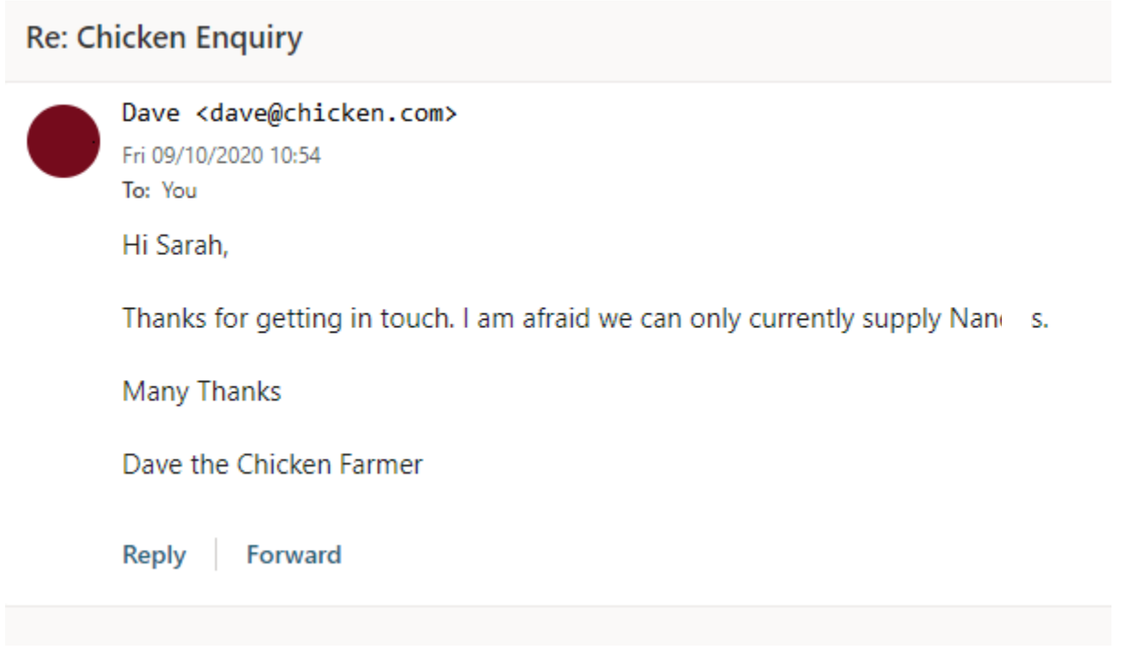
Last statement dated **14 August 2019**

Dave's Website





Email Dave




```
MIME-Version: 1.0
Date: Fri, 9 Oct 2020 09:51:16 +0000
Message-ID: <CAHGwVuyUalgLcZyE6TcRp9EjKedSSC5UU6HJaACid5aptwtRfA@mail.gmail.com>
Subject: Re: Chicken Enquiry
From: Dave <Dave@chicken.com>
To: Sarah <Sarah@mail.com>
Content-Type: multipart/alternative; boundary="000000000000f3a46805b139e376"

--000000000000f3a46805b139e376
Content-Type: text/plain; charset="UTF-8"

Hi Sarah,

Thanks for getting in touch. I am afraid we can only currently supply Nanc s.

Many Thanks

Dave the Chicken Farmer

--000000000000f3a46805b139e376
Content-Type: text/html; charset="UTF-8"

<div dir="ltr">Re: Chicken Enquiry</div>

--000000000000f3a46805b139e376--
```

Obtain Credentials for Dave's Gmail

- Trick Dave into entering his credentials into a fake google webpage.

Re: Chicken Enquiry

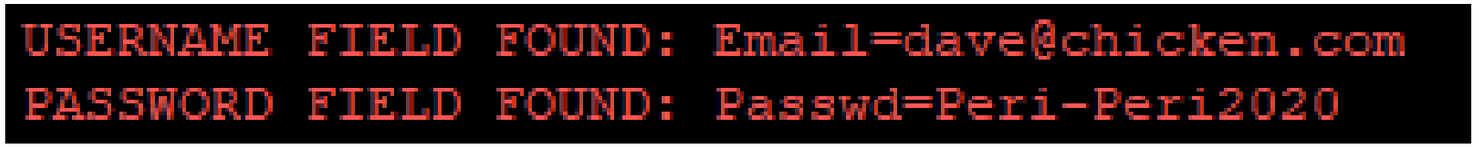
Many thanks Dave,

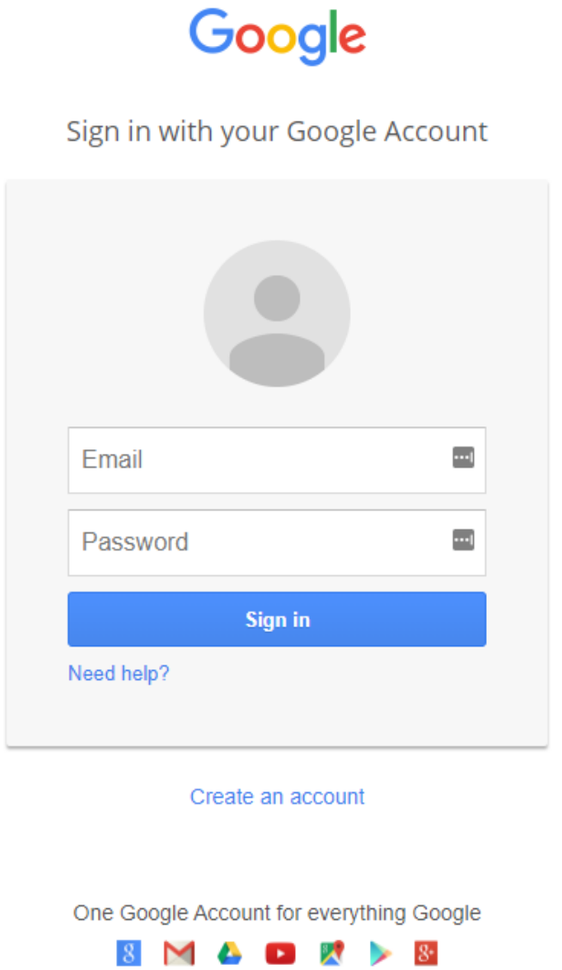
Thats not a problem, one thing you should know is that I think Nan ` s are going to change suppliers very soon.

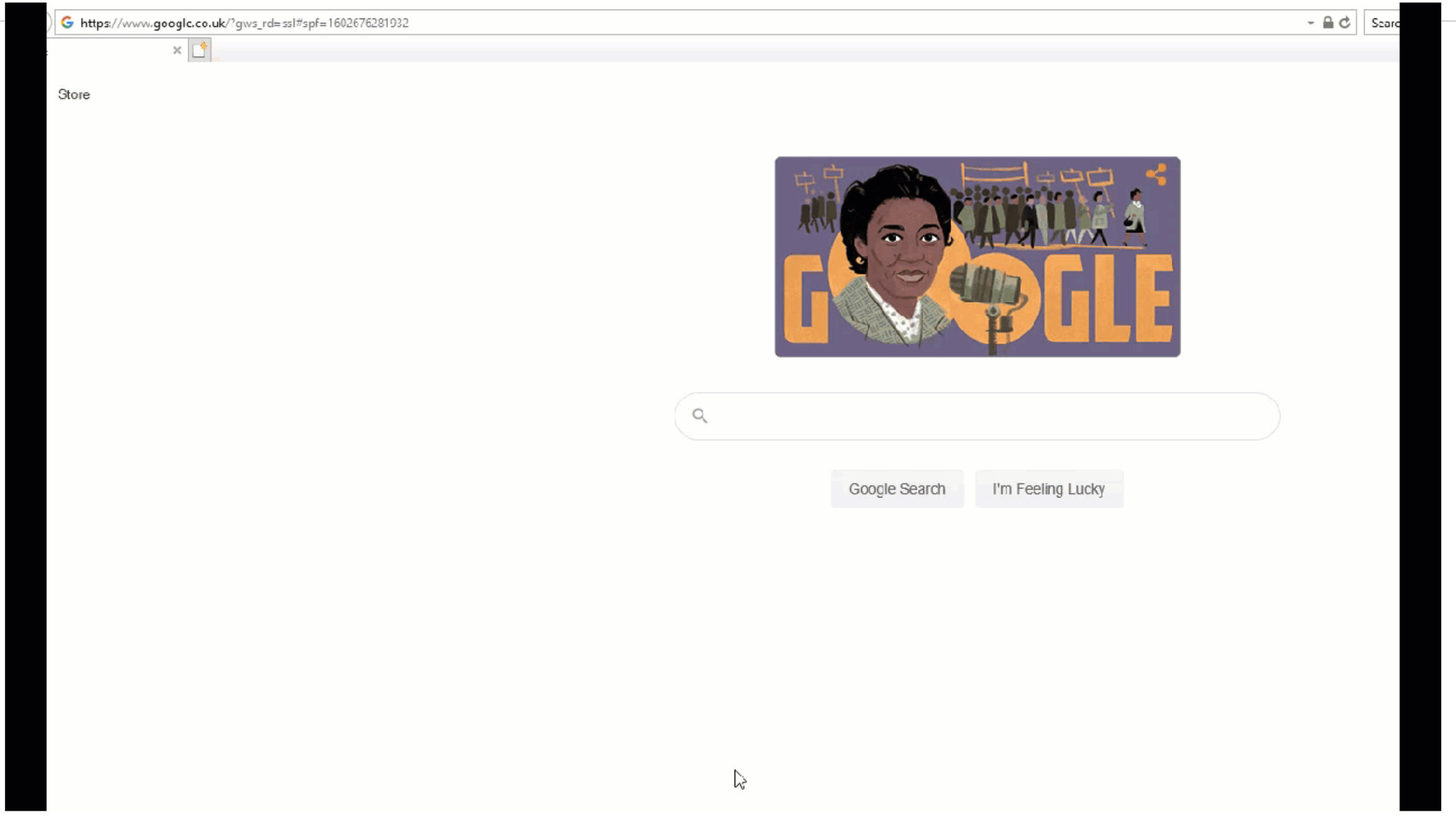
Read this secret document I have uploaded to google which someone passed to me ... https://bit.ly/2GIpqBz

Many thanks

Sarah



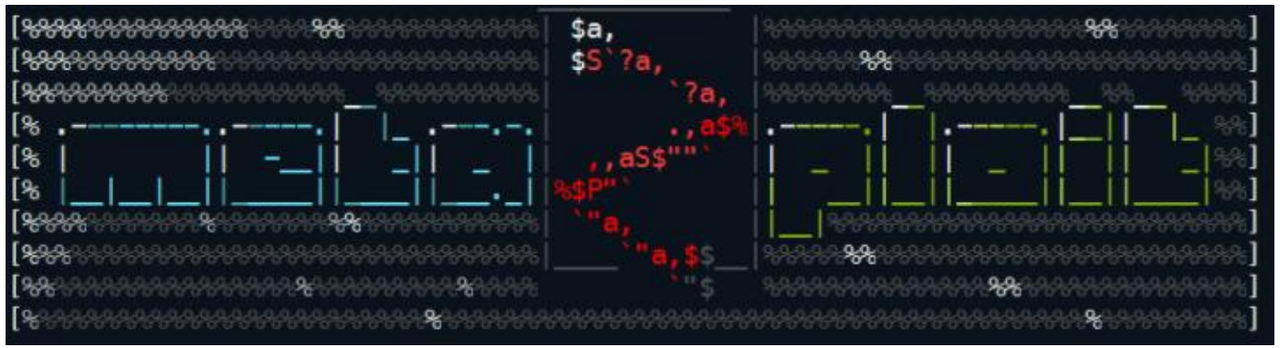



https://www.google.co.uk/?gws_rd=ssl#spf=1602676281932
Store
Google Search
I'm Feeling Lucky

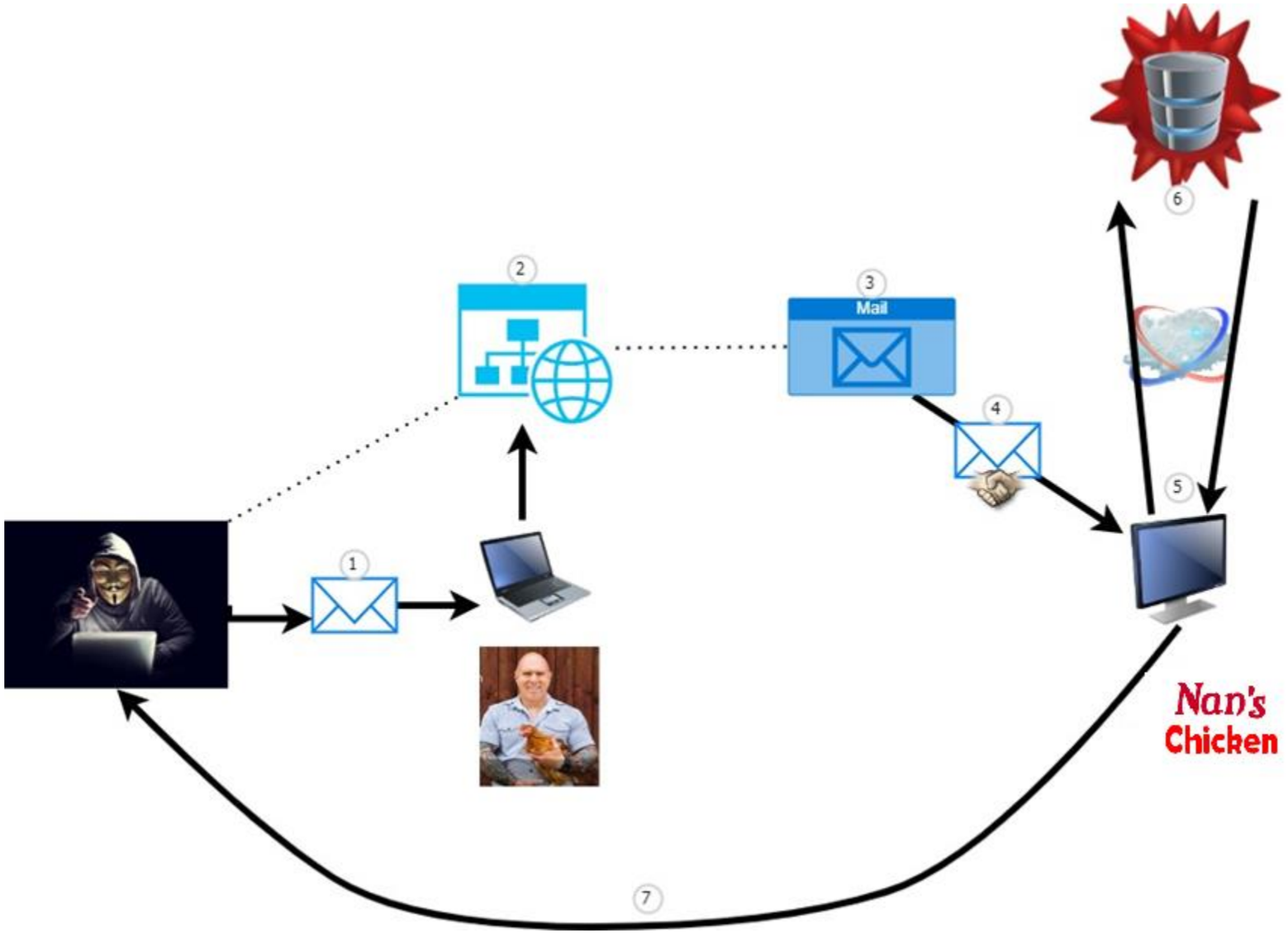
```
Edit this file, and change HARVESTER_REDIRECT and
HARVESTER_URL to the sites you want to redirect to
after it is posted. If you do not set these, then
it will not redirect properly. This only goes for
templates.

-------------------------------------------------------

  1. Java Required
  2. Google
  3. Twitter

set:webattack> Select a template:2

[*] Cloning the website: http://www.google.com
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] You may need to copy /var/www/* into /var/www/html depending on where your directory structure is.
Press {return} if you understand what we're saying here.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

We use Dave's email account

- Craft a payload to beacon back to our infrastructure
- Set up infrastructure
- Use Dave's email to send the payload
- Wait for reverse TCP connection

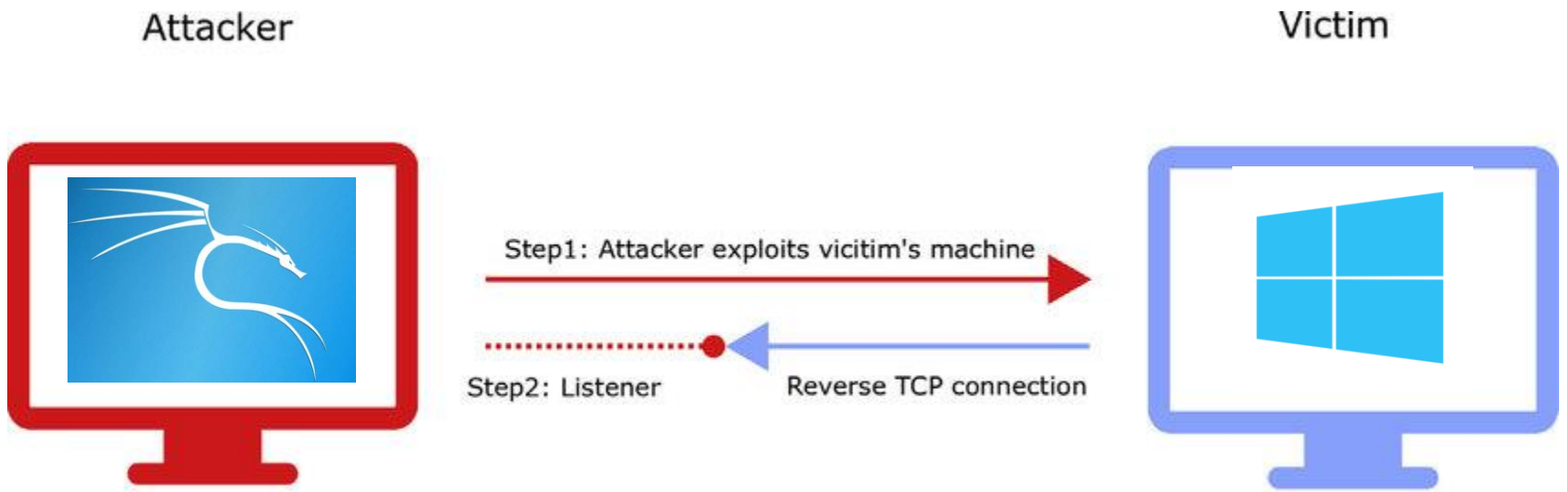


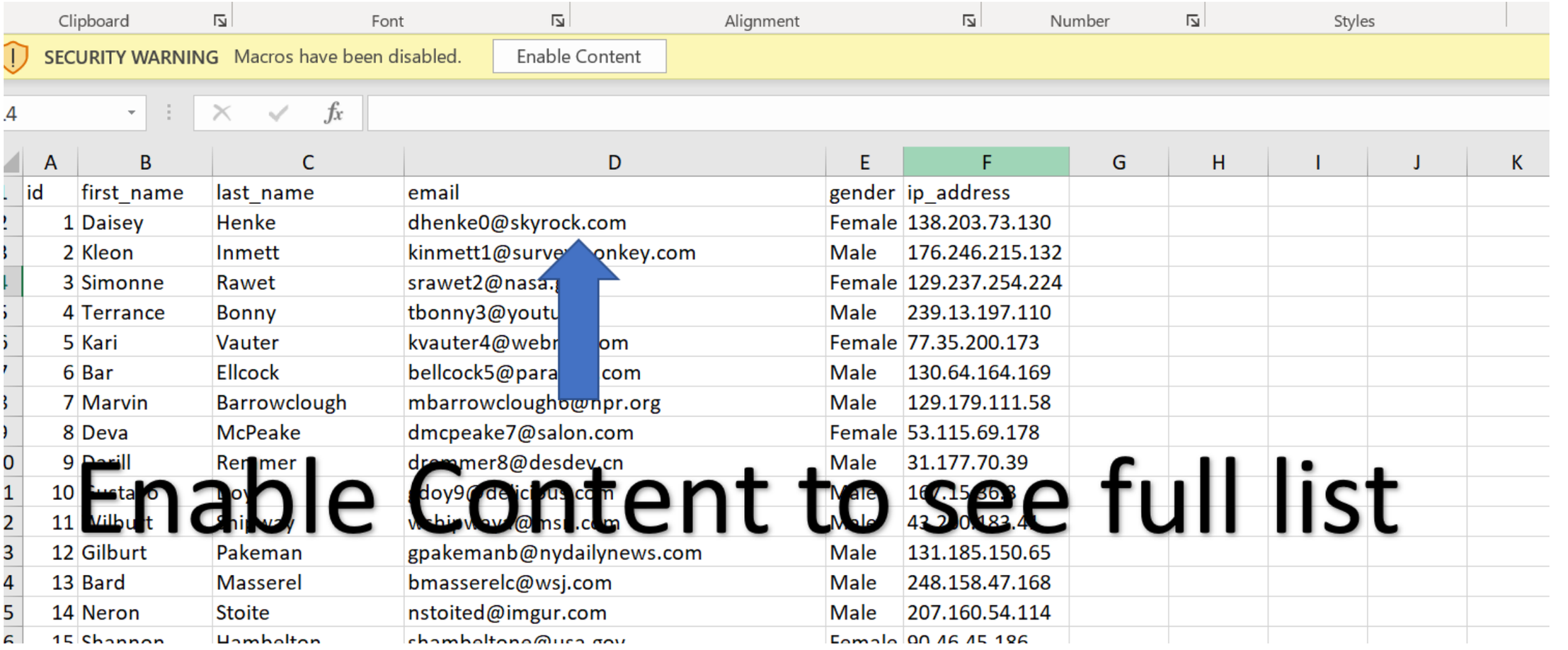
Recap



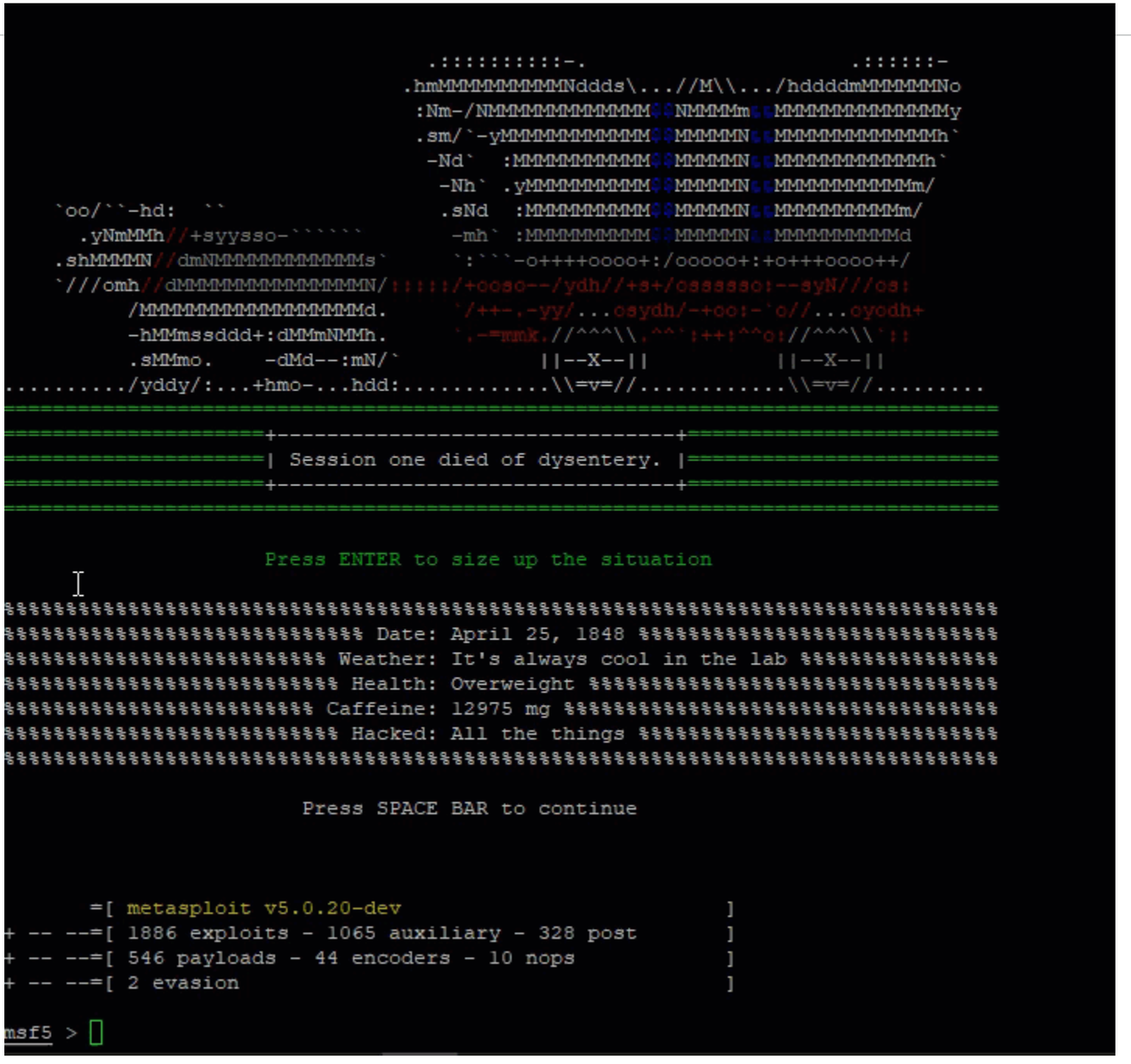
Capabilities of the Reverse TCP connection

- Read and Edit documents
- Upload/download files
- Execute binaries
- Privilege escalation
- Network scanning
- Clear event logs
- Search for files
- Open Webcam
- Screenshots





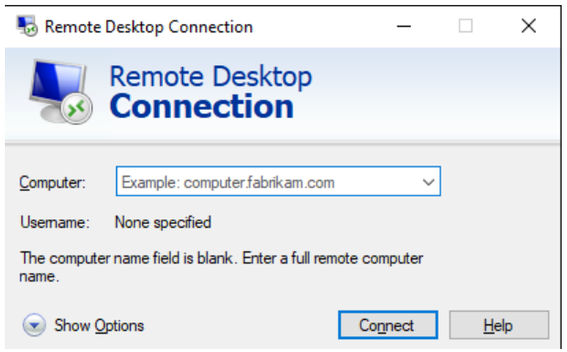
	A	B	C	D	E	F	G	H	I	J	K
1	id	first_name	last_name	email	gender	ip_address					
2	1	Daisey	Henke	dhenke0@skyrock.com	Female	138.203.73.130					
3	2	Kleon	Inmett	kinmett1@surve[illegible]onkey.com	Male	176.246.215.132					
4	3	Simonne	Rawet	srawet2@nasa.[illegible]	Female	129.237.254.224					
5	4	Terrance	Bonny	tbonny3@youtu[illegible]	Male	239.13.197.110					
6	5	Kari	Vauter	kvauter4@webr[illegible]om	Female	77.35.200.173					
7	6	Bar	Ellcock	bellcock5@para[illegible]com	Male	130.64.164.169					
8	7	Marvin	Barrowclough	mbarrowclough6@npr.org	Male	129.179.111.58					
9	8	Deva	McPeake	dmcpeake7@salon.com	Female	53.115.69.178					
10	9	Derill	Rem[illegible]mer	dr[illegible]mer8@desdev.cn	Male	31.177.70.39					
11	10	Gustavo	Doy[illegible]	gdoy9@delicious.com	Male	167.153.36.8					
12	11	Wilburt	Shipway	wshipway[illegible]@ms[illegible].com	Male	43.200.183.47					
13	12	Gilburt	Pakeman	gpakemanb@nydailynews.com	Male	131.185.150.65					
14	13	Bard	Masserel	bmasserelc@wsj.com	Male	248.158.47.168					
15	14	Neron	Stoite	nstoited@imgur.com	Male	207.160.54.114					
16	15	Shannon	Hambelton	shambeltone@usa.gov	Female	90.46.45.186					

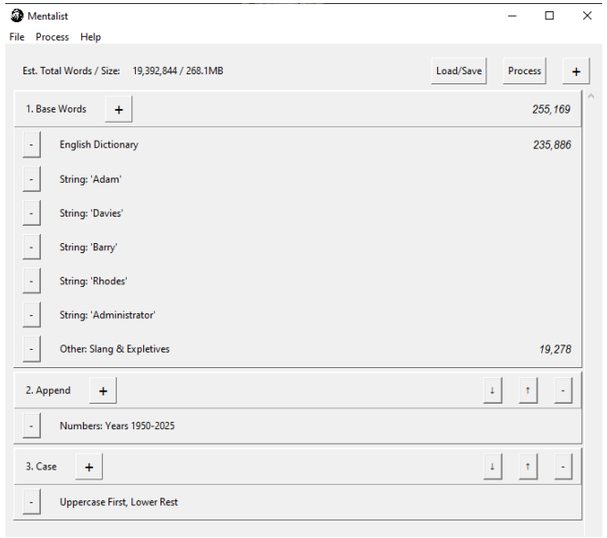

Session one died of dysentery.
Press ENTER to size up the situation
Date: April 25, 1848
Weather: It's always cool in the lab
Health: Overweight
Caffeine: 12975 mg
Hacked: All the things
Press SPACE BAR to continue
=[metasploit v5.0.20-dev
+ -- --=[1886 exploits - 1065 auxiliary - 328 post
+ -- --=[546 payloads - 44 encoders - 10 nops
+ -- --=[2 evasion
msf5 >

RDP Brute Force

Externally facing systems with RDP access

- Remote scans of networks to identify systems
- Username often visible
- Password brute force attack mounted until access gained



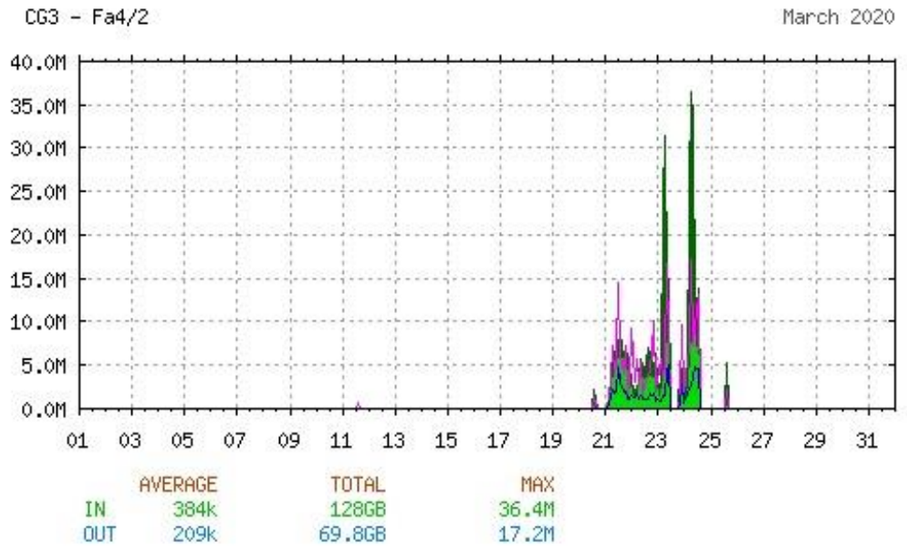


Type	Date	Time	Event	Source	Category	User	Computer
Audit Failure	09/07/2020	08:11:38	4625	Microsoft-Windows-Se	Logon	N/A	DESKTOP-CC8SR0E
Audit Failure	09/07/2020	08:11:38	4625	Microsoft-Windows-Se	Logon	N/A	DESKTOP-CC8SR0E
Audit Failure	09/07/2020	08:11:37	4625	Microsoft-Windows-Se	Logon	N/A	DESKTOP-CC8SR0E
Audit Failure	09/07/2020	08:11:37	4625	Microsoft-Windows-Se	Logon	N/A	DESKTOP-CC8SR0E
Audit Failure	09/07/2020	08:11:37	4625	Microsoft-Windows-Se	Logon	N/A	DESKTOP-CC8SR0E
Audit Failure	09/07/2020	08:11:37	4625	Microsoft-Windows-Se	Logon	N/A	DESKTOP-CC8SR0E
Audit Failure	09/07/2020	08:11:37	4625	Microsoft-Windows-Se	Logon	N/A	DESKTOP-CC8SR0E
Audit Failure	09/07/2020	08:11:37	4625	Microsoft-Windows-Se	Logon	N/A	DESKTOP-CC8SR0E
Audit Failure	09/07/2020	08:11:37	4625	Microsoft-Windows-Se	Logon	N/A	DESKTOP-CC8SR0E
Audit Failure	09/07/2020	08:11:37	4625	Microsoft-Windows-Se	Logon	N/A	DESKTOP-CC8SR0E
Audit Failure	09/07/2020	08:11:37	4625	Microsoft-Windows-Se	Logon	N/A	DESKTOP-CC8SR0E
Audit Failure	09/07/2020	08:11:37	4625	Microsoft-Windows-Se	Logon	N/A	DESKTOP-CC8SR0E
Audit Failure	09/07/2020	08:11:37	4625	Microsoft-Windows-Se	Logon	N/A	DESKTOP-CC8SR0E
Audit Failure	09/07/2020	08:11:37	4625	Microsoft-Windows-Se	Logon	N/A	DESKTOP-CC8SR0E
Audit Failure	09/07/2020	08:11:37	4625	Microsoft-Windows-Se	Logon	N/A	DESKTOP-CC8SR0E
Audit Failure	09/07/2020	08:11:37	4625	Microsoft-Windows-Se	Logon	N/A	DESKTOP-CC8SR0E
Audit Failure	09/07/2020	08:11:37	4625	Microsoft-Windows-Se	Logon	N/A	DESKTOP-CC8SR0E
Audit Failure	09/07/2020	08:11:37	4625	Microsoft-Windows-Se	Logon	N/A	DESKTOP-CC8SR0E
Audit Failure	09/07/2020	08:11:37	4625	Microsoft-Windows-Se	Logon	N/A	DESKTOP-CC8SR0E
Audit Failure	09/07/2020	08:11:37	4625	Microsoft-Windows-Se	Logon	N/A	DESKTOP-CC8SR0E
Audit Failure	09/07/2020	08:11:37	4625	Microsoft-Windows-Se	Logon	N/A	DESKTOP-CC8SR0E
Audit Failure	09/07/2020	08:11:37	4625	Microsoft-Windows-Se	Logon	N/A	DESKTOP-CC8SR0E
Audit Failure	09/07/2020	08:11:37	4625	Microsoft-Windows-Se	Logon	N/A	DESKTOP-CC8SR0E
Audit Failure	09/07/2020	08:11:37	4625	Microsoft-Windows-Se	Logon	N/A	DESKTOP-CC8SR0E
Audit Failure	09/07/2020	08:11:37	4625	Microsoft-Windows-Se	Logon	N/A	DESKTOP-CC8SR0E
Audit Failure	09/07/2020	08:11:37	4625	Microsoft-Windows-Se	Logon	N/A	DESKTOP-CC8SR0E
Audit Failure	09/07/2020	08:11:37	4625	Microsoft-Windows-Se	Logon	N/A	DESKTOP-CC8SR0E
Audit Failure	09/07/2020	08:11:37	4625	Microsoft-Windows-Se	Logon	N/A	DESKTOP-CC8SR0E
Audit Failure	09/07/2020	08:11:37	4625	Microsoft-Windows-Se	Logon	N/A	DESKTOP-CC8SR0E
Audit Failure	09/07/2020	08:11:37	4625	Microsoft-Windows-Se	Logon	N/A	DESKTOP-CC8SR0E
Audit Failure	09/07/2020	08:11:37	4625	Microsoft-Windows-Se	Logon	N/A	DESKTOP-CC8SR0E
Audit Failure	09/07/2020	08:11:37	4625	Microsoft-Windows-Se	Logon	N/A	DESKTOP-CC8SR0E
Audit Failure	09/07/2020	08:11:37	4625	Microsoft-Windows-Se	Logon	N/A	DESKTOP-CC8SR0E

Description

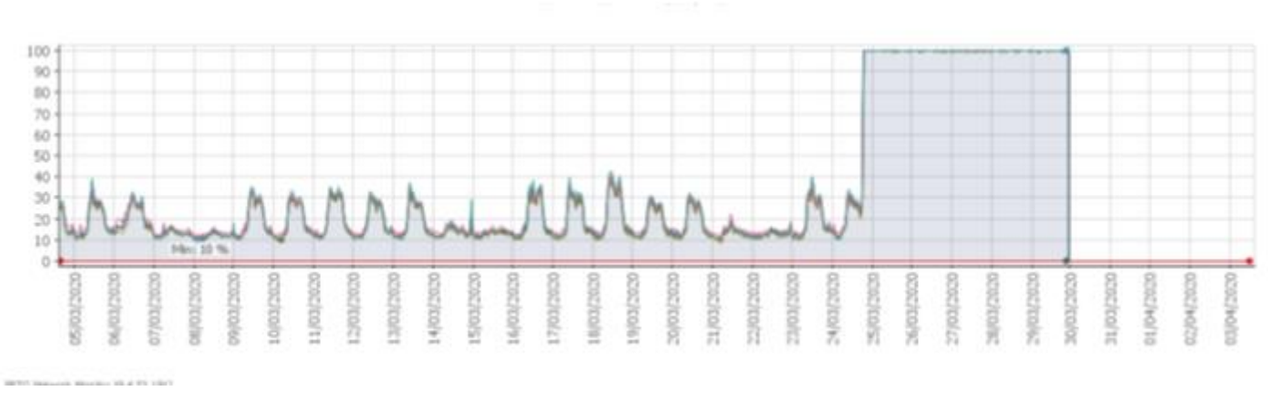
An account failed to log on.
Subject:
Security ID: S-1-0-0
Account Name: -
Account Domain: -
Logon ID: 0x0
Logon Type: 3
Account For Which Logon Failed:
Security ID: S-1-0-0
Account Name: User
Account Domain: ?
Failure Information:
Failure Reason: Unknown user name or bad password.
Status: 0xc000006d
Sub Status: 0xc000006a
Process Information:
Caller Process ID: 0x0
Caller Process Name: -
Network Information:
Workstation Name: CR-LT-108
Source Network Address: 192.168.1.159
Source Port: 0

Exfiltration of Data



Exfiltration methods observed

- Archiving of files for exfil
- RDPClip – Copy and pasting through remote session
- Mailbox syncing using stolen credentials
- Staging on Webserver for external download
- SMB shares
- Meterpreter Session over HTTPS
- FTP.exe



Remote Crisis Management

Managing cyber risk remotely

Awareness

Corporate Comms
Training
Phishing Simulation
Tech Talks

Corporate

Segregation
Multi Factor Authentication
Gateway Filtering
Audit and Logging

Home

Virtual Private Network
Change Default Settings
Update Devices
Dialogue with IT Teams

Three areas of focus for cyber crisis management

Companies are actively reviewing and changing their strategic approach to resilience, to bring clarity to uncertainty. We've outlined three of the common themes below

Leadership

- How can leaders improve the speed and response of decision making
- How can risk specialists help improve strategic decision making
- How can leaders educate themselves about the risks
- Knowing when to call a crisis

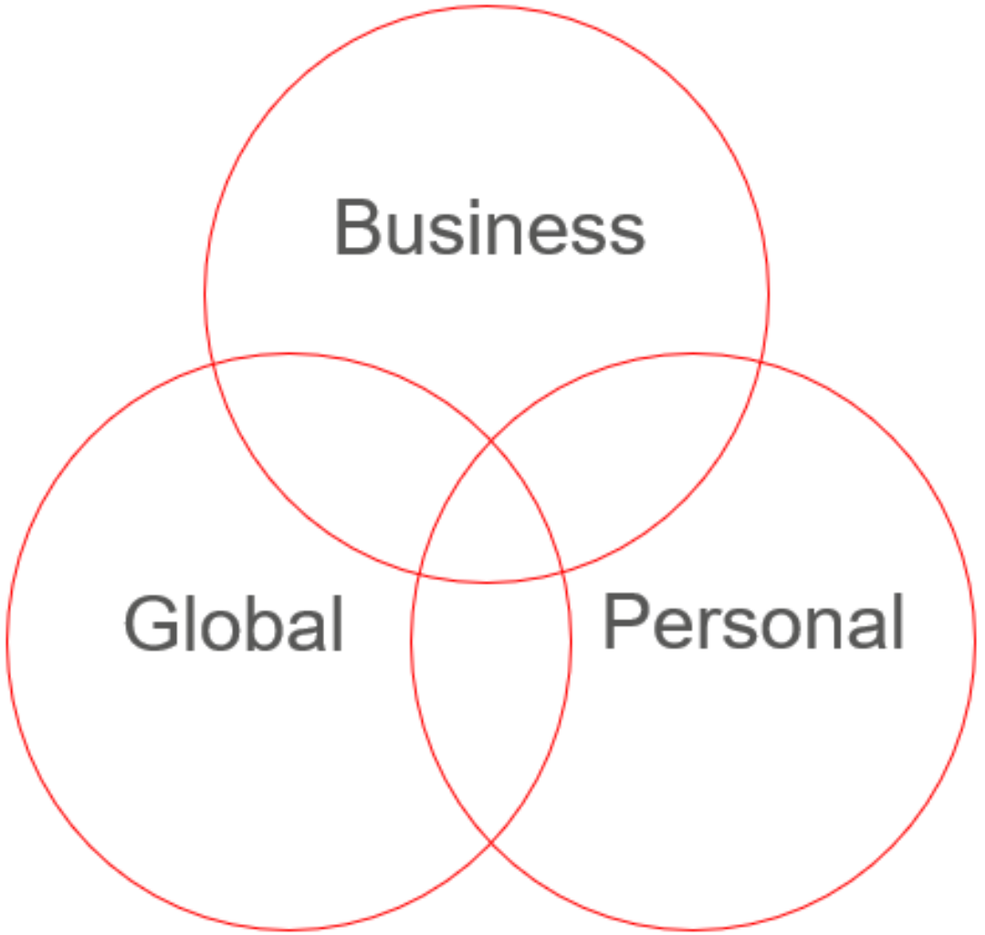
People

- How can people become a more integrated part of the resilience framework
- How can we enable employees to work flexibly while maintaining well-being and security
- What skills do employees need to develop

Intelligence

- Which risks need to be monitored and what triggers are needed
- How can the situation be understood and communicated to key stakeholders
- How do we make our cyber contingency plans agile and mobile
- Who are the experts we need to call

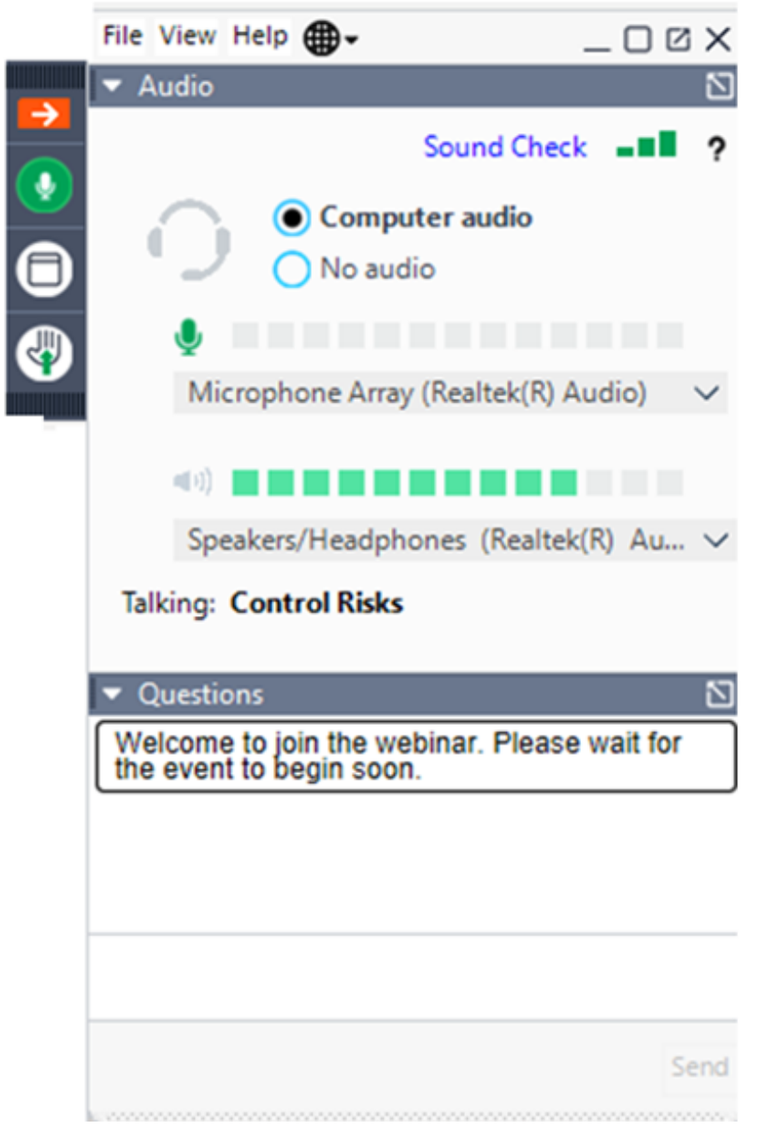
A final thought - developing resilience



Don’t go back to normal, go back to better

Q&A

Please type your questions here



controlrisks.com